OPTICAL CRYPTOGRAPHY USING PANDA RING RESONATOR FOR INFORMATION SECURITY

RATTIPONG PUTTHACHAROEN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
DOCTOR OF ENGINEERING IN ELECTRICAL ENGINEERING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2012

KMITL-2012-EN-D-018-033

หัวข้อวิทยานิพนธ์	**การเข้ารหัสสัญญาณทางแสงโดยใช้วงแหวนสั่นพ้องชนิดแพนด้า เพื่อความปลอดภัยของข้อมูลในระบบสารสนเทศ**
นักศึกษา	นายรัฐิติ์พงษ์ พุทธเจริญ
รหัสประจำตัว	48060056
ปริญญา	วิศวกรรมศาสตรดุษฎีบัณฑิต
สาขาวิชา	วิศวกรรมไฟฟ้า
พ.ศ.	2555
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ.ดร. สมศักดิ์ มิตะถา
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	รศ. ประทีป บัญญัตินพรัตน์

บทคัดย่อ

วิทยานิพนธ์นี้นำเสนอระบบรักษาความปลอดภัยให้กับการสื่อสารข้อมูลด้วยเส้นใยนำแสง โดยการประยุกต์ใช้สัญญาณเสมือนสัญญาณรบกวนที่สร้างจากวงแหวนสั่นพ้องชนิดแพนด้าเพื่อสร้างระบบสื่อสารด้วยเส้นใยนำแสงที่มีความปลอดภัยสูง

ผู้วิจัยเริ่มต้นด้วยการนำเสนอผลการศึกษาเทคโนโลยีพื้นฐานที่เกี่ยวข้อง เช่น โซลิตอนแบบสว่างและแบบมืด อุปกรณ์ทางแสงที่เกี่ยวข้อง การเข้ารหัสข้อมูล สัญญาณรบกวน และการสื่อสารโดยใช้หลักการเคออส หลังจากนั้นผู้วิจัยได้ทำการนำเสนอผลการศึกษาพฤติกรรมผันผวนที่เกิดจากการแพร่กระจายและการชนกันของสัญญาณโซลิตอนแบบสว่างและแบบมืดในวงแหวนสั่นพ้องชนิดแพนด้า และตามด้วยการนำเสนอระบบที่ผู้วิจัยได้ทำการออกแบบขึ้น ซึ่งในการออกแบบนี้ผู้วิจัยเจาะจงเลือกใช้เฉพาะอุปกรณ์ทางแสงที่มีขนาดเล็กเป็นหลัก ในวิทยานิพนธ์นี้ผู้วิจัยได้ทำการประยุกต์ใช้สัญญาณเสมือนสัญญาณรบกวน ร่วมกับการใช้คีย์ลับ และคีย์เข้าและถอดรหัส ในการรักษาความปลอดภัยให้กับระบบสื่อสารข้อมูลด้วยเส้นใยนำแสง ระบบที่ออกแบบทำการสร้างสัญญาณเสมือนสัญญาณรบกวนจากพฤติกรรมผันผวนที่เกิดจากการแพร่กระจายและการชนกันของสัญญาณโซลิตอนแบบสว่างและแบบมืดในวงแหวนสั่นพ้องชนิดแพนด้า คีย์ลับถูกสร้างจากสัญญาณเสมือนสัญญาณรบกวนด้วยอุปกรณ์ออปติคัลแอดด์/ดรอปฟิวเตอร์ หลังจากนั้นคีย์เข้าและถอดรหัสจะถูกสร้างขึ้นจากคีย์ลับด้วยอุปกรณ์ออปติคัลแอดด์/ดรอปฟิวเตอร์เช่นเดียวกัน สัญญาณเสมือนสัญญาณรบกวนถูกนำส่งไปยังผู้รับผ่านช่องส่งสัญญาณพิเศษเฉพาะ เมื่อผู้รับได้รับสัญญาณเสมือนสัญญาณรบกวนแล้วผู้รับจะทำการสร้างคีย์ลับ และคีย์เข้าและถอดรหัส ด้วยกระบวนการแบบเดียวกันกับผู้ส่ง เห็นได้ว่าผู้รับและผู้ส่งได้ทำการสร้างคีย์ลับ และคีย์เข้าและถอดรหัสขึ้นเอง โดยไม่ต้องทำการแลกเปลี่ยนคีย์ผ่านระบบสื่อสารข้อมูลแต่อย่างใด ทำให้คีย์ปลอดภัยจากผู้ดักจับสัญญาณสำหรับกระบวนการเข้าและถอดรหัสข้อมูล คีย์เข้ารหัสและคีย์ถอดรหัสถูกใช้โดยอุปกรณ์รวมสัญญาณแสงในฝั่งผู้ส่งและโดยอุปกรณ์แยกสัญญาณแสงในฝั่งผู้รับตามลำดับ

ผลจากการจำลองระบบรักษาความปลอดภัยให้กับการสื่อสารข้อมูลด้วยเส้นใยนำแสงที่เสนอด้วยคณิตศาสตร์ เห็นได้ว่าระบบที่เสนอดังกล่าวสามารถสร้างการสื่อสารข้อมูลที่มีความปลอดภัยสูง โดยข้อมูลสารสนเทศที่ถูกส่งผ่านระบบสื่อสารข้อมูลด้วยเส้นใยนำแสงที่มีความเร็วสูง จะถูกแปลงให้มีลักษณะคล้ายกับสัญญาณรบกวนทำให้ยากต่อการแปลความหมาย ระบบที่เสนอใช้เฉพาะอุปกรณ์ทางแสงขนาดเล็กเท่านั้น โดยไม่มีอุปกรณ์หรือวงจรอิเล็กทรอนิกส์ใด ๆ มาเกี่ยวข้อง

Thesis Title	Optical Cryptography Using PANDA Ring Resonator for Information Security
Student	Mr. Rattipong Putthacharoen
Student ID.	48060056
Degree	Doctor of Engineering
Program	Electrical Engineering
Year	2012
Thesis Advisor	Assoc. Prof. Dr. Somsak Mitatha
Thesis Co-Advisor	Assoc. Prof. Pratheep Bunyatnopparat

ABSTRACT

This thesis proposes the new optical cryptography system which uses the noiselike signal generated by the PANDA ring resonator to form the secure communication for the information security.

Firstly authors begin by presenting the study of related theoretical backgrounds such as dark and bright solitons, related optical devices, theories of the cryptography, noises and chaos-based communication. Then, the investigation of the dynamic behavior of the dark-bright soliton propagation and collision within the PANDA ring resonator is presented, followed by the designed optical cryptography system using purely compact optical devices is proposed. In this thesis, the authors use the combination of the noiselike signal, secret key and encryption-decryption keys for securing the communication. The noiselike signal is obtained from the dynamic states of the dark-bright soliton propagation and collision within the PANDA ring resonator, the secret key is derived from the noiselike signal which is obtained from the optical add/drop filter, and the encryption-decryption keys are derived later from the secret key which propagates through the add/drop filter too. The noiselike signal is sent to the receiver via the separate channel for a noise synchronization, and both the transmitter and receiver use the same noiselike signal to create the secret key. The secret key and encryption-decryption keys are not distributed over the optical network so they are safe from eavesdroppers. The encryption key is used by Optical Power Modulator for masking the information signals and the decryption key is used by Optical Power Demodulator for unmasking the received signals (ciphertext). The eavesdroppers without the valid decryption key cannot recover the original information signals.

Finally, mathematical simulations are conducted and their results have been shown that the proposed optical cryptography system can be used to form the "noiselike" communication for the information security over the high bandwidth optical network without any electronic control circuit is required.

ACKNOWLEDGEMENTS

First I would like to express a great thankfulness to my advisor ; Assoc. Prof. Dr. Somsak Mitatha for his attentions, suggestions, supports, and encouragements during this research, and for being available at anytime to response my questions, which have been valuable for my research.

I am profoundly grateful to my co-advisor, Assoc. Prof. Pratheep Bunyatnopparat, more than eleven years with him since M.Eng. degree until D.Eng. degree, he has never hesitated to help me at anytime, his helps in several ways have always been in my mind and it will be forever in my mind.

I am grateful to Prof. Dr. Preecha Yupapin for introducing me the research topic, thank you for his intelligent ideas and constant encouragement. Working with him has been a great learning experience for me. I would not find the way to complete my D.Eng. degree without his support.

I would like to thank every member of Hybrid Computing Research Laboratory (HCRL) - Faculty of Engineering and the Advanced Research Center of Photonic Laboratory (ARCP) - Faculty of Science for their cooperation and support, it was my great time to work with them and I am so proud to be a part of this excellent team.

I would also like to thank my boss, my colleagues and my company that encourage me to complete my dream.

Last but not least, my thanks go to my family, I would like to say thank you dad and mum for your patient, support and encouragement over my life, I know it is terrible for both of you to push me up, thank you my wife for love, thank you my son for giving me the enormous power, and thank you sister, brother and brother in law for all the supports during my study. Now I can make it, I wish this is the most happiness that I can give to all of you, I hope you will be proud of me.

Rattipong Putthacharoen

CONTENTS

CONTENTS

CONTENTS (cont.)

CONTENTS (cont.)

LIST OF FIGURES

Figures

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 Motivation

The amount of information transmitted over optical networks has seen an enormous surge over the last decade. This process is likely to continue considering the demand for a greater variety of services and a faster user experience. One central issue of modern optical communication is its security. The main issue is how to conceal the content of messages transmitted through insecure channels to unauthorized users or transmitted through insecure channels to unauthorized uses or in other words, to guarantee privacy and confidentiality in the communication.

Noiselike and Chaos-based communications have entered the scene and have become popular, evolving from a theoretical concept and an experimental demonstration to an almost ready-to-use technique where successful field experiments have been reported [1-4]. The chaos-based communication takes the advantage of the complex behavior of chaotic dynamical systems to "hide" or "mask" information called chaos-based cryptography. Then, a system similar to (or inverse of) the transmitter is necessary at the authorized receiver to recover the message. Privacy relies on the difficulty to recover the message without the appropriate receiver. Many different implementations of this basic idea have been proposed in the open literatures. An overview of the different methods presented so far can be found in the literatures, but many of them are still complex and involved many components, so the search for the simple and compact system still remains.

1.2 Goal of this thesis

Over the past decade, optical devices have become increasingly important as integrated components for advanced optical technology and have been widely used as optical sensor [5], signal processing [6], optical communication [7], and secured communication [8-10]. To overcome the more compact device, the micro and nano devices are suggested to form the new era of micro and nano communications, where recently, a small optical device known as a microring resonator in the form of an optical add/drop filter [11-13] has been recommended and shown that the transmitted signals over the optical networks can be suppressed with the noiselike signals which later can form the secure communication, and it can be possible to be fabricated [14]. In addition,

the use of a PANDA ring resonator has been reported [15,16], in which the investigation of such a device has shown the interesting results [17]. One of the interesting aspects is the dynamic behavior of the dark-bright soliton propagation and collision within the PANDA ring resonator, in which such dynamic behavior can be possibly used to form the noiselike signal for the secure communication.

The primary goal of this thesis is to propose the optical cryptography system which primarily applies the noiselike signal obtained from the dynamic behavior of the dark-bright soliton propagation and collision within the PANDA ring resonator to secure the optical communication. Secondarily the proposed system must have the ability to keep the security keys secretly away from the eavesdroppers. Finally the proposed system is realized using only compact optical devices, it is also expected to assist in relieving the optical network from undesirable latencies caused by processing related to Optical to Electrical (O/E) and Electrical to Optical (E/O) conversion, in which all the encryption and decryption processes are performed all optically so that the high security communication can be successfully formed without any electronic control circuit is required.

1.3 Scope of work

The scope of this thesis is defined and shown as follows, anything else that is not mentioned in the below scope of work is out of scope which is not included in this thesis.

1. The necessary theories such as the soliton, nonlinear optics, related optical devices, cryptography, noises, and chaos-based communication are studied.

2. The dynamic behavior of the dark-bright soliton propagation and collision within the PANDA ring resonator is investigated.

3. The noiselike signal must be obtained from the PANDA ring resonator and applied for the secure communication.

4. The new optical cryptography system is designed and proposed. Only the compact optical devices are used in the design. The detail of the proposed system must be described.

5. The mathematical simulations are conducted, and the simulation results must be presented in detail.

1.4 Expected results

1. Necessary theories and mathematical backgrounds of the soliton, nonlinear

optics, related optical devices, cryptography, noises, and chaos-based communication are understood.

2. The cryptography, noises, and chaos-based communication are understood.

3. The dynamic behavior of the dark-bright soliton propagation and collision within the PANDA ring resonator can be used to form the noiselike signal.

4. The secure communication in the form of the "noiselike" communication can be formed between the transmitter and receiver.

5. The proposed system has the ability to keep the security keys secretly from the eavesdroppers.

6. The original information signal must be recovered correctly by the receiver.

7. The compact optical devices are only used in the design without the electronic control circuit is required.

CHAPTER 2
LITERATURE REVIEW

2.1 The history of Chaos Theory

The word 'chaos' generally refers to a phenomenon that is disordered and irregular. In modern scientific terminology, however, 'chaos' refers to a pseudo-random phenomenon generated in a deterministic system [18].

Henri Poincaré is acknowledged as the first person to glimpse the possibility of chaos. Poincaré discovered what is today known as homoclinic trajectories in the state space. He studied the stability properties of the solar system at the end of the 19^{th} century, and found that even in the case of three masses moving under Newton's law of attraction they could still show very complex behavior [19]. This kind of motion depends sensitively on the initial conditions, thereby rendering long-term prediction is impossible [20].

In 1927, Van der Pol and Van der Mark studied the behavior of a neonbulb RC oscillator driven by a sinusoidal voltage source [21]. They found that by increasing the capacitance in the circuit, sudden jumps from the drive frequency. These frequency jumps were observed and found that this process of frequency demultiplication eventually led to irregular noise. In fact, what they found, caused by bifurcations and chaos.

Birkhoff developed the methods discovered by Poincaré and found many different types of long-term limiting behaviors, such as ω-*limit set* and α-*limit set*. The term 'dynamical system' comes from his work [22] but the chaos has always been in the background. Birkhoff also discovered what he termed remarkable curves or thick curves which later these turned out to be a chaotic attractor of a discrete-time system. Birkoff proved his famous Ergodic Theorem in 1931 [23].

In the 1950s, Cartwright, Littlewood, and Levinson showed that a certain forced nonlinear oscillator had an infinite number of different periods. Smale extended the result of Cartwright, Littlewood, and Levinson in a general framework and illustrated the phenomenon with his 'horseshoe' mapping [24]. Meanwhile in a separate development, Poincaré's geometric methods were extended to yield a much deeper understanding of celestial mechanics. One of the most important mathematical achievements, the KAM theorem, named by taking the first letters of Kolmogorov, Arnol'd, and Moser, was proved in 1963. This theorem tells us that a Hamiltonian system will still be Hamiltonian

when it is subjected to tiny perturbations, which gives an answer that the solar system is stable in some degree. This theorem also implies that in energy preservation system complicated behavior would still arise.

Prior to Smale, E. Lorenz, an American meteorologist, rnade an important contribution in 1963 when he used a computer to study a group of ordinary differential equations. These equations were reduced from the partial differential equation which described the turbulent motion of the atmosphere. Lorenz found that a small change in initial conditions led to very different outcomes in a relatively short time; this property is called *sensitive dependence on initial conditions*. This is really a great discovery since almost all traditional scientists at that time believed that two trajectories emitted from close initial points would always be close when time evolves. Laplace's famous assertion is an extreme reflection of this idea: if there is an omnipotent spirit who can distinguish any tiny difference of initial conditions and can discriminate all the forces in the universe, then he can know all the history and all the future about everything in the universe. From the uncertainty principle in quantum mechanics we know that one can not exactly determine the position and velocity of a particle at the same time. This means that if a system has the property of sensitive dependence on initial conditions, then one cannot predict its long-term behavior since we cannot avoid the error of measurement on the initial conditions. Lorenz used the phrase 'butterfly effect' to refer to the phenomenon means that butterfly flapping its wings in Australia today could affect the weather in the United States a month later. It was not until the 1970s that Lorenz's work became known to the more theoretical mathematical community.

The 1970s were the boom years for chaos. In 1971 Ruelle and Takens proposed a new theory for the onset of turbulence in fluids, based on abstract considerations about strange attractors [25]. The word 'chaos' was first introduced by T. Y. Li and J. Yorke in 1975 [26] to designate systems that have aperiodic behavior more complicated than *equilibrium, periodic, or quasiperodic* motion. But, in fact, their work is a special case of the theorem obtained by Sharkovskii in 1964 [27], which, because of political reasons, was not known by western mathematicians for a long time. In 1976, May showed how chaos arises in iterated mappings in population dynamics, and wrote an influential review article that stressed the pedagogical importance of studying simple nonlinear systems, to counterbalance the often misleading linear intuition fostered by traditional education [28]. Next came the most surprising discovery of all, from the physicist Feigenbaum. He discovered that there are certain universal laws governing the transition from regular to chaotic behavior; roughly speaking, completely different

systems can go chaotic in the same way. His work established a link between chaos and phase transitions, and enticed a generation of physicists to the study of dynamics.

Entering into the 1980s, computers become a powerful tool, used to help researchers visualized the complicated structures of strange attractors, calculate characteristic indices of the chaotic systems, and provide evidence required by proofs [29,30]. Mandelbrot constructed the theory of fractal geometry at the end of the 1970s, and drew the first picture of a Mandelbrot set [31]. The theory of fractal geometry generalizes the notion of dimension from integers to real numbers and has become a powerful tool for characterizing the complicated structures of strange attractors. From the middle of the 1980s, more and more researchers have paid attention to how to control chaos, including suppression, synchronization, and chaotification.

Ott, Grebogi and Yorke, in 1990 [32], presented a method for controlling unstable trajectories embedded in a chaotic attractor. At the same time, there was another course of events leading to the field of chaos. This was the study of nonintegrable Hamiltomian systems in classical mechanics. Research in this field has led to the formulation and proof of the KAM theorem in the early 1960's. Numerical studies have shown that when the conditions stated by the KAM theorem fail, then stochastic behavior is exhibited by nonintegrable Hamiltonian systems.

Today, chaos has been discovered in bio-systems, meteorology, cosmology, economics, population dynamics, chemistry, physics, mechanical and electrical engineering, optical communication, and many other areas. The research direction has been transferring from finding the evidence of chaos existence into applications and deep theoretical study.

2.2 Chaotic Cryptography

Gilles Millérioux et al. [33] studied a connection between chaotic and conventional encryption in his paper, and presented amounts to scrambling a message with a chaotic dynamic which are very useful for our research.

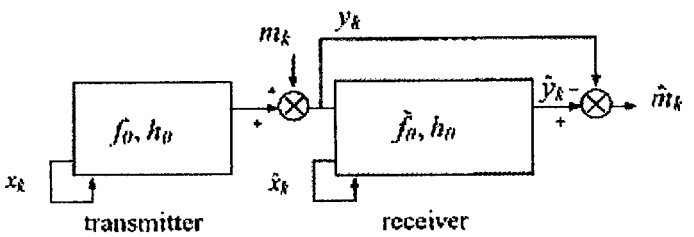

Fig. 2.1 Additive masking.

Various cryptosystems [34], corresponding to distinct ways of hiding a message, have drawn the attention of the researchers over the years. The most important schemes obeying such a principle are additive masking, chaotic switching, discrete or continuous parameter modulation, two-channel transmission, and message embedding. Additive masking was first suggested in [35] and [36]. Chaotic switching is also referred to as chaotic modulation or chaos shift keying. Such a technique has been mostly proposed in the digital communications context. A description with deep insights can be found in [37], even though the method was proposed a couple of years before, say, in 1993 [38]. Basically, two kinds of parameter modulations can be distinguished: the discrete [38,39] and the continuous one [40-43]. The two-channel transmission has been proposed, for example, in [44,45]. The message-embedded technique is given different names in the literature: embedding [46,47], nonautonomous modulation [48] or direct chaotic modulation [49]. A slightly different method derived from the message embedding is the hybrid message embedding. It was first proposed in [50] but the terminology "hybrid" terminology has been really introduced in [51].

Three relevant chaotic cryptosystems have been selected for their study: the additive masking, the message embedding and the hybrid message embedding. For those three cryptosystems, the chaotic dynamics are specified by a state representation with corresponding state vector x_k, the dimension of the system being n. Only a part of the state vector x_k, called the "output" and denoted by y_k , obtained via an output function is conveyed through the public channel. y_k is usually of low dimension and should be unidimensional in the ideal case. In what follows, the authors assume that y_k is a scalar (dimension 1), the transmitter being thus restricted to a so-called single-input single-output (SISO) system. The nonlinear function describing the chaotic dynamics as well as the output function are both parameterized by a vector θ which is intended to act as the secret key

2.2.1 Additive Masking

For the additive masking (Fig. 2.1), the information $m_k$to be hidden is merely added to the output y_k of the *transmitter*

$$\begin{cases} x_{k+1} = f_\theta(x_k) \\ y_k = h_\theta(x_k) + m_k \end{cases} \tag{2.1}$$

The generic equations of the *receiver* read

$$\begin{cases} \hat{x}_{k+1} = \tilde{f}_\theta(\hat{x}_k, y_k) \\ \hat{y}_k = h_\theta(\hat{x}_k) \end{cases} \tag{2.2}$$

The quantity $y_k$which appears in Eq.(2.2) reveals a unidirectional coupling between both the transmitter and the receiver systems. Retrieving the message m_k is

performed in two steps. The first step is called *synchronization*. It is based on a suitable choice of $\tilde{f}$ so that

$$\forall \hat{x}_0 \in U, \lim_{k\to\infty} \|Tx_k - \hat{x}_k\| = 0 \tag{2.3}$$

or

$$\exists k_f < \infty \, \forall \hat{x}_0 \in U \; and \; \forall k \geq k_f, \|Tx_k - \hat{x}_k\| = 0 \tag{2.4}$$

Where T is a constant matrix of appropriate dimension and U is a nonempty set of initial conditions. Eq.(2.3) corresponds to an asymptotic synchronization, while Eq.(2.4) corresponds to a finite time synchronization. As a matter of fact, synchronization can be viewed as a state reconstruction and in 1997, several papers [52-55] brought out this connection. The receiver often consists in an observer. If only a part of the components are reconstructed, the observer is a reduced observer and rank $(T) < n$. If all the components of the state vector are reconstructed, the observer is a full observer and T is the identity matrix.

The second step comprises the estimation of $m_k$through a suitable static function which depends on the internal state $\hat{x}_k$and the output y_k. Provided that synchronization Eq.(2.3) or Eq.(2.4) can be achieved, the recovering of the information is performed by $\hat{m}_k = y_k - \hat{y}_k$.

Unfortunately, the information cannot be exactly retrieved. Indeed, m_k acts as a channel disturbance and precludes the *receiver* from being exactly synchronized; neither Eq.(2.3) nor Eq.(2.4) can be exactly fulfilled. As a result, $\hat{x}_k \neq x_k$, $\hat{y}_k \neq y_k$ and, finally, $\hat{m}_k \neq m_k$for any k.

2.2.2 Message Embedding

For the message embedding (Fig. 2.2), at the transmitter part, the information m_k is directly injected (or, as it is also usually said, embedded) in a chaotic dynamic f_θ. The resulting system turns into a nonautonomous one since the information acts as an exogenous input. Injecting m_k into the dynamic can be considered as a "modulation" of the phase space. Only the output y_k of the system is transmitted. Two classes are considered. The first one corresponds to systems governed by the state equations.

$$\begin{cases} x_{k+1} = f_\theta(x_k, m_k) \\ y_k = h_\theta(x_k, m_k) \end{cases} \tag{2.5}$$

while the second class corresponds to

$$\begin{cases} x_{k+1} = f_\theta(x_k, m_k) \\ y_k = h'_\theta(x_k) \end{cases} \tag{2.6}$$

The systems Eq.(2.5) and Eq.(2.6) differ from each other by their *relative degree*.

Definition 1 [56] : The relative degree of a system with respect to the quantity m_k is the required number r of iterations of the output y_k so as y_{k+r} depends on $m_k$which actually appears explicitly in the expression of y_{k+r}.

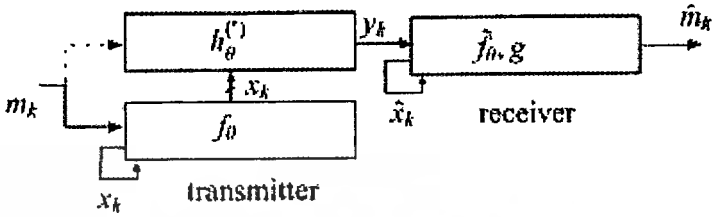

Fig. 2.2 Message embedding. When $r = 0, m_k$ is embedded into f_θ and h_θ. When $r > 0, m_k$ is only embedded into f_θ . The output function is h_θ or h'_θ according to the relative degree.

Remark 1: For Single-Input Single-Output (SISO) linear systems, the relative degree r corresponds to the difference between the degree of the denominator and the degree of the numerator in their transfer function.

Based on Definition 1, the relative degree of the systems Eq.(2.5) is clearly $r = 0$.

On the other hand, system Eq.(2.6) has a relative degree r strictly greater than 0. If the authors assume that is finite and constant (no time varying), after iterating r times the state vector x_k, the output y_{k+r} reads

$$y_{k+r} = h'_\theta(f_\theta^r(x_k, m_k)) \tag{2.7}$$

where

$$f_\theta^i(x_k, m_k) = x_k \; when \; i = 0$$
$$= f_\theta\left(f_\theta^{i-1}(x_k, m_k), m_{k+i-1}\right) \; \forall i \geq 1$$

and where m_k appears explicitly, that is for a given x_k, there exists $m'_k \neq m_k$ such that $y_{k+r} = h'_\theta(f_\theta^r(x_k, m_k)) \neq h'_\theta(f_\theta^r(x_k, m'_k))$ whereas for all $m'_k \neq m_k, y_{k+r'} = h'_\theta\left(f_\theta^{r'}(x_k, m_k)\right) = h'_\theta\left(f_\theta^{r'}(x_k, m'_k)\right) \; if \; r' < r$.

Two mechanisms have been proposed in the literature for the recovering of m_k : the inverse system approach [57] and the unknown input observer approach [58–63]. The transmitter exhibits an output behavior that depends both on the internal chaotic state vector $x_k$and on the input signal m_k. The role of the receiver is to reproduce the input m_k given the only available data y_k (and possibly their iterates). Hence, it really acts as an inverse system. A main problem arising in the inverse approach lies in that the inverse system is likely to have bad performance properties in a noisy context. In such a case, this drawback must be redressed and a refinement of the design is needed. This leads naturally to some structures named unknown input observers (UIOs).

The generic equations governing an inverse system or an UIO for Eq.(2.5) [or Eq.(2.6)] are

$$\begin{cases} \hat{x}_{k+r+1} = \tilde{f}_\theta(\hat{x}_{k+r}, y_k, \dots, y_{k+r}) \\ \hat{m}_{k+r} = g(\hat{x}_{k+r}, y_k, \dots, y_{k+r}) \end{cases} \tag{2.8}$$

with g such that

$$\hat{m}_{k+r} = g(\hat{x}_{k+r}, y_k, \dots, y_{k+r}) = m_k \; when \; \hat{x}_{k+r} = x_k \tag{2.9}$$

A delay equal to the relative degree r must be introduced for causality sake. The existence of an inverse system or an UIO is guaranteed under the assumption that the system Eq.(2.5) (or Eq.(2.6)) is left invertible. Looking into left invertibility is out of the scope. Hereafter, the authors assume that these conditions are fulfilled.

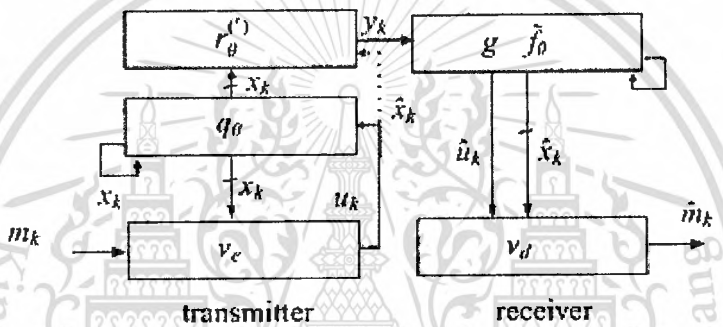

Fig. 2.3 Hybrid message embedding. The output function is r or r' according to the relative degree.

The functions $\tilde{f}_\theta$ and g must be chosen so as a so-called *synchronization* with unknown input can be ensured, that is

$$\forall \hat{x}_0 \in U \; and \; \forall m_k, \lim_{k\to\infty} \|x_k - \hat{x}_{k+r}\| = 0 \tag{2.10}$$

Or

$$\exists k_f < \infty \; \forall \hat{x}_0 \in U \; \forall m_k \; and \; \forall k \geq k_f, \|x_k - \hat{x}_{k+r}\| = 0 \tag{2.11}$$

Where U is a nonempty set of initial conditions. Eq.(2.10) corresponds to an asymptotic synchronization with unknown input, while Eq.(2.11) corresponds to a finite time synchronization with unknown input.

The message embedding is very attractive insofar as the synchronization Eq.(2.3) or Eq.(2.4) can be guaranteed without any restriction on the rate of variation of m_k.

2.2.3 Hybrid Message Embedding

For the hybrid message-embedded technique (Fig. 2.3), the authors also distinguished two different setups. The first one corresponds to a transmitter system having a relative degree $r = 0$ with respect to u_k

$$\begin{cases} x_{k+1} = q_\theta(x_k, u_k) \\ y_k = r_\theta(x_k, u_k) \\ u_k = v_e(x_k, m_k) \end{cases} \quad (2.12)$$

while the second class corresponds to systems having relative degree $r > 0$ with respect to u_k

$$\begin{cases} x_{k+1} = q_\theta(x_k, u_k) \\ y_k = r'_\theta(x_k) \\ u_k = v_e(x_k, m_k) \end{cases} \quad (2.13)$$

Similar to what happened with the message embedding technique when the relative degree r is strictly greater than zero, the authors assumed that the relative degree r is finite and constant (no time-varying), after iterating r times the state vector in Eq.(2.13), the output y_{k+r} reads

$$y_{k+r} = r'_\theta(q^r_\theta(x_k, u_k)) \quad (2.14)$$

Where

$$q^i_\theta(x_k, u_k) = x_k when\ i = 0$$
$$= q_\theta(q^{i-1}_\theta(x_k, u_k), u_{k+i-1})\ \forall i \geq 1$$

and where u_k appears explicitly, that is for a given x_k , there exists $u'_k \neq u_k$ such that $y_{k+r} = r'_\theta(q^r_\theta(x_k, u_k)) \neq r'_\theta(q^r_\theta(x_k, u'_k))$ whereas for all $u'_k \neq u_k, y_{k+r'} = r'_\theta\left(q^{r'}_\theta(x_k, u_k)\right) = r'_\theta\left(q^{r'}_\theta(x_k, u'_k)\right) if\ r' < r$.

For both schemes, the plaintext m_k is "preciphered" according to a function v_e which delivers the quantity u_k. Actually, it's a simple matter to notice that such a scheme is nothing but a message embedding scheme. However, it corresponds to a special decomposition of the dynamics f (and subsidiary of the output function h): the function q_θ on one hand and the function v_e on the other hand. Such a decomposition may be useful to highlight the hybrid aspect of f when this function combines boolean and arithmetic operations as suggested by [64] to significantly improve the resistance to attacks of ciphering primitives. It turns out that the decomposition makes the design of the receiver much more easier.

Similarly to the message-embedding technique, the *receiver* is an inverse system or an unknown input observer of the form

$$\begin{cases} \hat{x}_{k+r+1} = \tilde{f}_\theta(\hat{x}_{k+r}, y_k, \cdots, y_{k+r}) \\ \hat{u}_{k+r} = g_\theta(\hat{x}_{k+r}, y_k, \cdots, y_{k+r}) \\ \hat{m}_{k+r} = v_d(\hat{x}_{k+r}, \hat{u}_{k+r}) \end{cases} \quad (2.15)$$

with such g that

$$\hat{u}_{k+r} = g_{\tilde{\theta}}(\hat{x}_{k+r}, y_k, \cdots, y_{k+r}) = u_k when\ \hat{x}_{k+r} = x_k \quad (2.16)$$

and with v_d such that

$$\hat{m}_k = v_d(\hat{x}_k, \hat{u}_k) = m_k\ when\ \hat{x}_k = x_k\ and\ \hat{u}_k = u_k \quad (2.17)$$

The delay r is again introduced for causality sake. In other words, the *receiver* system is designed in such a way that both u_k and $x_k$can be recovered, given the only available data $y_k$and its subsequent iterates. Once u_k is recovered, the plaintext m_k is correctly extracted by applying the decryption function v_d. The existence of an inverse system or an UIO is guaranteed under the assumption that the system Eq.(2.12) (or Eq.(2.13)) is left invertible.

2.3 Dynamic modulated Gaussian pulse propagation within the double PANDA ring resonator system

Uomwech, Sarapat, and Yupapin [65] proposed the interesting results of light pulse propagation within a double PANDA ring resonator system as shown in Fig. 2.4. The authors used the technique of finite difference time domain that was implemented by the scientific programming method known as OPTI-WAVE PROGRAMMING to simulate and analyze the dynamic waveforms of propagating light pulse within the designed system. By using the input Gaussian pulse with center wavelength at 1550 nm and the other practical parameters, results obtained have shown that the multiwavelength light sources can be generated and achieved, and the dynamic behaviors of light pulses propagating within the system can be seen.

The use of Gaussian pulse has reported the interesting results of light pulse propagating within a nonlinear media [66,67]. In this work, the authors found that the broad spectrum of light pulse can be transformed to the discrete pulses. Moreover, Gaussian pulse can be amplified and enhanced by the nonlinear effect of the double PANDA ring resonator system.

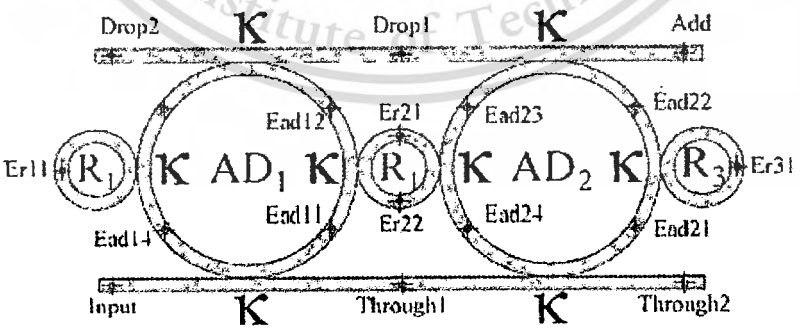

Fig. 2.4 A schematic of a double PANDA ring resonators where Ads are add/drop filter.

A schematic diagram of the double PANDA ring resonator system for dynamic pulse generation is designed and shown in Fig. 2.4 .The modulated Gaussian continuous wave (CW) with center wavelength (λ_0) at 1.55 μm, peak power at 50 mW is input into the system. The combination between the input and reflected light output can be seen as shown in Fig. 2.5. The suitable ring parameters are used to make the system associated with the practical device [68,69], the material type is InGaAsP/InP.

Ead is the pulse propagation in the add/drop device and Er is the pulse propagation in the nanoring resonator as illustrated in Fig. 2.4 The required output signals are obtained and seen at the drop and through ports. Fig. 2.5–2.8 show the results in the different points in the double PANDA ring resonator system. The maximum power of 120 mW is obtained as shown in Fig. 2.6(b), whereas the maximum number of peaks obtained is 18 peaks as illustrated in Fig. 2.8(b).

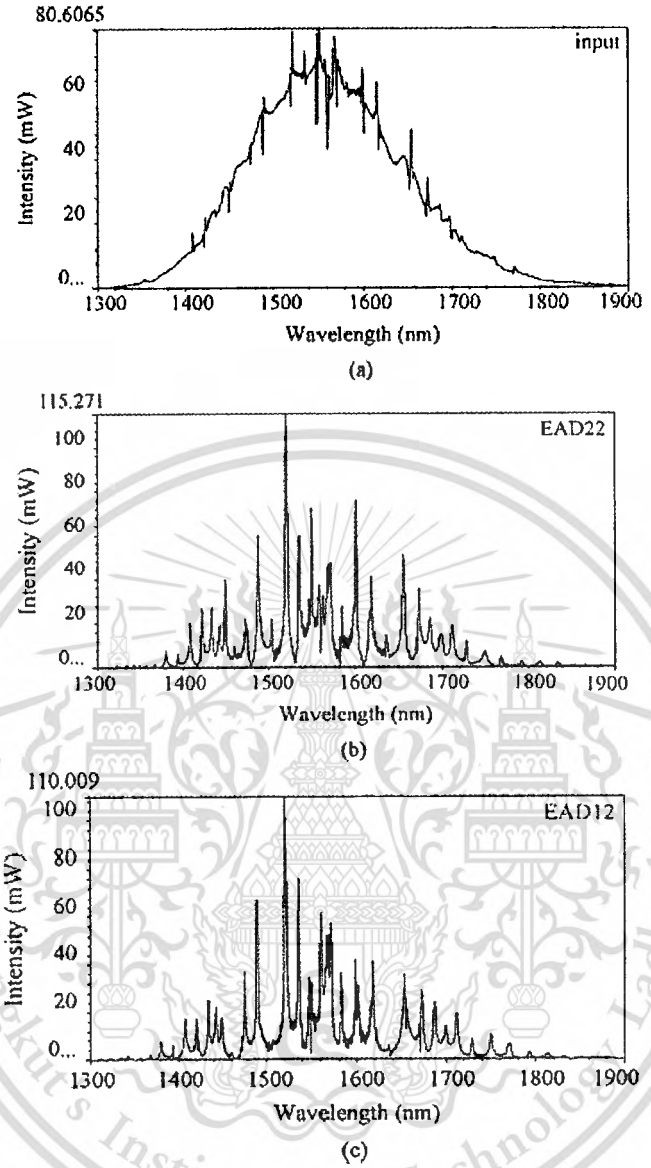

Fig. 2.5 Results of the output light intensity and wavelength at the certain locations, (a) an input pulse, (b) EAD22: Ead 22, and (c) EAD12: Ead12.

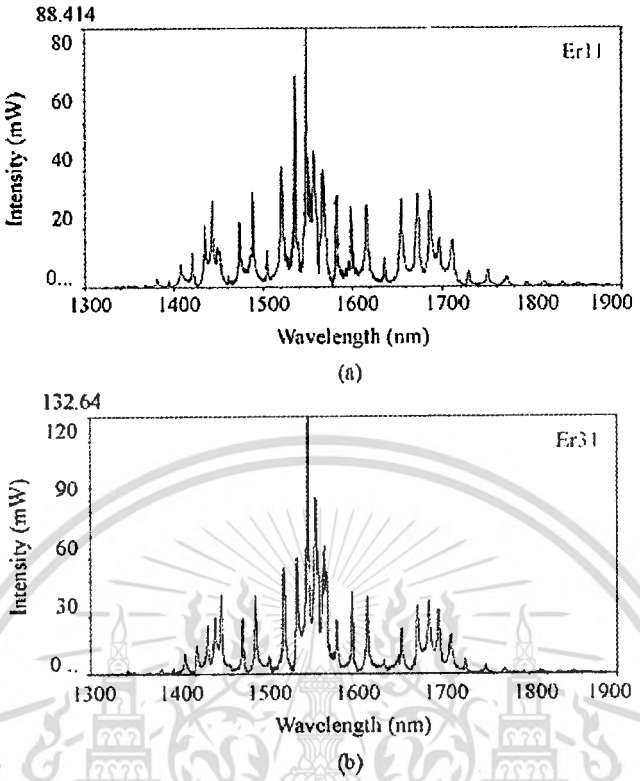

Fig. 2.6 Results of the output light intensity and wavelength at the certain locations, (a) Er11 and (b) Er31.

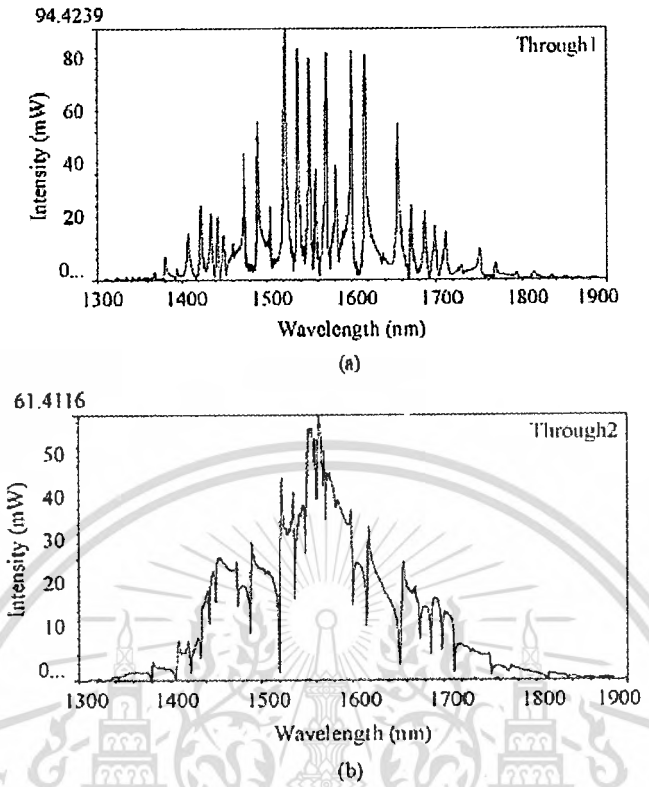

Fig. 2.7 Results of the output light intensity and wavelength at the certain locations, (a) Through 1 and (b) Through 2.

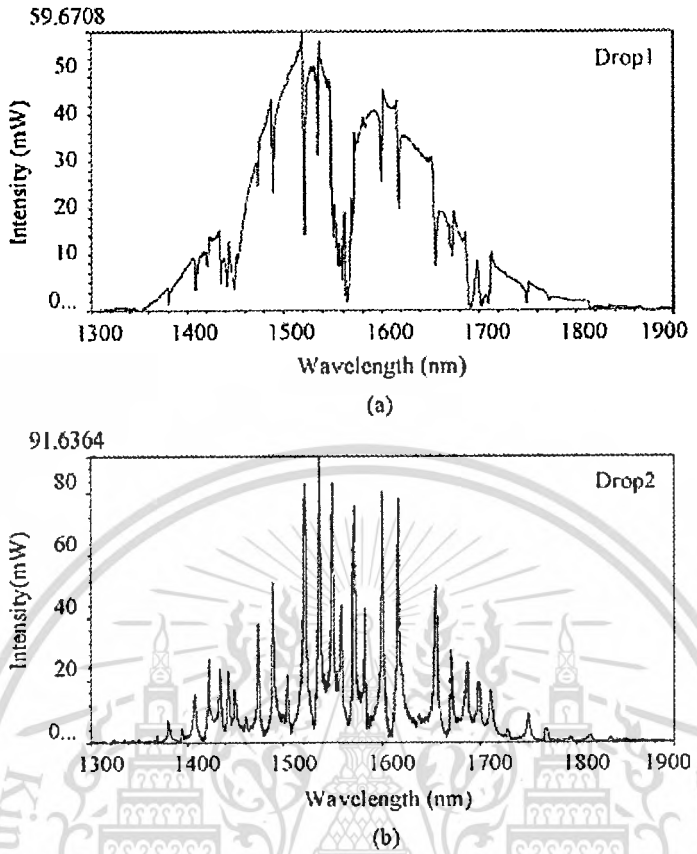

Fig. 2.8 Results of the output light intensity and wavelength at the certain locations, (a) Drop 1 and (b) Drop 2.

The authors have shown the dynamic behaviors of pulses propagation within the double PANDA ring resonators (nanoring resonators in conjunction with two add/drop filters). By using the OPTI-WAVE PROGRAMMING and the reasonable input parameters, the dynamic behaviors can be controlled, and the required output pulses can be obtained. In this case, the dynamic behavior can be controlled and used for the desired applications. The maximum number of peaks (counts) obtained is 18 peaks, which are available for multi light source or wavelength enhancement application; moreover, the output amplification is also obtained where the maximum power within the nanoring of 120 mW is obtained.

2.4 Public key suppression and recovery using a PANDA ring resonator for high security communication

Pakorn et al. [70] proposed an interesting security technique that applies a dynamic state of the dark-bright soliton propagation and collision within the PANDA ring resonator to form a cryptography system. The obtained output of the cryptography system is the digital public key which can be used for high security communication. In the paper, they propose the cryptography system that consists of the public key suppression and recovery modules. The sender has both public key suppression and recovery modules, the receiver has only the recovery module. The public key suppression module is responsible for generating the noisy signal, and the public key recovery module is responsible for extracting the digital public key from the noisy signal. The information can be later encrypted and decrypted by using the digital public key. The proposed cryptography system only uses the optical devices (PANDA ring resonator and microring resonator) to generate the digital public key without the electrical circuit is needed.

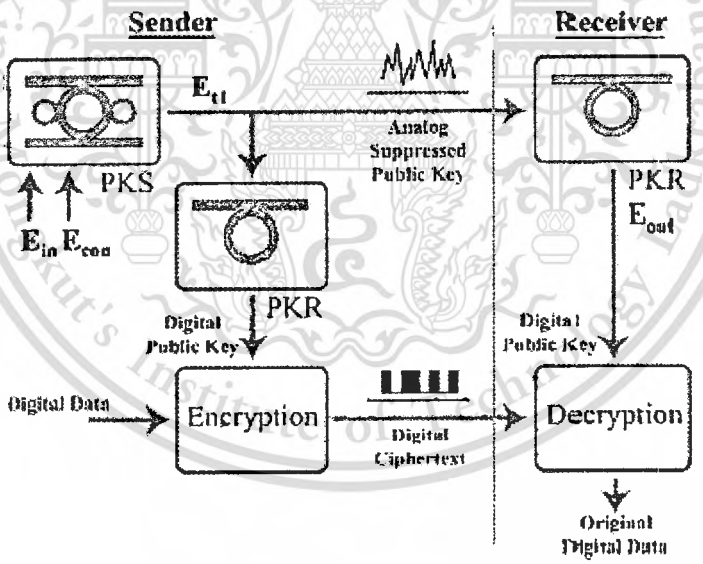

Fig. 2.9 Schematic diagram of the Public Key Cryptography system.

In operation, Fig. 2.9 shows the schematic diagram of the cryptography system where PKS is the public key suppression module and PKR is the public key recovery module. The transmitter (sender) part consists of the public key suppression, public key recovery and encryption modules, and the receiver part consists of the public key

recovery and decryption modules. The public key suppression module consists of one PANDA ring resonator, the bright soliton light pulse (E_{in}) and dark soliton light pulse (E_{con}) are input into the input and control ports of the PANDA ring resonator, respectively. The output signal obtained is the analog suppressed public key (E_{t1}) which is then sent to the public key recovery module of the transmitter itself and the receiver. The public key recovery module consists of one microring resonator, this module performs the digital public key generation for the transmitter and receiver. The suppressed public key is input into the input port of the microring resonator, then the digital public key is obtained at the output port (E_{out}). The transmitter uses the digital public key to encrypt the digital data at the encryption module where the ciphertext is later generated, and the receiver uses the digital public key to decrypt the ciphertext at the decryption module.

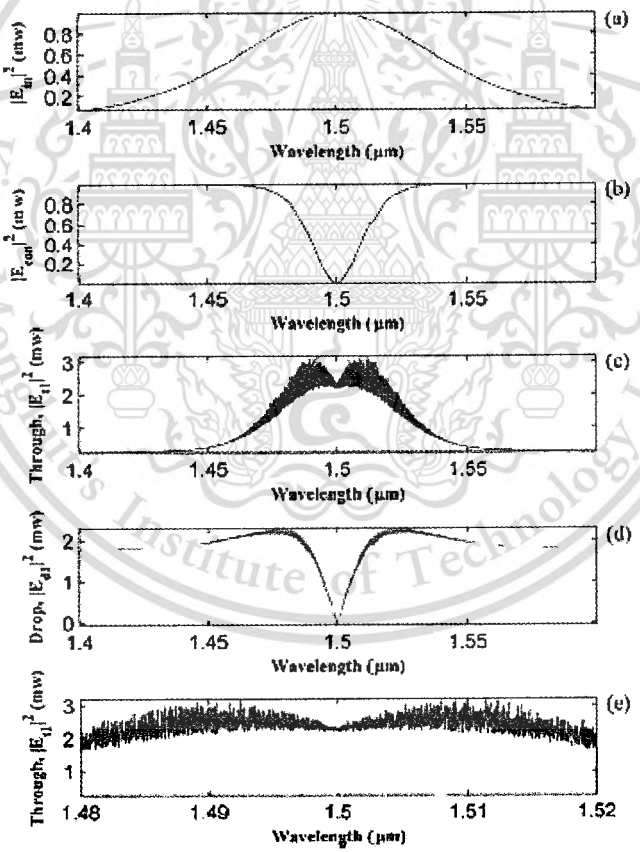

Fig. 2.10 Simulation result of the public key suppression.

Fig. 2.10 shows the simulation result of the public key suppression module at the center wavelength λ_0 = 1.50 μm. Fig. 2.10(a) shows the bright soliton light pulse at the

input port $|E_{in}|^2$ of the public key suppression module which the bright soliton light pulse with 1 mW peak power is input into the input port. Fig. 2.10(b) shows the dark soliton light pulse $|E_{con}|^2$ with 1 mW peak power at the control port. The output power at the drop port $|E_{d1}|^2$ is shown in Fig. 2.10(d). And Fig. 2.10(c) and 2.10(e) show the output power at the through port $|E_{t1}|^2$ of the public key suppression module which would be transmitted then to the public key recovery modules. We have observed that the peak power at the through and drop ports are 3.2 and 2.3 mW, respectively. They are larger than the input light pulses due to the optical nonlinear effects.

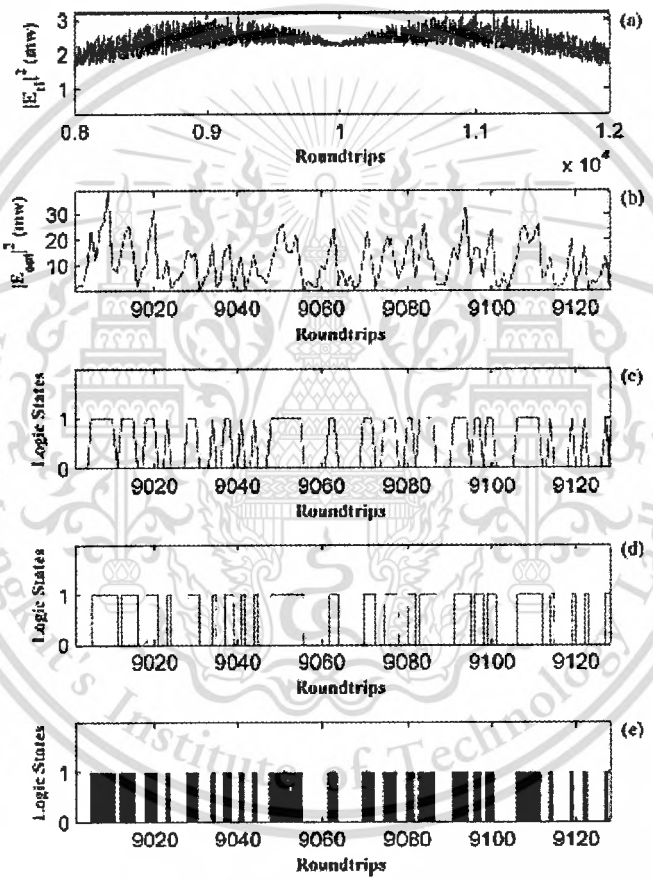

Fig. 2.11 Simulation results of the public key recovery module.

Fig. 2.11 shows the simulation result of the public key recovery module at the center wavelength λ0 = 1.50 μm. Fig. 2.11(a) is the suppressed public key generated from the public key suppression module. We have seen that the suppressed public key signal looks like the noise signal which has high randomness. Fig. 2.11(b) shows the output power of the public key recovery module at roundtrip 9001 to 9128. Fig. 2.11(c)–

2.11(e) show the results of the conversion from the analog public key to the digital public key. Fig. 2.11(c) shows the clipping signals and Fig. 2.11(d) shows the clipping signals after performing the least-squares method. Finally, the digital public key is obtained as shown in Fig. 2.11(e) "0000111111011110011100100001110001001100100100011111111000000110000000111001110011011110000111101101100000011111100100001001000010" which can later be used in the traditional digital cryptography system.

In summary, the cryptography system proposed by Pakorn extracts the digital public key from the noisy signal obtained from the PANDA ring resonator.

CHAPTER 3
THEORETICAL BACKGROUND

3.1 Nonlinear optics and Optical Kerr effect

Nonlinear optic is the study of optics that describes the behavior of light in nonlinear media. This nonlinearity is typically only observed at very high light intensities (typically 10^8 V/m) such as those provided by pulsed lasers. Another wide area is concerned with the effects of optical nonlinearities in various situations, e.g. for the propagation of intense ultrashort pulses in optical fibers, optical signal processing, secure communication and etc.

The Kerr effect is a change in the refractive index of a material in response to an applied electric field. The Kerr effect is generated in the nonlinear media which itself modifies the propagation properties of the light. This effect only becomes significant with very intense beams such as those from lasers. Many materials show a Kerr effect, but certain liquids display it more strongly than others. The Kerr effect is the effect of an instantaneously occurring nonlinear response, which can be described as modifying the refractive index. In particular, the refractive index for the high intensity light beam itself is modified according to

$$n = n_0 + n_2 I \tag{3.1}$$

Where n is the total refractive index, n_0 is the linear refractive index, n_2 is the nonlinear refractive index, and I is the intensity of the wave. The refractive index change is thus proportional to the intensity of the light travelling through the medium.

The values of n_2 are relatively small for most materials, on the order of 10^{-20} m^2/W for typical glasses. Therefore beam intensities (irradiances) on the order of 1 $GWcm^{-2}$ (such as those produced by lasers) are necessary to produce significant variations in refractive index via the Kerr effect.

The optical Kerr effect manifests itself temporally as self-phase modulation, a self-induced phase- and frequency-shift of a pulse of light as it travels through a medium. This process, along with dispersion, can produce optical solitons.

3.2 Optical soliton (dark and bright solitons)

Soliton optic is the optical field that does not change during propagation because of a delicate [71] balance between nonlinear and linear effects in the medium. There are two main kinds of the solitons:

Spatial solitons: the nonlinear effect can balance the diffraction. The electromagnetic field can change the refractive index of the medium while propagating, thus creating a structure similar to a graded-index fiber. If the field is also a propagating mode of the guide it has created, then it will remain confined and it will propagate without changing its shape

Temporal solitons: if the electromagnetic field is already spatially confined, it is possible to send pulses that will not change their shape because the nonlinear effects will balance the dispersion. Those solitons were discovered first and they are often simply referred as "solitons" in optics.

3.2.1 Temporal solitons

The main problem that limits transmission bit rate in optical fibers is group velocity dispersion. It is because generated impulses have a non-zero bandwidth and the medium that they are propagating through has a refractive index that depends on frequency (or wavelength). This effect is represented by the group delay dispersion parameter D; using it, it is possible to calculate exactly how much the pulse will widen:

$$\Delta\tau \approx DL\Delta\lambda \tag{3.2}$$

where L is the length of the fiber and $\Delta\lambda$ is the bandwidth in terms of wavelength. The approach in modern communication systems is to balance such dispersion with other fibers having D with different signs in different parts of the fiber: this way the pulses keep on broadening and shrinking while are propagating. With temporal solitons it is possible to remove such a problem completely.

The Optical Kerr effect as mentioned in the section 3.1 leads to an integrable non linear Schrodinger equation both in space and time, which can essentially be used to describe the optical properties of the solitons. Optical solitons form when the total refractive index seen by a beam is

$$n = n_0 + n_2 I = n_0 + n_2\left(\frac{P}{A_{eff}}\right) \tag{3.3}$$

where n_0 and n_2 are the linear and nonlinear refractive indices, 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}.

As noted earlier it can be seen that the total refractive index of the medium increases as the amplitude increases. The Kerr effect introduces a Self-phase modulation that changes the refractive index according to the intensity.

3.2.2 The wave equations in nonlinear optics

In glass-fiber optics where large radiation power passes through very small cross-sections, the nonlinear effect occurs. We can describe that nonlinear effect by using the nonlinear Schrödinger equation, called Manakov system, which is a model of wave propagation in fiber optics. The function ψ represents a wave and the nonlinear Schrödinger equation describes the propagation of the wave through a nonlinear medium. The second-order derivative represents the dispersion, while the κ term represents the nonlinearity. The equation models many nonlinearity effects in a fiber including but not limited to self-phase modulation, four-wave mixing, second harmonic generation, stimulated Raman scattering, etc. The nonlinear Schrödinger equation is described by

$$i\frac{\partial \psi}{\partial t} = -\frac{1}{2}\frac{\partial^2 \psi}{\partial x^2} + \kappa|\psi|^2\psi \tag{3.4}$$

The solution of the equation is simple and it is the fundamental soliton:

Bright Solitons : $$E_{in}(t) = A\,sec\,h\left[\frac{T}{T_0}\right]exp\left[\left(\frac{z}{2L_D}\right) - i\omega_0 t\right] \tag{3.5}$$

Dark Solitons : $$E_{in}(t) = A\,tanh\left[\frac{T}{T_0}\right]exp\left[\left(\frac{z}{2L_D}\right) - i\omega_0 t\right] \tag{3.6}$$

where A and z are the optical field amplitude and propagation distance, respectively. T is a soliton pulse propagation time in a frame moving at the group velocity, $T = t - \beta_1.z$, where β_1 and β_2 are the dispersion coefficient of the linear and second-order terms of Taylor expansion of the propagation constant, respectively. $L_D = T_0^2 / |\beta_2|$ is the dispersion length of the soliton pulse. T_0 in equation is a soliton

pulse propagation time at initial input where t is the soliton phase shift time, and the frequency shift of the soliton is ω_0. This solution describes a pulse that keeps its temporal width in variance as it propagates, and thus is called a temporal soliton. When a soliton peak intensity $\left(\left|\beta_2 / \Gamma T_0^2\right|\right)$ is given, then T_0 is known. For the soliton pulse in the microring device, a balance should be achieved between the dispersion length (L_D) and the nonlinear length $L_{NL} = 1/\Gamma\phi_{NL}$), where $\Gamma = n_2 k_n$,is the length scale over which dispersive or nonlinear effects makes the beam become wider or narrower. For a soliton pulse, there is a balance between dispersion and nonlinear lengths, hence $L_D = L_{NL}$.

3.3 The Ring Resonator

3.3.1 History of Ring Resonator

The proposal to use an integrated ring resonator for a bandpass filter has been made in 1969 by E. A. Marcatili [72]. The layout of the channel dropping filter is shown in Fig. 3.1. The transmission properties of the used guide consisted of a dielectric rod with rectangular cross section, surrounded by several dielectrics of smaller refractive indices have been described by E. A. Marcatili [73].

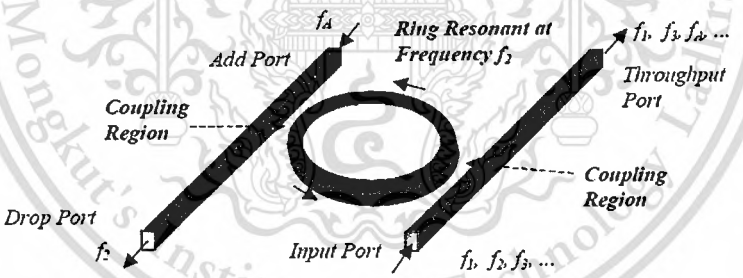

Fig. 3.1 Ring resonator channel dropping filter.

A general architecture for an autoregressive planar waveguide optical filter was demonstrated for the first time in 1996 [74]. The autoregressive lattice filters which were designed and fabricated consisted of one and two stages using Ge-doped silica waveguides.

A signal flow chart transformation for evaluating the filter transfer functions was demonstrated. Purely passive single ring resonator filters as shown in Fig. 3.1 have been realized in the material system AlGaAs-GaAs [75, 76] and Si-SiO_2 [77] and Si_3N_4- SiO_2 [78].

The radius of the used ring resonators is between 5 μm and 30 μm and the free spectral range (FSR) achieved is between 20 nm and 30 nm. Passive ring resonators in the form of a racetrack have been realized in the material system GaInAsP [79] and AlGaAs-GaAs [80]. The filter performance is limited by bending and scattering losses in the resonator. These losses could be compensated for by using an active material instead or in addition.

3.3.2 Basic Ring Resonator

A ring resonator [81] is simply a waveguide shaped into a ring structure as shown in Fig. 3.2. 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_{r2} 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.

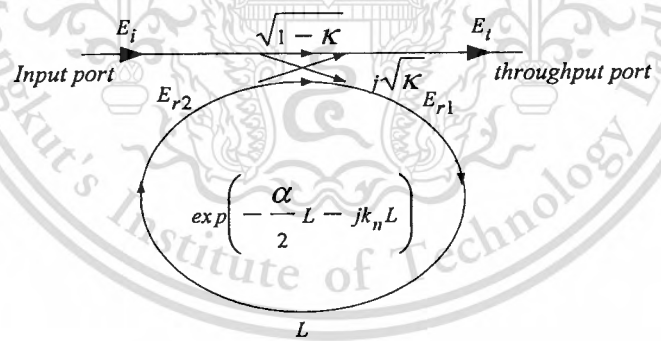

Fig. 3.2 Schematic diagram for a ring resonator coupled to a single waveguide.

The transfer function of this configuration is derived using Z-transform analysis. The circumference of the ring is L ($L=2\pi R$, the radius is R), the coupling coefficient of the coupler is κ. The Z-transform parameter is represented by $z^{-1}=exp^{-jk_nL}$ where $k_n=\frac{2\pi}{\lambda}n_{eff}$ is the propagation constant and n_{eff} is the effective index of the waveguide. The one round trip loss is $a=exp^{-\alpha L/2}$, α is the intensity attenuation coefficient inside

the waveguide [unit $length^{-1}$]. The transmitted or throughput field at the output of the straight waveguide, E_t and inserted electric field, E_i relations can be derived as follows:

$$E_t = \sqrt{1-\gamma} \times \left[E_i \cdot \sqrt{1-\kappa} + j \cdot E_{r2} \sqrt{\kappa} \right] \tag{3.7}$$

$$E_{r1} = \sqrt{1-\gamma} \times \left[j \cdot E_i \cdot \sqrt{\kappa} + E_{r2} \cdot \sqrt{1-\kappa} \right] \tag{3.8}$$

$$E_{r2} = E_{r1} \cdot a\, z^{-1} \tag{3.9}$$

Using these equations, E_t / E_i can be calculated:

$$\frac{E_t}{E_i} = \sqrt{1-\gamma} \times \left[\frac{\sqrt{1-\kappa} - \sqrt{1-\gamma} \cdot a z^{-1}}{1 - \sqrt{1-\gamma} \cdot \sqrt{1-\kappa} \cdot a z^{-1}} \right] \tag{3.10}$$

The transfer function in Eq.(3.10) indicates that a ring resonator is very similar to a Fabry-Perot cavity. In the particular case shown in Fig. 3.2, the corresponding Fabry-Perot cavity would have an input mirror with a field reflectivity 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.

In the following, new parameter will be used for simplification:

$$D = \sqrt{1-\gamma}\,, x = D \cdot exp^{-\alpha L/2}\,, y = \sqrt{1-\kappa}\,,\ \phi = k_n \cdot L \tag{3.11}$$

The intensity relation for the output port is given by:

$$T = \frac{I_t}{I_i}(\phi) = \left| \frac{E_t}{E_i} \right|^2 = D^2 \cdot \left[1 - \frac{(1-x^2)\cdot(1-y^2)}{(1-x\cdot y)^2 + 4 \cdot x \cdot y \cdot sin^2\left(\frac{\phi}{2}\right)} \right]. \tag{3.12}$$

The transmission spectrum [81, 82] of a single ring resonator is shown in Fig. 3.3. The maximum and minimum transmissions are calculated, using:

$$T_{max} = D^2 \cdot \frac{(x+y)^2}{(1+x\cdot y)^2}. \tag{3.13}$$

$$T_{min} = D^2 \cdot \frac{(x-y)^2}{(1-x\cdot y)^2}. \tag{3.14}$$

The minimum transmission T_{min} , occurs at resonant point when the circumference of the ring L, is an integral number of guide wavelength which is defined by

$$\phi = k_n \cdot L = 2m\pi, \qquad m = integer,\ m \cdot \lambda_m = n \cdot L. \tag{3.15}$$

Here, m is the mode number, λ_m is the resonant mode wavelength.

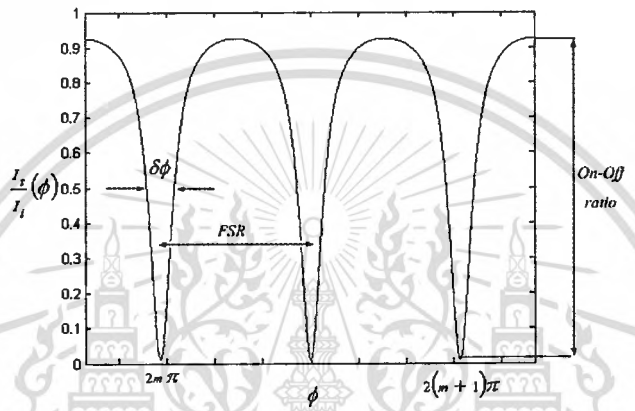

Fig. 3.3 Transmission characteristic of a single ring resonator.

The on-off ratio for the throughput and drop ports, which is the ratio of the on-resonance intensity to the off- resonance intensity which is given by:

$$ON-OFF\ ratio = \frac{T_{max(throughput\ port)}}{T_{min(drop\ port)}}. \tag{3.16}$$

The on-off ratio will become maximum if

$$T_{min} = 0 \Rightarrow x = y \Rightarrow \alpha = -\frac{1}{L} \cdot ln(\frac{1-\kappa}{D^2}). \tag{3.17}$$

This relationship is also referred to as the critical coupling. The maximum on-off ratio [$\frac{I_t}{I_i}(2m\pi) = 0$, Fig. 3.3] can be achieved by varying the coupling factor κ or the intensity attenuation coefficient α (Eq.(3.17) [81, 82]). The value of α can only be changed severely by the implementation of an SOA within the ring resonator or using an all-active ring resonator.

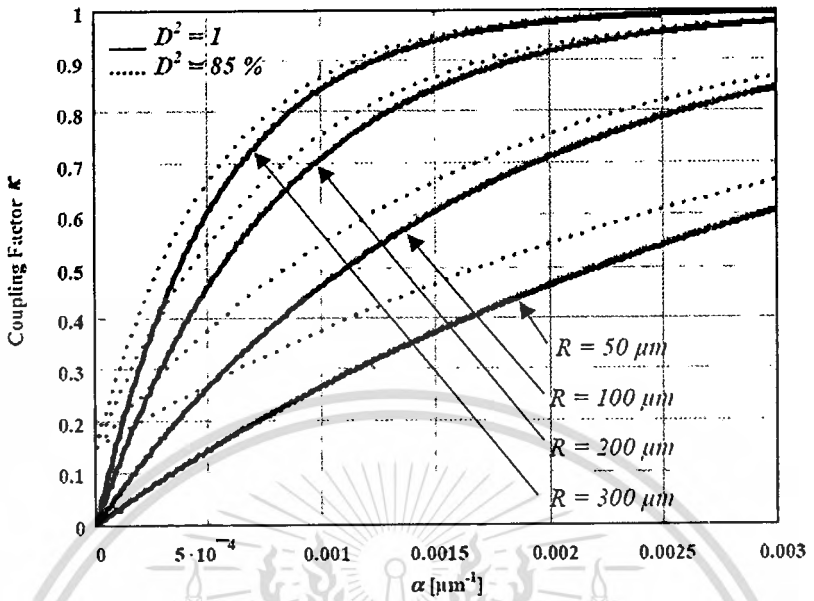

Fig. 3.4 Evaluation of the ideal coupling coefficient κ for a given intensity attenuation coefficient α.

The ideal intensity attenuation coefficient α for the single ring resonator to achieve a maximum on-off ratio $[\frac{I_t}{I_i}(2m\pi) = 0]$, for example, with a radius of R=100 μm, a power coupling coefficient of $\kappa = 0.5$, an intensity insertion loss of the coupler of $D^2 = 85\%\,(\gamma = 15\%)$, is taken from the diagram (Fig. 3.4) [81,82] to be $\alpha = 0.0008\,\mu m^{-1}$ (or $\alpha = 800$).

3.4 Optical Add/Drop Filter

Unlike Fabry-Perot cavities, Bragg gratings, and distributed feedback waveguide devices, the ring geometry permits more than one waveguide to be coupled to the ring resonator. This in return allows multiple input/output accessibility and no need for external circulators to manipulate the input, reflected and throughput data streams. For instance, if one more waveguide is coupled to the filter described earlier, an optical add/drop filter is obtained, as shown in Fig. 3.5.

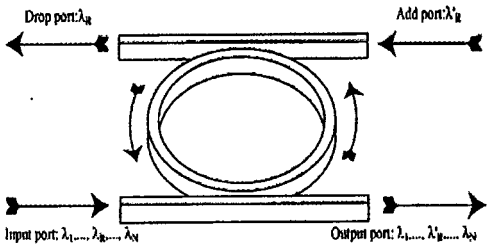

Fig. 3.5 Schematic diagram for a ring resonator coupled to two waveguides, in an add/drop filter configuration.

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 occur. 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.

3.4.1 Architecture of optical add/drop filter

Consider the architecture of double coupler ring resonator (DCRR) [81, 82] which is sometime called optical add/drop filter as illustrated in Fig. 3.6, which is constructed by 2×2 optical couplers.

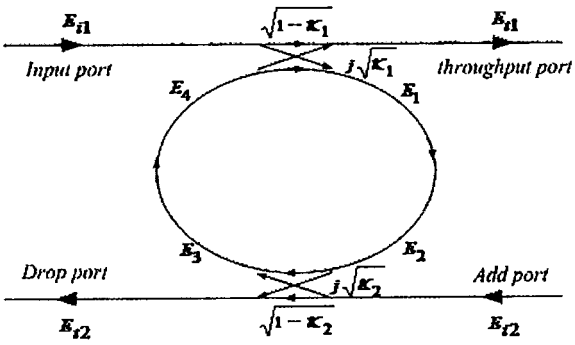

Fig. 3.6 The architecture of DCRR or add/drop filter.

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

$$E_{t1} = \sqrt{1-\gamma_1}\left[j\sqrt{\kappa_1}E_4 + \sqrt{1-\kappa_1}E_{i1} \right] \tag{3.18}$$

$$E_1 = \sqrt{1-\gamma_1}\left[j\sqrt{\kappa_1}E_{i1} + \sqrt{1-\kappa_1}E_4 \right] \tag{3.19}$$

where γ and κ_1 are the loss and the coupling coefficients, respectively. The incoming light of E_{i1} and E_4 are coupled through the first coupler to the output light E_{t1} and E_1, and the output light E_1 is then transmitted through the ring becomes output light E_2. According to light transmission theory in linear optical systems, we obtain the following relation between E_1 and E_2

$$E_2 = E_1 e^{-\frac{\alpha L}{2}\frac{1}{2} - jk_n\frac{L}{2}} \tag{3.20}$$

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

$$E_{t2} = E_1 e^{-\frac{\alpha L}{2}\frac{1}{2} - jk_n\frac{L}{2}} \cdot j\sqrt{1-\gamma_2}\sqrt{\kappa_2} \qquad \text{at } E_{i2} = 0 \tag{3.21}$$

$$E_3 = E_1 e^{-\frac{\alpha L}{2}\frac{1}{2} - jk_n\frac{L}{2}} \sqrt{1-\gamma_2}\sqrt{1-\kappa_2} \tag{3.22}$$

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

$$E_4 = E_3 e^{-\frac{\alpha L}{2}\frac{1}{2} - jk_n\frac{L}{2}} \tag{3.23}$$

$$E_1 = \frac{E_{i1} j\sqrt{1-\gamma_1}\sqrt{\kappa_1}}{1-\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}} \tag{3.24}$$

$$E_4 = \frac{E_{i1} j\sqrt{1-\gamma_1}\sqrt{\kappa_1}}{1-\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL} \tag{3.25}$$

By using the above equations, the transfer function for throughput port and drop port in Fig. 3.6 can thus be expressed as follows:

Throughput port:

$$\begin{aligned}\frac{E_{t1}}{E_{i1}} &= \frac{-(1-\gamma_1)\kappa_1\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}+\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}}{1-\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}} \\ &= \frac{-(1-\gamma_1)(1-\kappa_1)\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}}{1-\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}} \\ &= \frac{-\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}+\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}}{1-\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}}\end{aligned} \tag{3.26}$$

Drop port:

$$\frac{E_{t2}}{E_{i1}} = \frac{-\sqrt{1-\gamma_1}\sqrt{1-\gamma_2}\sqrt{\kappa_1\cdot\kappa_2}e^{-\frac{\alpha}{2}\frac{L}{2}-jk_n\frac{L}{2}}}{1-\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}} \tag{3.27}$$

The intensity relations for the throughput and drop ports can be obtained by normalizing the transfer functions in Eqs.(3.26) and (3.27) which are given by

$$\frac{I_{t1}}{I_{i1}} = \left|\frac{E_{t1}}{E_{i1}}\right|^2 = \frac{\begin{array}{c}1-(1-\gamma_1)\kappa_1-2\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\cdot\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L}\cos(k_nL)\\ +(1-\gamma_2)(1-\kappa_2)e^{-\alpha L}\end{array}}{\begin{array}{c}1+(1-\gamma_1)(1-\kappa_1)\cdot(1-\gamma_2)(1-\kappa_2)e^{-\alpha L}\\ -2\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\cdot\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L}\cos(k_nL)\end{array}} \tag{3.28}$$

$$\frac{I_{t2}}{I_{i1}}=\left|\frac{E_{t2}}{E_{i1}}\right|^2=\frac{(1-\gamma_1)(1-\gamma_2)\cdot\kappa_1\kappa_2 e^{-\frac{\alpha}{2}L}}{1+(1-\gamma_1)(1-\kappa_1)\cdot(1-\gamma_2)(1-\kappa_2)e^{-\alpha L}} \tag{3.29}$$
$$-2\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\cdot\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L}cos(k_nL)$$

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

$$x=exp\left(-\frac{\alpha}{2}L\right) \tag{3.30}$$
$$c_1=\sqrt{1-\kappa_1} \tag{3.31}$$
$$c_2=\sqrt{1-\kappa_2} \tag{3.32}$$

The intensity relations Eqs.(3.28) and (3.29) are then given by

$$\frac{I_{t1}}{I_{i1}}(\phi)=\left|\frac{E_{t1}}{E_{i1}}\right|^2=1-\frac{\left(1-c_1^2\right)\cdot\left(1-c_2^2x^2\right)}{\left(1-c_1c_2x\right)^2+4c_1c_2xsin^2\left(\frac{\phi}{2}\right)} \tag{3.31}$$

$$\frac{I_{t2}}{I_{i1}}(\phi)=\left|\frac{E_{t2}}{E_{i1}}\right|^2=\frac{\left(1-c_1^2\right)\cdot\left(1-c_2^2\right)\cdot x}{\left(1-c_1c_2x\right)^2+4c_1c_2xsin^2\left(\frac{\phi}{2}\right)} \tag{3.32}$$

3.4.2 Optical add/drop filter in operation

The transfer of power between the two port waveguides of a four port micro-resonator is only possible at discrete wavelength regions at which the optical path length of the light in the resonator is an integer multiple of its effective wavelength.

The process by which power is transferred through the resonator is characterized by three distinct phases [83]: the initial, transient and Steady State as shown in Fig. 3.7.

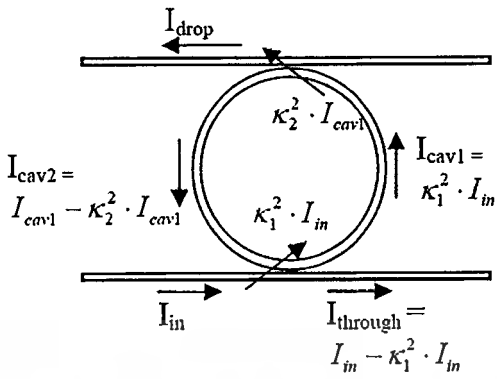

Fig. 3.7 The process by which the power is transferred through the ring resonator.

3.4.2.1 The Initial State

1. Incoming light I_{in} of a certain wavelength propagates along one of the port waveguides of the micro-resonator.
2. When the light reaches the first coupler, a small power fraction $K_1^2 \cdot I_{in1}$ is then evanescently coupled into the resonator.
3. Most of the light, however, will continue its path along the port waveguide as $I_{through}$. The light I_{cav1} that is now in the resonator will propagate along the resonator until it reaches the other port waveguide and the second coupler.
4. Here a small fraction $K_2^2 \cdot I_{cav1}$ of the light is coupled out of the resonator as I_{drop} while the larger fraction I_{cav2} continues its roundtrip towards the first coupler.

3.4.2.2 The Transient State

1. In the transient phase the dominant factor that determines the buildup of the power in the resonator is the modal phase of the light I_{cav2} as it interferes with the light in the port waveguide at the first coupler.
2. If the resonance condition $\emptyset_T = m \cdot 2\pi, m \epsilon N$ is satisfied for the roundtrip phase of I_{cav2} , constructive interference will occur at the resonator side of the first coupler, results in a net increase of power within the resonator.
3. At the same time, destructive interference at the port waveguide side results in a decrease of the power $I_{through}$.

3.4.2.3 The Steady State

1. The process of power enhancement within the cavity while transferring more power from I_{in} will repeat itself many times as I_{cav2} continues to interfere with the light in the port waveguide on every round-trip.
2. The intra-cavity power cannot rise indefinitely, however, and at a certain power level a state of equilibrium is reached between the light I_{cav2} in the cavity and the light in the port waveguide I_{in}.
3. At this point no additional power can be transferred from I_{in} and the resonator is operating in a steady state condition. The power in the through port $I_{through}$ is now at its lowest level while the power in the drop port I_{drop} is at its highest level. The resonator has thus effectively transferred power from the input to the drop port.

CHAPTER 4
CRYPTOGRAPHY AND CHAOS-BASED COMMUNICATION

4.1 Cryptography

Cryptography is techniques for the secure communication in the presence of third parties[84]. Generally Cryptography is related to various aspects in information security such as data confidentiality, data integrity, and authentication[85]. Applications of cryptography include Virtual Private Network (VPN), ATM cards, computer passwords, and electronic commerce. Cryptology converts the information from a readable state to apparent nonsense. The sender retained the ability to decrypt the information and therefore avoid unwanted persons being able to read it.

4.1.1 Modern Cryptography

Modern cryptography designs cryptographic algorithms around computational hardness assumptions, making such algorithms are difficult to break by eavesdroppers. It is theoretically possible to break such a system but it is infeasible to do so by any practical means. These schemes are therefore computationally secure.

4.1.1.1 Private-Key Encryption

The cryptography is historically concerned with secret communication, specifically the construction of ciphers (now called encryption schemes) for providing secret communication between two parties sharing some information in advance. The setting in which the communicating parties share some secret information in advance is now known as the private-key [86]. In the private-key setting, two parties share a key, and use this key when they wish to communicate secretly with each other. A party sending a message uses the key to encrypt the message prior to it is sent, and the receiver uses the same key to decrypt and recover the message upon receipt. The message itself is called the plaintext, and the encrypted information is called the ciphertext; see Fig. 4.1. The shared key is used to distinguish the communicating parties from eavesdroppers over a public channel.

In this setting, the same key is used to convert the plaintext into a ciphertext and back. This explains why this setting is also known as the symmetric-key setting, where the symmetry lies in the fact that both parties use the same key for both encryption and decryption. This is in contrast to the setting of asymmetric encryption (introduce in next section), where the sender and receiver use different keys for encryption and

decryption.

Using the private-key encryption, the communicating parties must have some way of initially sharing a key in a secret manner. (Note that if one party simply sends the key to the other over the public channel, the eavesdropper obtains the keys too!). Despite this, there are still many settings where the private-key methods are sufficient and in wide use; one example is disk encryption, where the same user uses a fixed secret key to both write to and read from the disk. As we will explore further in the next section, the private-key encryption is also widely used in conjunction with asymmetric methods.

The private-key encryption scheme consists of three algorithms: the first is a procedure for key generation, the second a procedure for encryption, and the third a procedure for decryption. These have the following functionality:

1. The key-generation algorithm (**KeyGen**) is a probabilistic algorithm that outputs a key *Key* chosen according to some distribution that is determined by the scheme.

2. The encryption algorithm (**Encryption**) takes as input a key *Key* and a plaintext message *Mess* and outputs a ciphertext *Ctext*. We denote by $\mathbf{Encryption}_{key}(Mess)$ the encryption of the plaintext *Mess* using the key *Key*.

3. The decryption algorithm (**Decryption**) takes as input a key *Key* and a ciphertext *Ctext* and outputs a plaintext *Mess*. We denote the decryption of the ciphertext *Ctext* using the key *Key* by $\mathbf{Decryption}_{key}(Ctext)$.

The set of all possible keys output by the key-generation algorithm is called the key space denoted by *Kspace*. The **KeyGen** simply chooses a key randomly from the key space. The set of all the messages is denoted *Mset* and is called the plaintext (or message) space. Since any ciphertext is obtained by encrypting some plaintext under some key, the sets *Kspace* and *Mset* together define a set of all possible ciphertexts denoted by *Cset*. An encryption scheme is fully defined by specifying the three algorithms (KetGen,Encryption,Decryption) and the plaintext space *Mset*.

The basic correctness requirement of any encryption scheme is that for every key *Key* outputs by **KeyGen** and every plaintext message $Mess \in Mset$, it holds that.

$$\mathbf{Decryption}_{Key}(\mathbf{Encryption}_{Key}(Mess)) = Mess \tag{4.1}$$

To decrypt a ciphertext yields the original message that was encrypted.

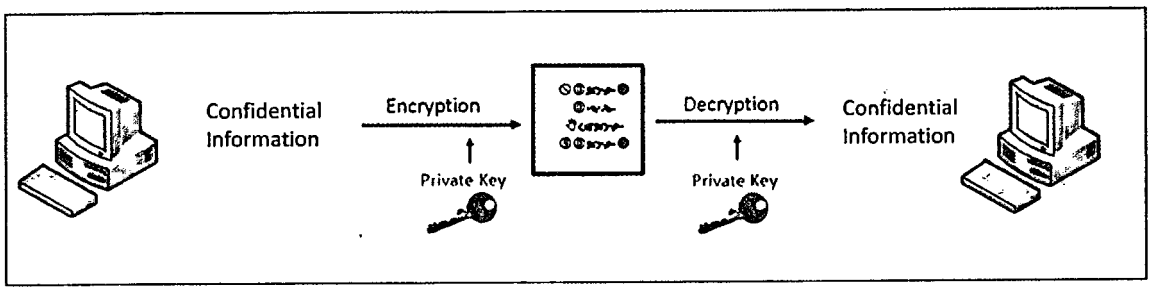

Fig 4.1 The basic setting of the private-key encryption

4.1.1.2 Public-Key Encryption

As mentioned previously, for the private key technique, cryptographers must rely on shared, secret keys to achieve the secure communication. Public-key technique [86], in contrast, allows parties to communicate secretly without having agreed on any secret information in advance. In the setting of the private-key encryption, two parties agree on a secret key *Key* which can be used (by either party) for both encryption and decryption. Public-key encryption is asymmetric which one party (the receiver) generates a pair of keys (*PubKey,PriKey*), called the public key and the private key, respectively. The public key is used by the sender to encrypt a message for the receiver; the receiver then uses the private key to decrypt the ciphertext.

The goal is to avoid the need for two parties to meet in advance to agree on any information, there are essentially two ways to do this. If the receiver knows that the sender wants to communicate with him, the receiver can generate (*PubKey,PriKey*), and then send *PubKey* in the clear to the sender; the sender can then use *PubKey* to encrypt his message.

In the second way, the receiver generates (*PubKey,PriKey*) in advance, independent of any particular sender. Then the receiver widely spread the public key *PubKey* e.g. publishing it on the webpage, or sending it via the email. Now, anyone who wishes to communicate privately with the receiver can look up his public key and proceed as above. Multiple senders can communicate multiple times with the receiver using the same public key *PubKey.*

An important point is that *PubKey* is public, it can easily be learned by an eavesdropper. In the first case, the eavesdropper can trap on the communication somewhere between the sender and receiver to obtain *PubKey* by simply listening to the first message that the receiver sends to the sender; in the second case, an eavesdropper could just look up the receiver's public key on his own. An important thing is that the security of the public-key encryption cannot rely on the secrecy of

PubKey, but must instead rely on the secrecy of *PriKey*. It is therefore crucial that the receiver must not reveal his *PriKey* to anyone, including the sender.

4.1.1.3 Comparison of Private-Key Encryption

The key difference between the private and public key encryptions [86] is that the private-key encryption requires complete secrecy of all cryptographic keys, whereas the latter requires secrecy for "only" half the key-pair (*PubKey,PriKey*). The private-key setting the communicating parties must somehow be able to share the secret key without allowing third party to learn it; in the public-key setting, the public key can be sent from one party to the other over the public channel without compromising security. As the private-key encryption schemes use the same key for both encryption and decryption, while the public-key encryption schemes use different keys for each operation. For this reason, the public-key encryption schemes are sometimes called asymmetric which the roles of the sender and receiver are not interchangeable the way they are in the private-key setting: a given instance of the public-key encryption scheme allows communication in one direction only (the public-key encryption scheme forces a distinction between one user who acts as a receiver and other users who act as senders). On the other hand, a single instance of the public-key encryption scheme enables multiple senders to communicate privately with a single receiver, in contrast to the private-key case where a secret key shared between two parties enables only those two parties to communicate privately.

In summary, we see that the public-key encryption has the following advantages relative to the private-key encryption.

1. The most important advantage is that the public-key encryption addresses the key distribution problem since communicating parties do not need to secretly share a key in advance of their communication. The public-key encryption allows two parties to communicate secretly even if all communications between them are monitored.

2. Once one receiver is communicating with many senders, it is much more convenient for the receiver to store a single private key *PriKey* rather than to share many different secret keys (i.e., one for each sender). In fact, the public-key encryption allows enormous flexibility, and is clearly essential for an on-line business.

The main disadvantage of the public-key encryption is that it is at least 2 to 3 times slower than the private-key encryption. This means that it can be a challenge to implement the public-key encryption in severely resource-constrained devices like mobile devices, smartphones, smartcards, radio-frequency identification (RFID) tags and etc. In any case, we may conclude that if the private-key encryption is on option (i.e., if

two parties can securely share a key in advance) it should always be used. In fact, the private-key encryption is used in the public-key setting to improve the efficiency of the (public-key) encryption of long messages, in this case, the private-key encryption is used to exchange the public-key privately.

4.2 Noise

Noise is undesired signal [87] that is intrinsically objectionable or that interferes with other signals being propagated. In information theory, the noise refers to those random, unpredictable, and undesirable signals, or changes in signals, that mask the desired information content. The noise differs from periodic vibrations in the random change in the instantaneous values of the quantities characterizing a given process. Often, the noise is a mixture of random and periodic vibrations. Depending on the temporal, spectral, and spatial structure of noise, various mathematical models are used to describe it.

The noise is subdivided into statistically stationary and nonstationary noise. The theory and methods of measuring stationary noise, the classical model of which is white noise, are most highly developed. Stationary noise is characterized by the constancy of the average parameters: intensity (power), spectral distribution of intensity (spectral density), and the autocorrelation function. The noise observed in practice, which results from the action of many independent sources, such as the noise of a crowd of people, the sea, or a vortex air flow or the noise at a radio-receiver output, is quasi-stationary. Noise that lasts for short time intervals is called nonstationary noise. Such noise includes, for example, the street noise of passing traffic, individual sounds in production processes, and infrequent impulse noise in radio engineering.

4.2.1 Phase and Frequency noises

4.2.1.1 Phase noise

The phase noise [87] represents of rapid, short-term, random fluctuations in the phase of a waveform in frequency domain, caused by time domain instabilities ("jitter"). Recently, IEEE changed the definition of the phase noise to

$$L(f) = \frac{S_\phi}{2} \tag{4.2}$$

where S_ϕ is the (single-sided) spectral density of a signal's phase fluctuations.

All real oscillators have phase modulated noise components. The phase noise

components spread the power of a signal to adjacent frequencies, resulting in noise sidebands. Consider the following noise free signal:

$$v(t) = A\cos(2\pi f_0 t) \tag{4.3}$$

The phase noise is added to this signal by adding a stochastic process represented by φ to the signal as follows

$$v(t) = A\cos(2\pi f_0 t + \varphi(t)) \tag{4.4}$$

Pulse trains exhibit some deviations of the temporal pulse positions from those in a perfectly periodic pulse train, this phenomenon is called *timing jitter*. Sometimes there is a confusion between the phase noise and timing jitter because timing jitter can also be seen as a kind of the phase noise: a timing change by one pulse period can be interpreted as a phase change of 2π. The phase noise can be converted to jitter using the following formula :

Jitter (seconds) = Phase error (degrees)/(360 x Frequency (Hertz)) (4.5)

4.2.1.2 Frequency Noise

The frequency noise [87] is noise of the instantaneous frequency of an oscillating signal. The term *frequency noise* refers to random fluctuations of the instantaneous frequency of an oscillating signal. The instantaneous frequency is defined as

$$v(t) = \frac{1}{2\pi}\frac{d\varphi}{dt} \tag{4.6}$$

i.e. essentially as the temporal derivative of the oscillation phase φ. Any random deviation from a purely linear phase evolution is seen as the frequency noise.

The phase noise is directly related to the frequency noise, as the instantaneous frequency is essentially the temporal derivative of the phase. The power spectral density of the frequency noise (with units of Hz^2/Hz) is directly related to that of the phase noise shown as follows.

$$S_v(f) = f^2 S_\varphi(f) \tag{4.7}$$

where f is the noise frequency.

The phase noise and the frequency noises are just different ways of describing

the same phenomenon. However, numerical processing of frequency noise rather than the phase noise can have technical advantages in certain situations.

4.2.2 Intensity Noise

A most important type of noise in a light beam is noise of its intensity [87]. Strictly, the noise of the optical *power*, rather than of the optical intensity, is usually considered, but the common term is *intensity noise* rather than *power noise*.

4.2.2.1 Specifications for Intensity Noise

Intensity noise is usually quantified as *relative intensity noise* (RIN), i.e. as noise of the power divided by the average power. Common specifications are based on an root-mean-square (r.m.s: the square root of the mean of the squares of the values) or a power spectral density.

4.2.2.2 Origins of Intensity Noise

Intensity noise of a laser results partly from quantum noise (associated with laser gain and resonator losses) and partly from technical noise sources [87] such as excess noise of the pump source, vibrations of resonator mirrors, thermal fluctuations in the gain medium, propagation of light beam in the ring resonator etc. The resulting intensity noise also depends on the operation conditions, e.g. it often becomes weaker at high pump powers, where relaxation oscillations are strongly damped. Fig. 4.2 shows the Intensity noise spectrum of a solid-state laser which it can be seen that the noise power fluctuates up and down, plotted referring to frequency intervals in the range of 0 to 400 kHz, increased low-frequency noise is caused by excess noise of the pump source.

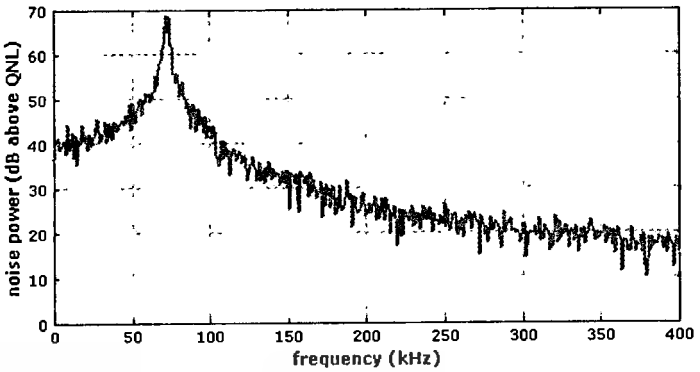

Fig. 4.2 Intensity noise spectrum of a solid-state laser, increased low-frequency noise is caused by excess noise of the pump source.

4.2.3 Measurement of Intensity Noise

Intensity noise is normally measured by detecting the intensity (or power) with a fast photodetector (e.g. with a PIN photodiode) and evaluating the noise spectrum with an electronic spectrum analyzer.

4.2.3.1 Relative Intensity Noise (RIN)

Relative intensity noise [87] describes the instability in the power level of a laser. The noise term is important to describe lasers used in fiber-optic communication. Relative intensity noise can be generated from cavity vibration, fluctuations in the laser gain medium or simply from transferred intensity noise from a pump source. Since intensity noise typically is proportion to the intensity, the relative intensity noise is typically independent of laser power.

RIN is the ratio of the mean-square optical intensity noise to the square of the average optical power:

$$\text{RIN} = \frac{\langle \Delta P^2 \rangle}{P^2} \text{ dB/Hz} \tag{4.8}$$

where: $\langle \Delta P^2 \rangle$ is the mean-square optical intensity fluctuation (in a 1-Hz bandwidth) at a specified frequency, and P is the average optical power.

4.2.3.2 Power Spectral Density

Power Spectral Density [87] is optical power or noise power per unit frequency interval. In optics, power spectral densities (also sometimes just called power densities) occur basically in two different forms:

1. Optical power spectral densities are defined as the optical power per optical

frequency (or wavelength) interval, e.g. specified in mW/THz or mW/nm. When the spectral distribution of optical power e.g. of some laser source is measured e.g. with an optical spectrum analyzer, the result is usually given either as a power spectral density (e.g. in units of mW/nm or dBm/nm, with dBm = dB relative to 1 mW), or as a power for a given measurement bandwidth.

2. Noise power densities are defined as the power spectral density of the fluctuations of a quantity such as an optical power or phase, where the frequency argument refers to a noise frequency (rather than to an optical frequency). In the case of noise powers, a PSD always refers to averaged power levels related to intervals of noise frequency (rather than optical frequency). Such noise PSDs can occur in the context of any optical or electrical signals.

Fig. 4.3 shows the power spectral density of black bodies at various temperatures according to Planck's law, plotted referring to frequency intervals. In the graph it shows the relation between the intensity of black bodies at various temperatures and the frequencies in the range of 0 to 600 THz. The power spectral density can be shown in the wavelength intervals, as Fig 4.4 shows the relation between the intensity of black bodies at various temperatures and the wavelengths in the range of 300 to 1,500 nm.

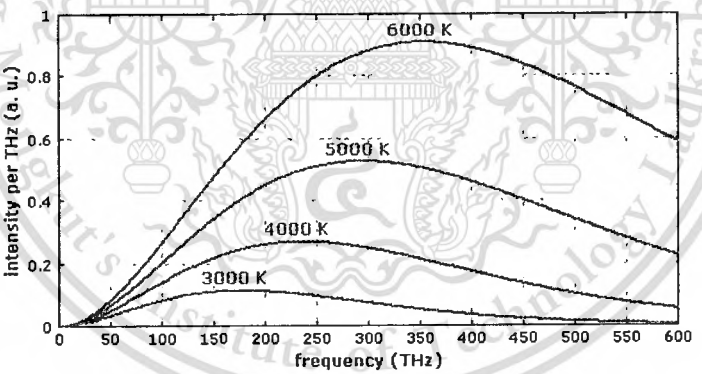

Fig. 4.3 Power spectral density of black bodies at various temperatures according to Planck's law, plotted referring to frequency intervals.

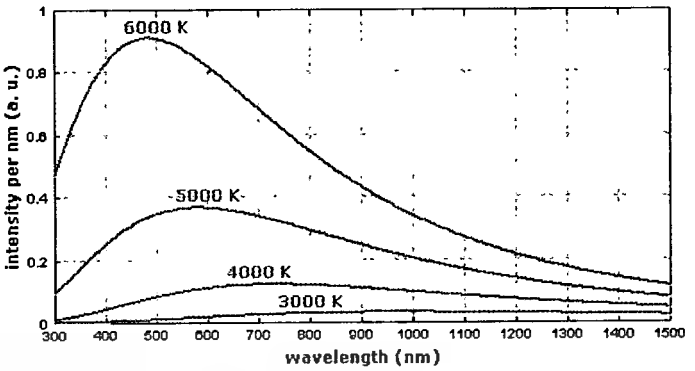

Fig. 4.4 is similar to Fig. 4.3, but referring to wavelength intervals.

4.2.3.3 Signal-to-noise ratio

Signal-to-noise ratio [87] is the ratio of signal power to noise power in a detector. It compares the level of a desired signal to the level of background noise. A ratio higher than 1:1 indicates more signal than noise.

$$SNR = \frac{P_{signal}}{P_{noise}} \tag{4.9}$$

Where P is average power, both signal and noise power must be measured at the same or equivalent points in a system, and within the same system bandwidth.

The quality of optical and other measurements is often characterized with a signal-to-noise ratio (SNR, S/N ratio). This is generally understood to be the ratio of the detected powers (not amplitudes), and is often expressed in decibels.

The signal-to-noise ratio often limits the accuracy which some measurement can be done. For digital signals, it can limit the reliability of detecting correctly, which can be quantified with a bit error rate. The latter situation is common in optical fiber communications, where some required bit error rate can only be achieved with a sufficiently high signal-to-noise ratio at the detector.

4.2.4 Auto-correlation

The auto-correlation function [88] shows how similar two signals are, and for how long they remain similar when one is shifted with respect to the other. It measures the correlation of a signal with itself shifted by some time delay. Correlating a signal with itself is called autocorrelation. Different sorts of signal have distinctly different autocorrelation functions. In signal processing, the auto-correlation function is normalized by mean and variance, it is sometimes referred to as the autocorrelation coefficient.

Given a signal $f(t)$, for the continuous case, the continuous autocorrelation $R_{ff}(\tau)$ is most often defined as the continuous cross-correlation integral of $f(t)$ with itself, at lag τ.

$$R_{ff}(\tau) = (f(t) * \bar{f}(-t))(\tau) \tag{4.10}$$

$$= \int_{-\infty}^{\infty} f(t+\tau)\,\bar{f}(t)dt \tag{4.11}$$

$$= \int_{-\infty}^{\infty} f(t)\,\bar{f}(t-\tau)dt \tag{4.12}$$

Where $\bar{f}$ represents the complex conjugate and $*$ represents convolution. For a real function, $\bar{f} = f$.

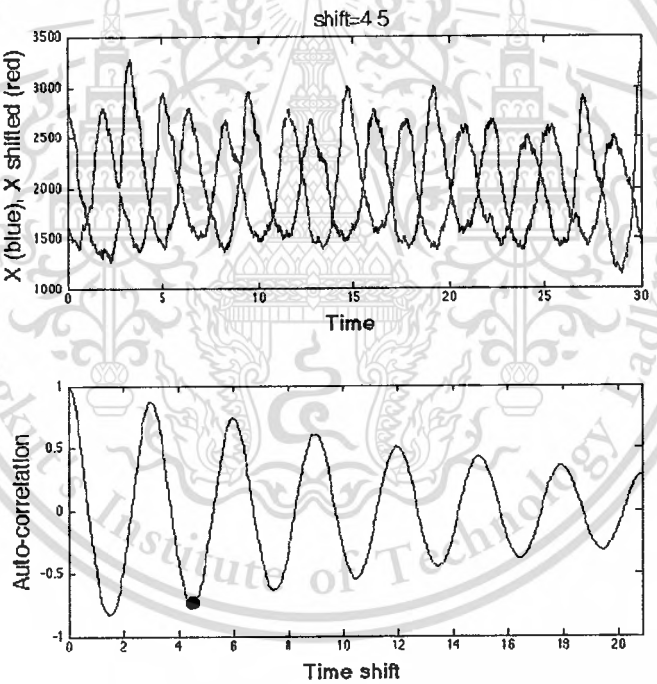

Fig. 4.5 shows the auto-correlation function when the signal is shifted.

Fig. 4.5 [88] shows the auto-correlation function when the signal is shifted from itself. The auto-correlation function can be used to detect repeats or periodicity in a signal. It can be used to assess the effect of fluctuations (noise) on a periodic signal. In absence of noise, the auto-correlation function oscillates with a constant amplitude, the period of the auto-correlation corresponds to the period of the signal. In presence of noise, the envelop of the auto-correlation function decreases exponentially, more

important is the noise, faster is this decreasing, thus the speed of the decreasing can be used to quantify the effect of noise.

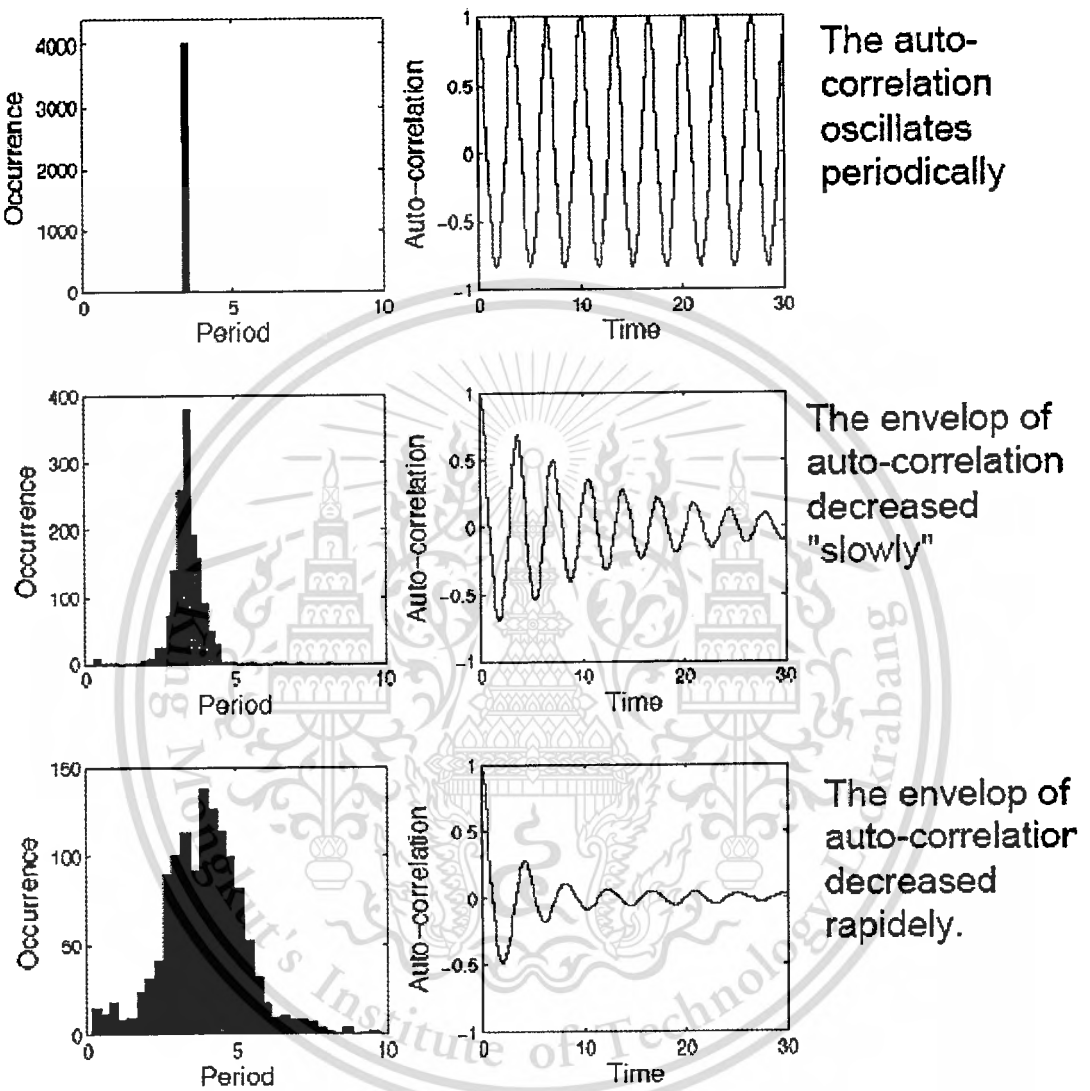

Fig. 4.6 shows how the auto-correlation function detects the effect of fluctuations (noise) on a periodic signal.

Fig. 4.6 [88] shows how the auto-correlation function detects the effect of the noise on a periodic signal, the envelop of the auto-correlation decreases more, when there is the higher noise. An illustration of the usefulness of the auto-correlation function is when we know the spectrum of the signal, and now wish to design the appropriate filter; for this we also need to know the spectrum of the noise. The first step is to auto-correlate a long sample of the noise, it uses a Fourier analysis of the auto-

correlation function; this yields the power spectrum of the noise, from which we can take the square root, at each frequency, to obtain the amplitude spectrum of the noise. The Fourier transform of an autocorrelation function is the power spectrum, or equivalently, the autocorrelation is the inverse Fourier transform of the power spectrum.

The relationship between the autocorrelation and the Fourier transform is known as the Wiener-Khinchin theorem. The Wiener–Khinchin theorem states that the power spectral density of a wide–sense stationary random process is the Fourier transform of the corresponding autocorrelation function.

For the continuous case

$$R(\tau) = \int_{-\infty}^{\infty} S(f) e^{j2\pi f\tau} df \tag{4.13}$$

$$S(f) = \int_{-\infty}^{\infty} R(\tau) e^{-j2\pi f\tau} d\tau \tag{4.14}$$

Where $R(\tau)$ is the autocorrelation function, $S(f)$ is the power spectral density , f is signal frequency , and τ is delay. The Wiener–Khinchin theorem can be re-expressed in terms of real cosines only:

$$R(\tau) = \int_{-\infty}^{\infty} S(f) \cos(2\pi f\tau) df \tag{4.15}$$

$$S(f) = \int_{-\infty}^{\infty} R(\tau) \cos(2\pi f\tau) d\tau \tag{4.16}$$

4.3 Background in Chaos Theory

Traditionally, signals have been partitioned into two broadly defined classes, i.e., stochastic and deterministic [89]. Stochastic signals are compositions of random waveforms with each component being defined by and underlying probability distribution, whereas deterministic signals are resulted from deterministic dynamical systems which can produce a number of different steady state behaviors including periodic, and chaotic solutions.

Periodic behavior is the simplest type of steady state oscillatory motion. Sinusoidal signals are periodic solutions of continuous-time deterministic dynamical systems, which are universally used as carriers in analog and digital communication systems.

Deterministic dynamical systems also admit a class of nonperiodic signals, which are characterized by a continuous "noiselike" broad power spectrum. This is called Chaos.

4.3.1 Properties of Chaos

It is now well-known that a deterministic dynamical system [89] is one whose state evolves with time according to a deterministic evolution rule. The time evolution of the state is completely determined by the initial state of the system, the input, and the rule. For example, the state of a digital filter is determined by the initial state of the filter, the input, and a difference equation which describes the evolution of the state from one time instant to the next.

In contrast to a stochastic dynamical system, which may follow any number of different trajectories from a given state according to some probabilistic rule, trajectories of a deterministic dynamical system are unique. From any given state, there is only one "next" state. Therefore, the same system started twice from the same initial state with the same input will follow precisely the same trajectory through the state space. Deterministic dynamical systems can produce a variety of steady-state behaviors, the most well-known are stationary, periodic, and quasi-periodic solutions. These solutions are "predictable" in the sense that a small piece of a trajectory enables one to predict the future behavior along that trajectory.

Chaos refers to solutions of deterministic dynamical systems which, while predictable in the short-term, exhibit long-term unpredictability. Since the initial state, input, and rule uniquely determine the behavior of a deterministic dynamical system, it is not obvious that any "unpredictability" is possible. Long-term unpredictability occurs because the dynamics of a chaotic system persistently amplifies errors in specifying the state. Thus, two trajectories starting from the small different initial conditions quickly become uncorrelated. This is because in a chaotic system, the precision with which the initial conditions must be specified in order to predict the behavior over some specified time interval growing exponentially with the length of the prediction interval. As a result, long-term prediction becomes impossible. This long-term unpredictability is apparent itself in the frequency domain as a continuous power spectrum, and in the time domain as random "noiselike" signal.

To get a better understand of what chaos is, here is a list of its main characteristics [89]:

1. Chaos results from a deterministic nonlinear process.
2. The motion looks disorganized and erratic, although sustained. In fact, it can usually pass all statistical tests for randomness (thereby we cannot distinguish chaotic data from random data easily), and has an invariant probability

distribution. The Fourier spectrum (power spectrum) is "broad" (noiselike) but with some periodicities sticking up here and there [90,91].

3. Details of the chaotic behavior are very sensitive to changes in initial conditions (small changes in the starting values of the variables). Equivalently, chaotic signals rapidly decorrelate with themselves.
4. It can result from relatively simple systems.
5. For given conditions or control parameters, chaos is entirely self-generated. In other words, changes in external variables or parameters are not necessary.
6. It is not the result of data inaccuracies, such as sampling error or measurement error. Any specific initial conditions, as long as the control parameter is within an appropriate range, can lead to chaos.
7. In spite of its disjointed appearance, chaos includes one or more types of order or structure. The phase space trajectory may have fractal property (self-similarity).
8. The ranges of the variables have finite bounds, which restrict the attractor to a certain finite region in the phase space.
9. Forecasts of long-term behavior are impossible. Short-term predictions, however, can be relatively accurate.
10. As a control parameter changes systematically, an initially non-chaotic system follows one of a few typical scenarios, called routes to chaos.

4.4 Spread Spectrum Communications

Typical communication systems, such as Frequency Shift Keying (FSK) , Amplitude Shift Keying (ASK) and Phase Shift Keying (PSK) systems as shown in Fig. 4.7, concentrate their transmission power over a bandwidth that is roughly equal to the data rate. To provide a good BER performance, the signal strength needs to be much stronger than the background noise. In consequence, they are readily detected by anyone, even by the eavesdropper. Hence, such narrowband systems provide little security against eavesdropping.

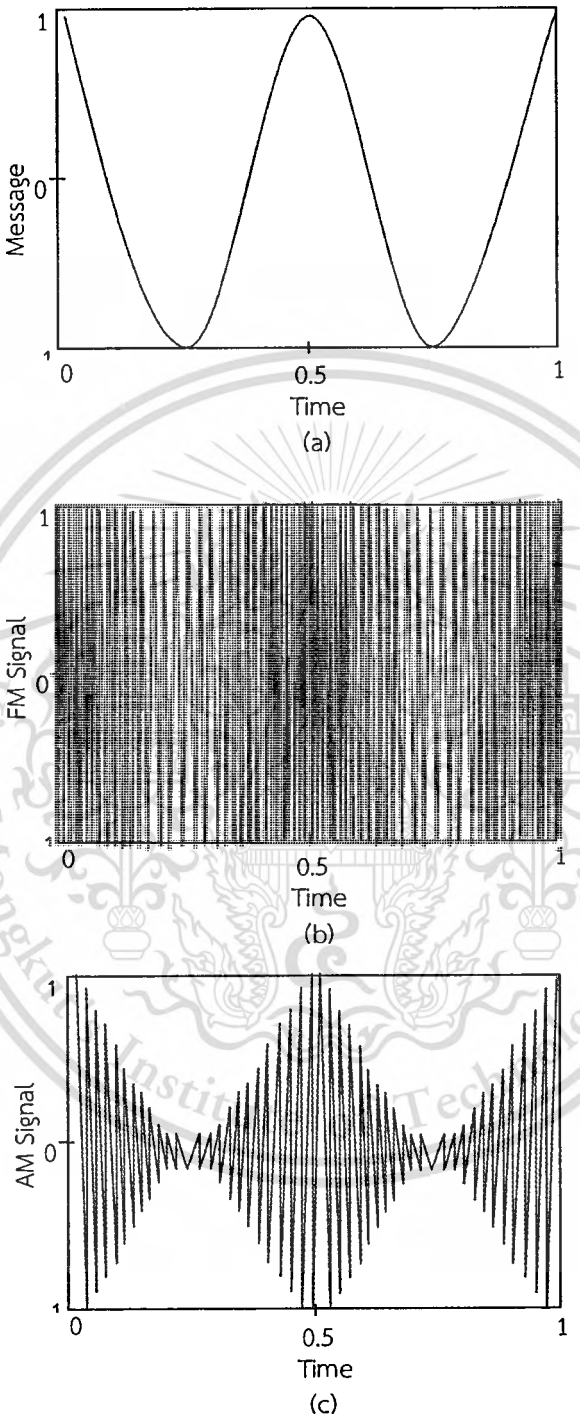

Fig 4.7 Waveforms plotted against time. (a) Message (modulating) signal to be sent; (b) frequency-modulated signal; (c) amplitude-modulated signal.

In spread-spectrum communications [106], the transmitted signal is "spread over a much larger bandwidth compared with that of a narrowband signal. As shown in Fig. 4.8, when the signal spreads, the average power spectral density becomes much lower and the signal can be hidden in the background noise. Because of this feature, it is not easy to detect the presence of the signal without prior knowledge of the communication system or the use of sophisticated equipment. Furthermore, even if the presence of the signal is detected, without the appropriate decoding information, it is very difficult to recover the message. For the intended parties, the demodulation process requires the "dispreading" of the incoming signal back to a narrowband signal, during which the effect of jammers like sinusoids will be substantially reduced. Thus, even in the presence of jamming signals, the message can be recovered satisfactorily in a spread-spectrum communication system.

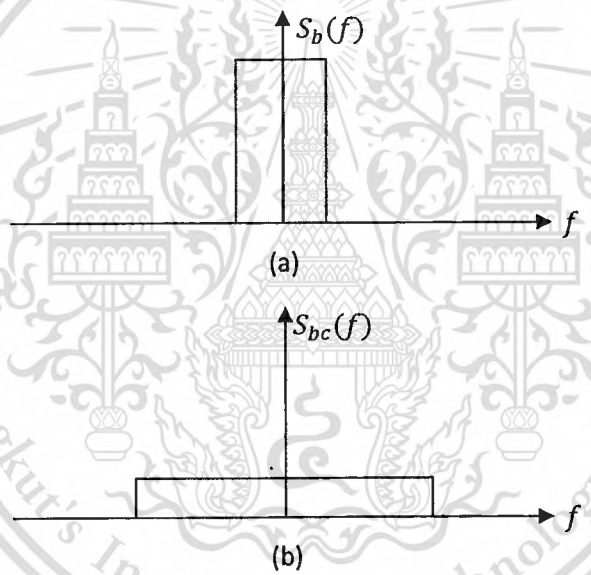

Fig. 4.8 Power spectrum of a spread-spectrum signal (a) before spreading; and (b) after spreading.

4.4.1 Conventional Spread Spectrum

The huge demand for communications results in a large number of users; therefore, today's communication systems are limited primarily by interference from other users. In some applications, the efficient use of available bandwidth is extremely important, but in other applications, where the exploitation of communication channels is relatively low, a wideband communication technique having limited bandwidth efficiency can also be used.

Often, many users must be provided with simultaneous access to the same or neighboring frequency bands. The optimum strategy in this situation, where every user appears as interference to every other user, is for each communicator's signal to look like white noise which is as wideband as possible.

There are two ways in which a communicator's signal can be made to look like wideband noise [89]:

1. To spread each information signal using a pseudo-random sequence to increase the bandwidth of the transmitted signal:
2. To represent each information signal by a piece of "noiselike" waveform [92].

The conventional solution to this problem is the first approach: to use a synchronizable pseudo-random sequence to distribute the energy of the information signal over a much larger bandwidth. The transmitted signal appears similar to noise and is therefore difficult to be detected by eavesdroppers. Therefore, the conventional solution can [89]:

1. Hide a signal "in the noise" by transmitting it in the form of the noiselike; and
2. Have some message privacy in the presence of eavesdroppers.

4.4.2 Spread Spectrum with Chaos

The properties of chaotic signals are similar in many ways those of the stochastic ones [89]. Chaotic signals also have a deterministic nature [89], which makes it possible to generate "noiselike" chaotic signals in a theoretically reproducible manner. Therefore, a pseudo-random sequence generator is a "practical" case of a chaotic system, the principal difference being that the chaotic system has an infinite number of (analog) states, while pseudo-random generator has a finite number (of digital states). A pseudo-random sequence is produced by visiting each state of the system once in a deterministic manner. With only a finite number of states to visit, the output sequence is necessarily periodic. By contrast, an analog chaos generator can visit an infinite number of states in a deterministic manner and therefore produces an output sequence, which never repeats itself. With appropriate modulation and demodulation techniques, the "random" nature and "noiselike" spectral properties of chaotic system can be used to provide simultaneous spreading and modulation of a transmission.

4.5 Chaotic Synchronization

The aim of using the chaotic signal is to hide the information signal in a chaotic carrier and then extract it by some nonlinear, dynamical means at the receiver [89].

If we do this in real-time, we immediately lead to the requirement that somehow the receiver must have a duplicate of the transmitter's chaotic signal or, better yet, synchronize with the transmitter. In fact, synchronization is a requirement of many types of communication, not only chaotic possibilities.

Early work on chaotic synchronization was done by Yamada and Fujisaka [89,93,94]. In that work, it was brought out by a study of the Lyapunov exponents of synchronized coupled systems. Later, Afraimovich *et al.* [95] proposed many of the concepts necessary for analyzing synchronous chaos. A crucial progress was made by Pecora and Carroll [96-100], who have shown theoretically and experimentally that two chaotic systems can be synchronized. This discovery bridges between chaos theories and communications, and opens up a new research area in communications using chaos.

The driving-response synchronization method proposed by Pecora and Carroll is shown in Fig. 4.9, in which the Lorenz system is used in the transmitter and the receiver, where x_i or x_i^r (i = 1,2,3, r standing for the response system) is the state variable of the Lorenz system [101], $l_i$is the ith state equation, and $n(t)$is additive channel noise. The drive-response synchronization method indicates that if a chaotic system can be decomposed into subsystems, a drive system x_1 and a conditionally stable response system (x_2, x_3) in this example [98], then the identical chaotic system at the receiver can be synchronized when is driven with a common signal. The output signal $x_2^r$and x_3^r will follow the signals $x_2$and x_3. For more discussions can see [99].

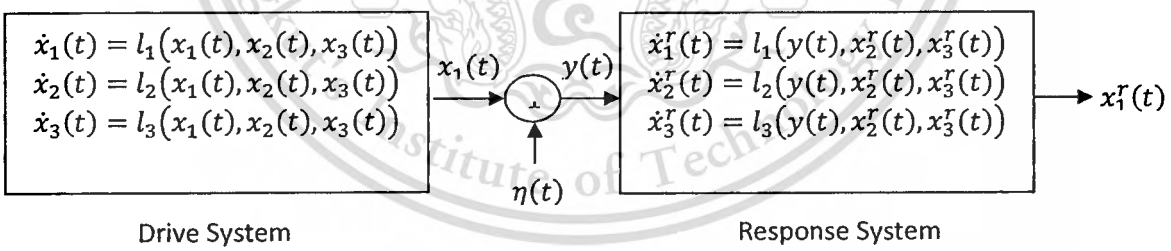

Fig. 4.9 Drive-response synchronization schematic diagram, in which x_i or x_i^r(i=1,2,3, r stands for the response system) is the state variable of the Lorenz system [101], $l_i$is the ith state equation, and $\eta(t)$is additive channel noise.

Inspired by Pecora and Carroll's work, many other synchronization schemes have been proposed, including error feedback synchronization [102], generalized synchronization [103-105], etc.

4.6 Chaos based Communications

Chaotic signals are nonperiodic, random-like signals derived from non-linear dynamical systems [106]. Chaotic signals are also characterized by their impulse-like autocorrelation and low cross-correlation properties [106]. Moreover, chaotic signals are distinguished by their inherent wideband attribute. A typical frequency spectrum of a chaotic signal is shown in Fig. 4.10. Thus, when chaotic signals are used as wideband carriers to convey information, they offer advantages as the conventional spread-spectrum communication systems, such as difficulty of uninformed detection and mitigation to multipath fading. Furthermore, a large number of chaotic carriers can be produced easily as a consequence of the sensitivity to initial conditions and variation of parameters. Thus, chaos can provide a low-cost technique for spread-spectrum communications.

In the past decade, a number of modulation and demodulation schemes based on chaos have been proposed for using in communications. As in conventional communication systems, chaos-based communication systems can be categorized into analog and digital [106], as distinguished by the type of information being carried. For chaos-based analog communication systems, two main techniques have been proposed chaotic masking and chaotic modulation [106]. In chaotic masking, the analog information signal is added to the noiselike chaotic signal. At the receiver, the chaotic signal is regenerated through a chaos synchronization process. Then the analog information signal is recovered by subtracting the reconstructed chaotic signal from the received noiselike signal. The successful demodulation of the signal is subject to a robust synchronization method. Moreover, the analog information signal must have a very small amplitude compared with that of the chaotic carrier. In another chaos-based analog communication system is named the chaotic modulation, the information to be sent is used to change a suitably chosen parameter of the chaos generator. The task of the receiver is then to extract the information of the same parameter based on the received signal, the synchronization is not required during the demodulation process. Although the chaos-based analog communication systems can provide reasonable performance under a noiseless environment, they do not posses sufficient noise immunity in a practical condition. However, digital communication systems based on chaos are more robust against noise.

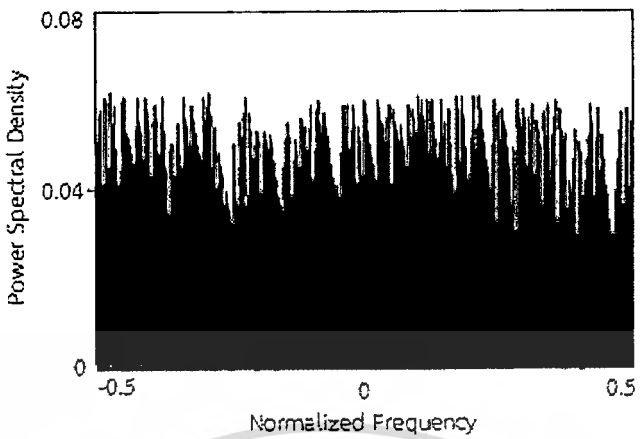

Fig. 4.10 Power Spectrum of a chaotic signal against normalized frequency.

4.6.1 Chaotic Masking

The chaotic communication relies on synchronization [106]. The information signal to be communicated is simply carried by a chaotic waveform [106]. A receiver, synchronized to the transmitter, is able to recover the information signal from the chaos. The applications of chaotic synchronization to communication were suggested in [106,107]. The first configuration suggested which is easiest to explain is the Lorenz system as shown in Fig. 4.11, a small-amplitude information signal is added to the much larger chaotic fluctuation of the x_3 variable and transmitted to the receiver. Because the information signal has a smaller amplitude than the chaotic signal, it is effectively hidden, or masked, by the chaotic signal during transmission. The other communication channel is used to transmit the $x_2$variable to the receiver where it is substituted for the receiver's own y_2 variable, as shown in Fig. 4.11. This substitution of the x_2 for the $y_2$variable causes the entire y system to synchronize to the x system. This synchronization enables the original information signal to be recovered from the masking signal by simply subtracting y_3 from the encoded transmission, $x_3 + i(t)$.

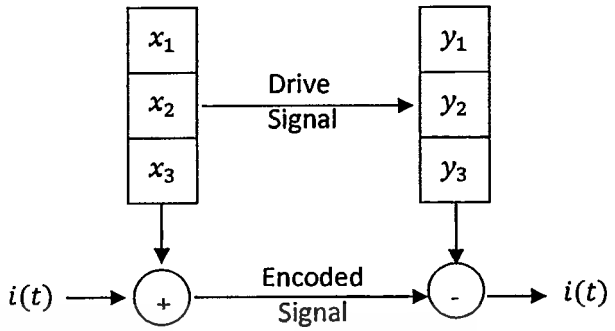

Fig. 4.11 Representation of a simple chaotic communication technique.

A small amplitude information signal,$i(t)$, is masked by a larger amplitude chaotic signal, $x_3(t)$ during transmission. Because the two systems are synchronized, subtraction of y_3, from $x_3 + i(t)$ recovers the information signal that was buried in the chaotic transmitted signal. In the technique described above, two channels between the systems are required for the chaotic communication as shown in Fig. 4.11.

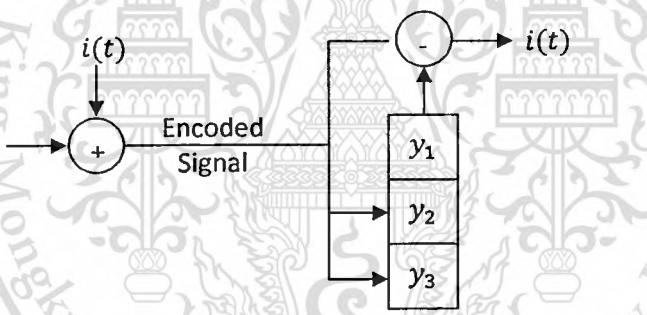

Fig. 4.12 Representation of the chaotic communication technique that does not require separate signal transmission.

The second configuration described here is the chaotic communication that does not require separate transmission channel. As in Fig. 4.12, a small amplitude information signal, $i(t)$, is masked by a larger amplitude chaotic signal, $x_1(t)$. The composite signal, $x_1(t) + i(t)$, drives the receiver system to synchronize with the transmitter system. The information signal is recovered by subtracting $y_1(t)$ from the composite signal. A small-amplitude information signal is transmitted along with a much larger chaotic masking signal. Thus, the small-amplitude information signal in the transmitted signal acts as a small noise to the larger chaotic driving signal. This principle suggests that chaotic synchronization for two systems can be used as a way of filtering noisy chaotic signals.

The third configuration is as shown in Fig. 4.13, the x_1 variable is substituted for

y_1, but only in the equations governing the evolution of $y_2$and $y_3$and not y_1. Even with this partial substitution, however, the synchronization of the two systems is globally asymptotically stable. A subtraction of the relevant signals from the transmitter and receiver permits information signal recovery. To demonstrate how the information signal can be carried by a chaotic signal and still be perfectly recovered, a specific realization of the "inverse system" can be provided here. In this approach, an invertible function of transmitter dynamical variables and information signal is used to drive the receiver system.

The receiver is able to invert the function and recover the information signal because it synchronizes exactly to the transmitter. Again, the Lorenz model is used for the example provided here, although other chaotic systems can additionally be investigated. The transmitter, then, is just the modified Lorenz system:

$$\dot{x}_1 = \sigma(s - x_1) \tag{4.17}$$

$$\dot{x}_2 = rx_1 - x_2 - x_1x_3 \tag{4.18}$$

$$\dot{x}_3 = x_1x_2 - bx_3 \tag{4.19}$$

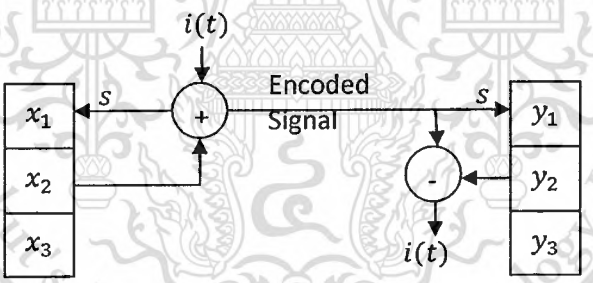

Fig. 4.13 Realization of the "inverse system" approach involving two Lorenz systems.

Where, as usual, $\sigma = 10, b = 8/3$, and $r = 28$. Also, the invertible function s has been chosen as:

$$s = x_2 + i(t) \tag{4.20}$$

Where the information signal is represented by $i(t)$. The second system has exactly the same form:

$$\dot{y}_1 = \sigma(s - y_1) \tag{4.21}$$

$$\dot{y}_2 = ry_1 - y_2 - y_1y_3 \tag{4.22}$$

$$\dot{y}_3 = y_1y_2 - by_3 \tag{4.23}$$

The configuration for this type of communication system is shown in Fig 4.13. The two systems synchronize exactly, allowing potentially perfect reconstruction of the information signal. The equations for the error dynamics, $e = x - y$ are

$$\dot{e}_1 = -\sigma e_1 \tag{4.24}$$

$$\dot{e}_2 = re_1 - e_2 - e_1 x_3 - e_3 x_1 \tag{4.25}$$

Clearly, $e_1 = 0$ as $t \to \infty$ and $e_1 = 0$ is a stable fixed point. With that fact the remaining eigenvalues (Lyapunov exponents), $\lambda_{2,3}$for $e_2$and e_3 are

$$\lambda_{2,3} = \frac{1}{2}(-(b+1) \pm \sqrt{(b+1)^2 - 4(b + x_1^2)}) \tag{4.26}$$

Stable synchronization of the two systems results if these Lyapunov exponents have negative real parts. This condition is met for all times if $b > 0$ because x_1^2 is always positive. Therefore, the systems are guaranteed to synchronize because the parameter $b = 8/3$. This proof of synchronization is not affected by the amplitude or frequency of the information signal. When these systems have synchronized, the information signal can be easily recovered by subtracting $y_2$from s.

Many researchers have sought to use chaotic signals as a means of sending secret information. Certainly, fundamental properties of chaotic systems seem to make them ideal for this purpose. Chaotic systems are inherently unpredictable. Their dynamic are aperiodic, and irregular. A small message added to or modulated onto unpredictable, aperiodic, and irregular waveforms can be difficult to decipher without a second chaotic system, identical to the first, which can synchronize to the transmitter.

Claude Shannon discussed three aspects of secret communication systems in his pioneering paper, "Communication Theory of Secrecy Systems," [108]: concealment, privacy, and encryption. These aspects can be interpreted in the context of chaotic communication. Firstly, the concealment of the information signal using chaotic carrier signals is possible because the carrier is irregular, aperiodic and noiselike. The presence of the information signal in the chaotic fluctuations may not be detected. Secondly the communication privacy occurs for systems in which special equipment is required to recover the information signal. This situation is present with the chaotic communication systems because an eavesdropper must have the proper receiver system, with matched parameter setting, to decrypt the message. Finally, the encryption occurs naturally in chaotic communication techniques. In conventional encryption techniques, a "key" is often used to encrypt the information signal. If the transmitter and receiver share the same key, the scrambled information signal can be recovered by the receiver. In chaotic systems, the transmitter's key itself acts as a "dynamical key." The receiver must be able to synchronize to the transmitter's dynamics which requires matched systems and

parameters in order to recover the information signal. Using a chaotic carrier to encrypt the information signal dynamically does not replace the use of more traditional encryption schemes as well. A chaotic signal, therefore, can act as an additional layer of the encryption for information that has already been encrypted by conventional encryption schemes.

4.6.2 Chaos-based Digital Communication Systems

In digital communication systems, each symbol is represented by a piece of sinusoidal signal, which is periodic. In chaos-based digital communication systems [106], each symbol is now denoted by a segment of chaotic signal, which is aperiodic. Therefore, even if the same symbol is being sent repeatedly, the chaotic signals representing the same symbol are never the same. We can broadly categorize chaos-based digital communication systems into those that require the regeneration of chaotic carriers at the receivers, namely coherent systems and those that do not have such a requirement, namely noncoherent systems. Although robust chaos synchronization techniques are not yet available, the study of coherent systems is important because it can provide useful benchmark for performance comparison. On the other hand, noncoherent systems are more practical.

4.6.2.1 Chaos Shift Keying

Chaos shift keying (CSK) [106] was first proposed by parlitz et al. and Dedieu et al. Fig. 4.14 shows the block diagram of the CSK digital communication system. To denote the bit duration by T_b, the transmitter consists of two chaos generator f and g, to produce signal $\hat{c}(t)$ and $\check{c}(t)$, repectively, during the l bit duration, i.e. $[(l-1)T_b, lT_b]$, if a binary "+1" is sent, $\hat{c}(t)$ is transmitted, and if "0" is sent, $\check{c}(t)$ is transmitted. Several demodulation algorithms have been proposed for the CSK system.

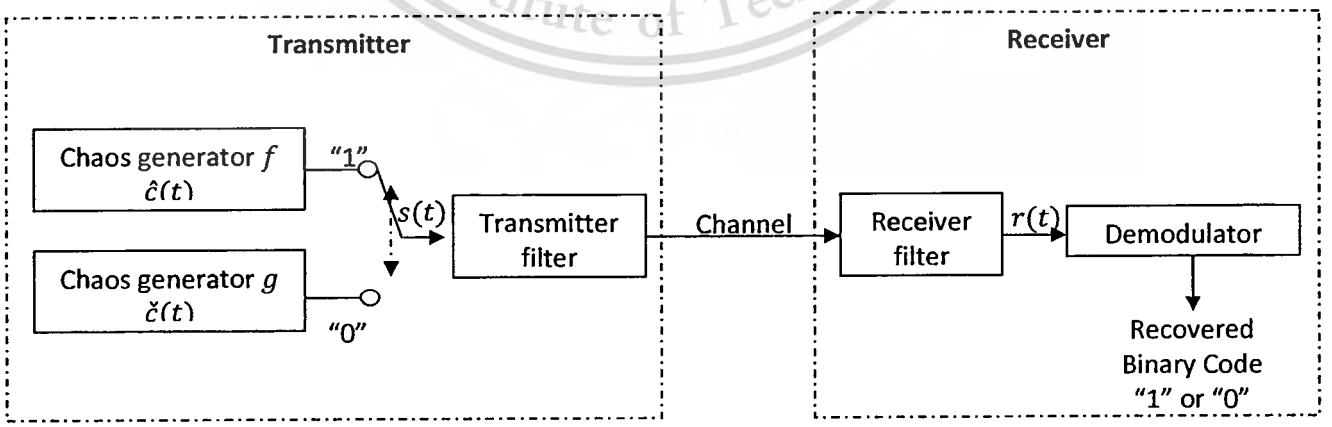

Fig. 4.14 CSK digital communication system.

1. Coherent Demodulation Based on Synchronization Error

In the original CSK systems [106] studied by Parlitz et al. and Dedieu et al., demodulation of the received signal is based on the self-synchronizing property of chaotic systems as shown in Fig. 4.15. The received signal is applied to drive two self-synchronization subsystems $\tilde{f}$ and $\tilde{g}$, which are matched to f and g, repectively. It is supposed that the channel is perfect and lossless as well as the filters at the transmitter and receiver are distortionless. If the signal $\hat{c}(t)$ has been transmitted, the subsystem $\tilde{f}$ will be synchronized with the incoming signal whereas $\tilde{g}$ will not, and vice versa. Therefore, by evaluating the difference (error) between the incoming signal and the output of the self-synchronization subsystems, the transmitted symbol can be estimated.

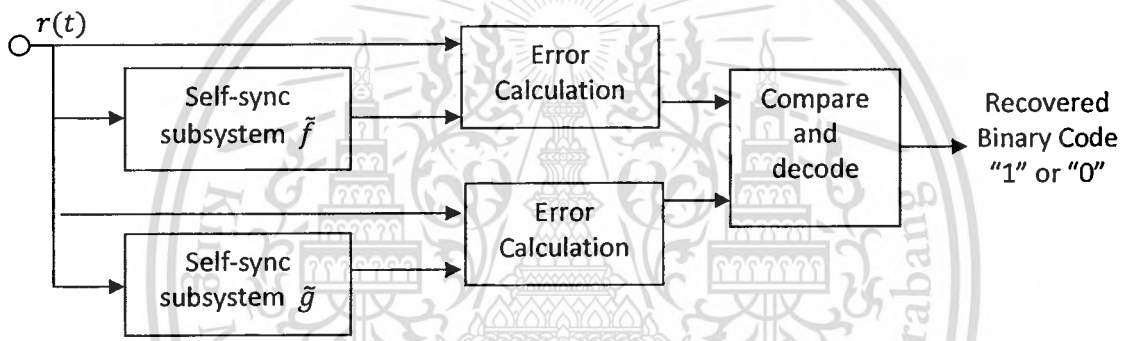

Fig. 4.15 Synchronization-error-based CSK demodulator.

2. Coherent Demodulation Based on Correlation.

In communications, the correlation function is generally used to evaluate the "likeness" between two signals [106]. In Fig 4.16, two synchronization circuits attempt to recover two chaotic signals $\hat{c}(t)$ and $\check{c}(t)$ from the incoming signal $r(t)$. Further, it is assumed that an acquisition time T_s is required for the synchronization blocks to lock to the incoming signal. The correlation of the reproduced chaotic signals and the incoming signal, implemented by a multiplier and an integrator, is then performed during the remainder of the bit duration. After that the outputs of the correlators are sampled and compared. If the input to the threshold detector, denoted by $y(lT_b)$, is positive, a "+1" is decoded for the lth symbol. Otherwise, a "0" is decoded.

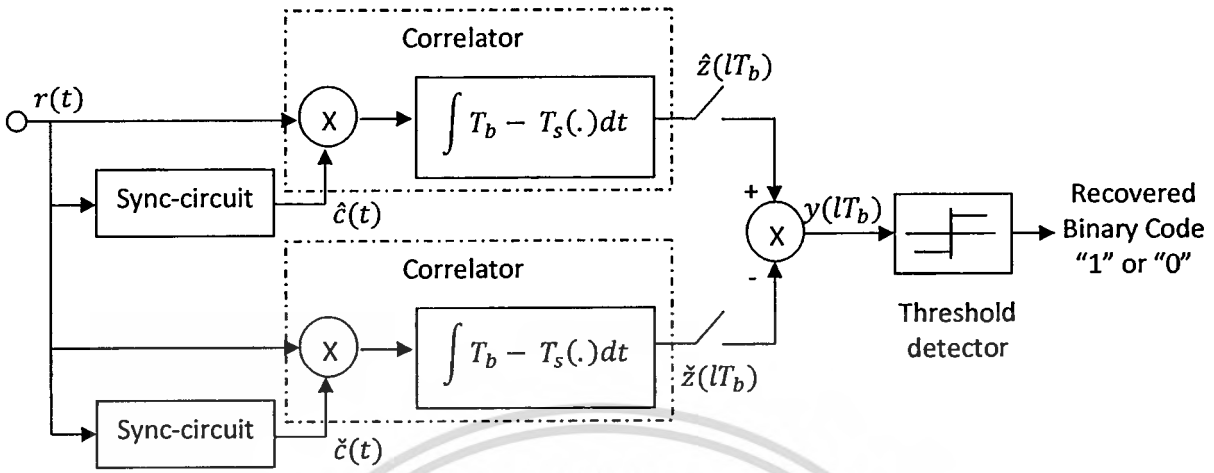

Fig. 4.16 Correlator-based coherent CSK demodulator.

We assume that the filters are distortionless and the synchronization time T_s is negligible compared to the bit period, we plot the histograms of $y(lT_b)$ for different SNRs as shown in Fig. 4.17. The value of $y(lT_b)$ is bound to vary even for the same symbol sent because of the aperiodicity of the chaotic signal. As shown in Fig 4.17, when the SNR is high, the two distinct regions in the histogram guarantee that the transmitted symbols can be decoded correctly. However, when the SNR is low, the two regions overlap and errors become unavoidable.

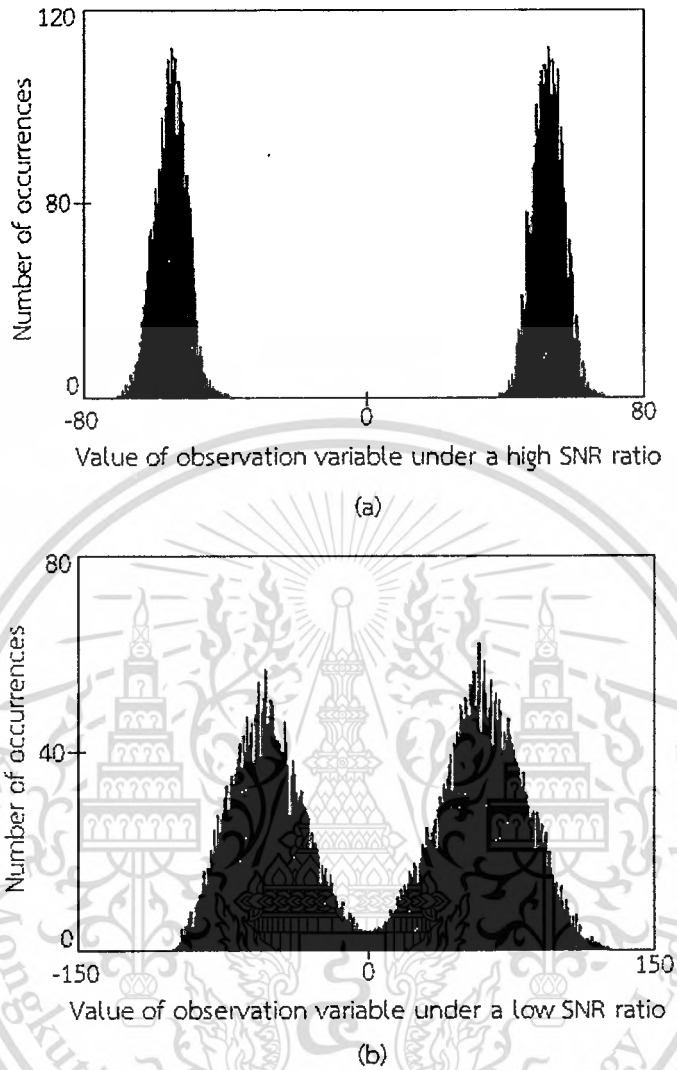

Fig. 4.17 Histograms of the observation variable $y(lT_b)$ for a coherent CSK system for (a) high SNR ratio, and (b) low SNR ratio.

3. Noncoherent Demodulation Based on Bit-Energy Estimation

In noncoherent CSK demodulation [106], the chaotic carriers are not recovered at the receiver. The signal recovery must be done based on some distinguishable property of the transmitted signals. One such property is the bit energy, which can be deliberately made different for different symbols in the modulation process. If a binary symbol "+1" is sent during the interval $[(l-1)T_b, lT_b]$, a chaotic signal $\hat{c}(t)$ with average bit energy $\hat{E}_c$ is transmitted, and if "0" is sent, a chaotic signal $\check{c}(t)$ with average bit energy $\check{E}_c$ is transmitted. We may use two chaos generators to produce chaotic signals with different average bit energies, or alternatively a single chaos generator can

be used to produce two chaotic signals of different bit energies with the use of two amplifiers of different gains as shown in Fig. 4.18.

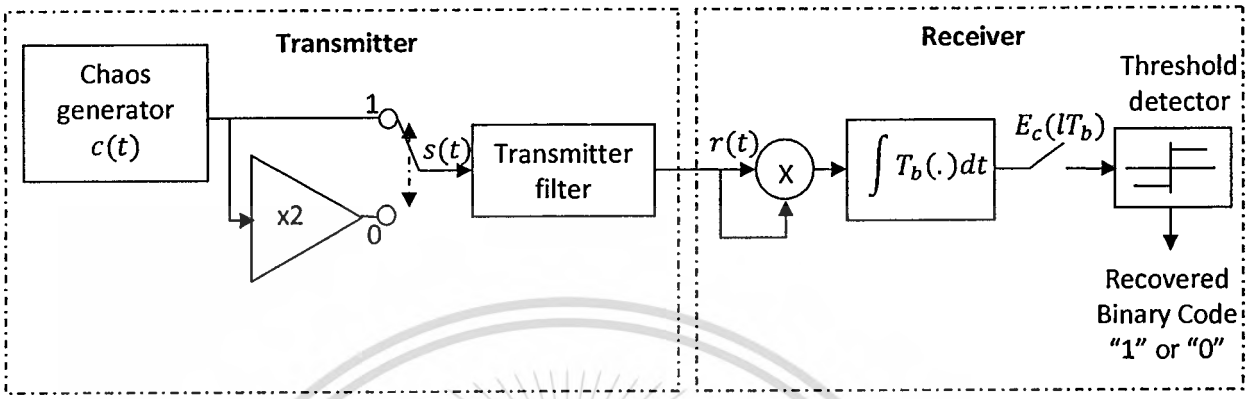

Fig. 4.18 CSK based on bit energy estimation.

At the receiver, the bit energy can be estimated by a square-and-integrate process as shown in Fig. 4.18. We assume that the additive noise is limited by the receiver's filter. Fig. 4.19 plots the histogram of the estimated bit energy $E_c(lT_b)$. In conventional modulation schemes, the bit energy is constant for a given symbol. However, in the CSK system, due to the aperiodicity of chaotic signals, the bit energy for the same symbol varies with time (i.e., varies from bit to bit), as illustrated by the histogram shown in Fig. 4.19a for the high SNR case. Note that $E_c(lT_b)$ does not show up as two distinct values in the histogram, but rather as clusters around the two average bit energies of the two chaotic signals with certain variances. By setting the threshold mid-way between the two average bit energies, the received symbols can be decoded correctly. For a moderate SNR environment, the calculated bit energies will generally be larger compared to the high SNR case because of the increase in noise energy. Fig. 4.19b shows the histogram begin to widen. As the two regions start overlapping with each other, bit errors begin to emerge. The optimal threshold is obviously dependent upon the SNR, this causes *threshold-shift* problem which is one of the drawbacks of this type of bit-energy-based noncoherent CSK system. In addition, the detection based on different bit energies can be easily achieved by eavesdroppers.

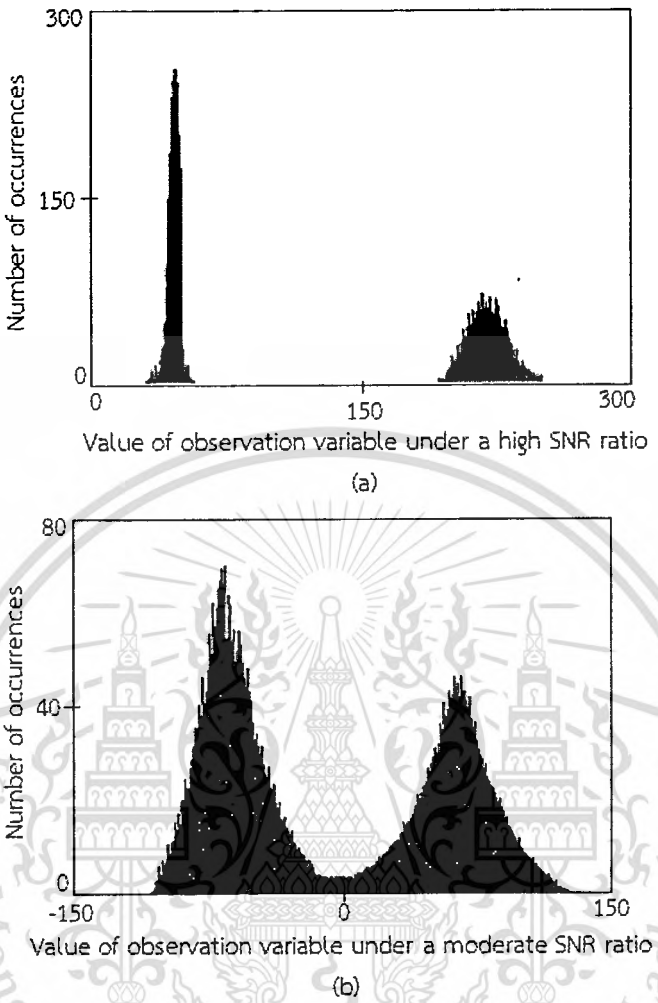

Fig. 4.19 Histograms of the received bit energy for a noncoherent CSK system for (a) high SNR, and (b) moderate SNR.

4.6.2.2 Differential Chaos Shift Keying

To address the threshold-shift problem for the noncoherent detection of a CSK system based on bit-energy estimation. In this section, we present the differential chaos-shift-keying (DCSK) modulation scheme, a modulation method that is primarily designed for noncoherent detection but the threshold level of the demodulator is fixed at zero.

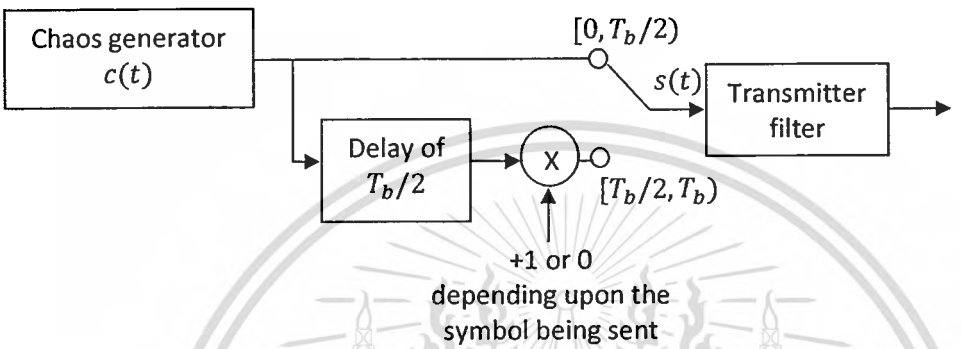

Fig. 4.20 DCSK modulator.

Fig. 4.20 shows a DCSK modulator. In this modulation scheme, every transmitted symbol is represented by two consecutive segments of chaotic signals. The first one serves as the reference (reference signal) whereas the second one carries the data (data-bearing signal). If a "+1" is sent, the data-bearing signal will be identical to the reference signal, and if a "0" is sent, an inverted version of the reference signal will be used as the data-bearing signal. Usually, the data-bearing signal sent follows the reference signal. Thus, for each of the symbol period, we have

$$s(t) = \begin{cases} c(t) & for\ 0 \le t < \frac{T_b}{2} \\ c\left(t - \frac{T_b}{2}\right) & for\ \frac{T_b}{2} \le t < T_b \end{cases} \tag{4.27}$$

If "+1" is sent, and

$$s(t) = \begin{cases} c(t) & for\ 0 \le t < \frac{T_b}{2} \\ -c\left(t - \frac{T_b}{2}\right) & for\ \frac{T_b}{2} \le t < T_b \end{cases} \tag{4.28}$$

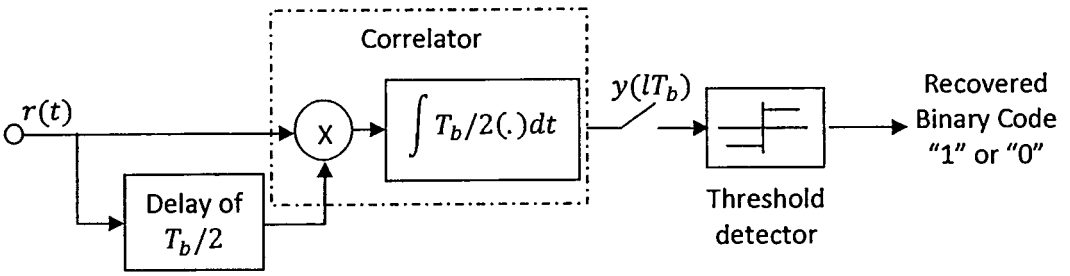

Fig. 4.21 DCSK demodulator

At the receiver, the correlation of the reference signal and the data-bearing signal is evaluated as shown in Fig. 4.21. Fig. 4.22a shows the statistical distribution of the correlator output under a high SNR environment. Note that the centers of the two clusters corresponding to the two symbols are located at equal distance from zero. Thus, by setting the threshold level to zero, it is sufficient to differentiate the two symbols. If the channel is noisy, however, the two clusters broaden and overlap each other, as shown in Fig. 4.22b. Under such a condition, errors are unavoidable but it is clear that the threshold remains at zero, which is an advantage over the noncoherent CSK detection scheme based on bit-energy detection. The main drawback of DCSK, however, is that its data rate is cut to half of the other systems because it spends half of the time transmitting the reference signals.

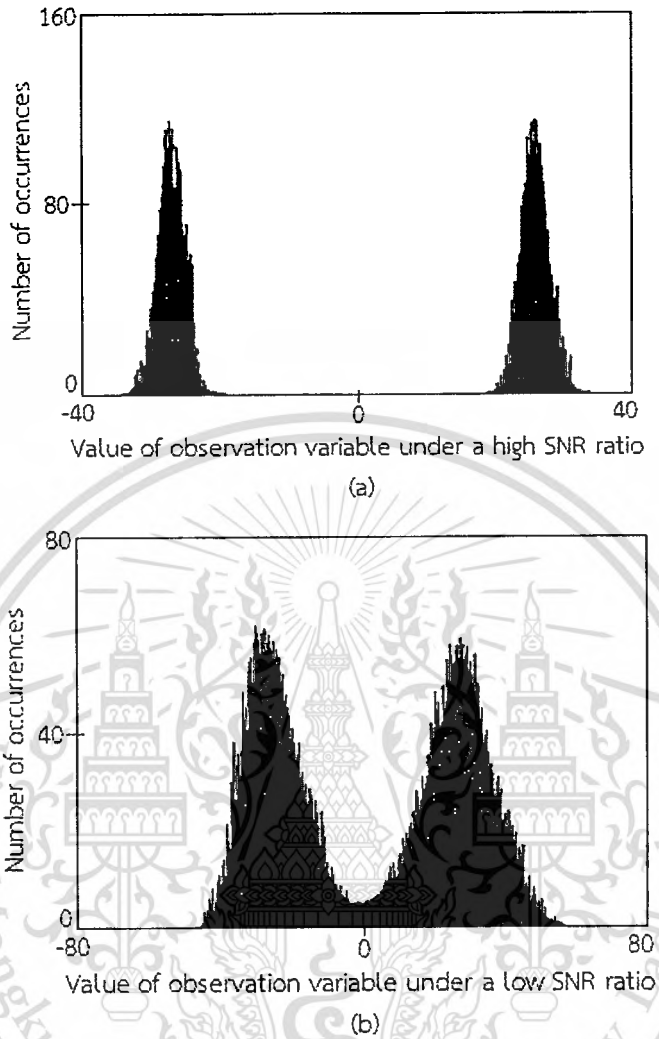

Fig. 4.22 Histogram of the observation variable $y(lT_b)$ for a DCSK system. (a) High SNR ratio; (b) low SNR ratio.

CHAPTER 5

SYSTEM DESIGN AND MODELING

5.1 Introduction

All optical devices are increasingly becoming important as integrated components for advanced optical applications and are widely used as optical sensor, signal processing, and optical communication. The communication security segment has been recognized as a promising tool for information that requires the security and privacy. Today, the security schemes, such as quantum and optical techniques, have been widely used in many applications such as sensors, computing, and optical communications. Recently, an optical device, known as a microring resonator in the form of an optical add/drop filter, has been found in many applications [11-13]. The authors have shown that the transmitted signals can be suppressed by the noiselike signals generated from the microring resonator. However, the search for new devices and techniques still remains. In this chapter, we present the use of the noiselike signal obtained from the dynamic behavior of the dark-bright soliton propagation and collision within the PANDA ring resonator for the high security communication. The secret key of the proposed optical cryptography system is inherently derived from the noiselike signal, and encryption and decryption keys are later derived from the secret key. The Optical Power Modulator and Optical Power Demodulator are used to encrypt and decrypt the information signal using the encryption and decryption keys, respectively. The necessary mathematical backgrounds, the system design and modeling, and simulation results of the proposed system are presented in this chapter.

5.2 Mathematical backgrounds of the used optical devices

The proposed system consists of four types of optical devices, namely PANDA ring resonator, optical add/drop filter, Optical Power Modulator and Optical Power Demodulator, as shown in Fig. 5.1, 5.2, and 5.3. The transmitter part of the proposed optical cryptography system consists of one PANDA ring resonator, two optical add/drop filters, and one Optical Power Modulator. The receiver consists of two optical add/drop filters, and one Optical Power Demodulator. The modified optical add/drop filter coupled with smaller left and right rings known as the PANDA ring resonator, and the optical add/drop filter, are shown in Fig. 5.1 and Fig. 5.2, respectively. To perform the dark-bright soliton propagation and collision within the PANDA ring resonator, the dark

and bright soliton pulses are first input into the PANDA ring resonator. The input optical field (E_{in}) and the control optical field (E_{con}) of the bright and dark soliton pulses are given by [109]

$$E_{in}(t) = Asech\left[\frac{T}{T_0}\right] exp\left[\left(\frac{z}{2L_D}\right) - i\omega_0 t\right] \quad (5.1)$$

$$E_{con}(t) = Atanh\left[\frac{T}{T_0}\right] exp\left[\left(\frac{z}{2L_D}\right) - i\omega_0 t\right] \quad (5.2)$$

Where A and z are the optical field amplitude and propagation distance, respectively. T is a soliton pulse propagation time in a frame moving at the group velocity, $T = t - \beta_1.z$, where β_1 and β_2 are the coefficients of the linear and second-order terms of Taylor expansion of the propagation constant. $L_D = T_0^2/|\beta_2|$ is the dispersion length of the soliton pulse. T_0 is the soliton pulse propagation time at initial input (or soliton pulse width), where t is the soliton phase shift time, and the frequency shift of the soliton is ω_0. This solution describes a pulse that keeps its temporal width invariance as it propagates, and thus is called a temporal soliton. When the soliton peak intensity ($|\beta_2/\Gamma T_0^2|$) is given, then T_0 is known. For the soliton pulse in the microring device, a balance should be achieved between the dispersion length (L_D) and the nonlinear length ($L_{NL} = 1/\Gamma\phi_{NL}$), where $\Gamma = n_2 k_n$, is the length scale over which dispersive or nonlinear effect makes the beam become wider or narrower. For a soliton pulse, there is a balance between dispersion and nonlinear lengths, hence $L_D = L_{NL}$.

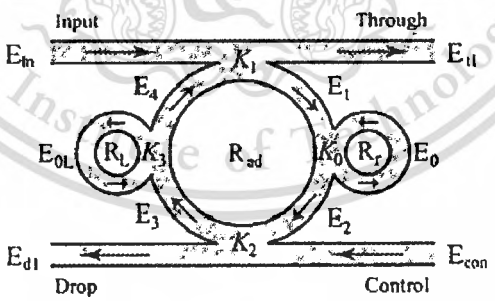

Fig. 5.1 Schematic diagram of PANDA ring resonator.

The PANDA ring resonator shown in Fig. 5.1 is used for the noiselike signal generation. When the input light pulse passes through the first optical coupler, the transmitted and circulated optical fields can be written as [110]

$$E_{t1} = \sqrt{1-\gamma_1}\left[\sqrt{1-\kappa_1}E_{in} + j\sqrt{\kappa_1}E_4\right] \quad (5.3)$$

$$E_1 = \sqrt{1-\gamma_1}\left[\sqrt{1-\kappa_1}E_4 + j\sqrt{\kappa_1}E_{in}\right] \quad (5.4)$$

$$E_2 = E_0 E_1 e^{-\frac{aL}{22} - jk_n\frac{L}{2}} \quad (5.5)$$

Where κ_1 is the intensity coupling coefficient, γ_1 is the fractional coupler intensity loss (or coupling loss), α is the attenuation coefficient, $k_n = 2\pi/\lambda$ is the wave propagation number, λ is the input wavelength light field, and $L = 2\pi R_{ad}$, R_{ad} is the radius of the central ring.

The optical fields at the second coupler are given by

$$E_{d1} = \sqrt{1-\gamma_2}\left[\sqrt{1-\kappa_2}E_{con} + j\sqrt{\kappa_2}E_2\right] \quad (5.6)$$

$$E_3 = \sqrt{1-\gamma_2}\left[\sqrt{1-\kappa_2}E_2 + j\sqrt{\kappa_2}E_{con}\right] \quad (5.7)$$

$$E_4 = E_{0L}E_3 e^{-\frac{aL}{22} - jk_n\frac{L}{2}} \quad (5.8)$$

Where κ_2 is the intensity coupling coefficient, γ_2 is the fractional coupler intensity loss (or coupling loss). The circulated light fields, E_0 and E_{0L} , are the light field circulated components of the microring radii, R_r and R_L, which couple into the right-hand side (RHS) and left-hand side (LHS) microrings of the PANDA ring resonator, respectively. The light field transmitted and circulated components on the RHS microring radius, R_r, are given by

$$E_2 = \sqrt{1-\gamma_0}\left[\sqrt{1-\kappa_0}E_1 + j\sqrt{\kappa_0}E_{r2}\right] \quad (5.9)$$

$$E_{r1} = \sqrt{1-\gamma_0}\left[\sqrt{1-\kappa_0}E_{r2} + j\sqrt{\kappa_0}E_1\right] \quad (5.10)$$

$$E_{r2} = E_{r1}e^{-\frac{\alpha}{2}L_1 - jk_nL_1} \quad (5.11)$$

Where κ_0 is the intensity coupling coefficient, γ_0 is the fractional coupler intensity loss (or coupling loss), α is the attenuation coefficient, $k_n = 2\pi/\lambda$ is the wave propagation number, λ is the input wavelength light field, and $L_1 = 2\pi R_r$, R_r is the radius of RHS microring. From Eqs.(5.9)–(5.11), the circulated roundtrip light fields of the RHS microring radius, R_r, are given in Eqs.(5.12) and (5.13), respectively,

$$E_{r1} = \frac{j\sqrt{1-\gamma_0}\sqrt{\kappa_0}E_1}{1-\sqrt{1-\gamma_0}\sqrt{1-\kappa_0}e^{-\frac{\alpha}{2}L_1-jk_nL_1}} \tag{5.12}$$

$$E_{r2} = \frac{j\sqrt{1-\gamma_0}\sqrt{\kappa_0}E_1e^{-\frac{\alpha}{2}L_1-jk_nL_1}}{1-\sqrt{1-\gamma_0}\sqrt{1-\kappa_0}e^{-\frac{\alpha}{2}L_1-jk_nL_1}} \tag{5.13}$$

Thus, the output circulated light field, E_0, for the RHS microring is given by

$$E_0 = E_1\left\{\frac{\sqrt{1-\gamma_0}\sqrt{1-\kappa_0}-(1-\gamma_0)e^{-\frac{\alpha}{2}L_1-jk_nL_1}}{1-\sqrt{1-\gamma_0}\sqrt{1-\kappa_0}e^{-\frac{\alpha}{2}L_1-jk_nL_1}}\right\} \tag{5.14}$$

Similarly, the output circulated light field, E_{0L}, for the LHS microring is given by:

$$E_{0L} = E_3\left\{\frac{\sqrt{1-\gamma_3}\sqrt{1-\kappa_3}-(1-\gamma_3)e^{-\frac{\alpha}{2}L_2-jk_nL_2}}{1-\sqrt{1-\gamma_3}\sqrt{1-\kappa_3}e^{-\frac{\alpha}{2}L_2-jk_nL_2}}\right\} \tag{5.15}$$

where κ_3 is the intensity coupling coefficient, γ_3 is the fractional coupler intensity loss, α is the attenuation coefficient, $k_n = 2\pi/\lambda$ is the wave propagation number, λ is the input wavelength light field, and $L_2 = 2\pi R_L$, $R_L$is the radius of the LHS microring. From Eqs.(5.3)–(5.15), the circulated light fields, E_1, E_3, and E_4 are defined by given $x_1 = \sqrt{1-\gamma_1}$, $x_2 = \sqrt{1-\gamma_2}$, $y_1 = \sqrt{1-\kappa_1}$, and $y_2 = \sqrt{1-\kappa_2}$. Thus,

$$E_1 = \frac{jx_1\sqrt{\kappa_1}E_{in}+jx_1x_2y_1\sqrt{\kappa_2}E_{0L}E_{con}e^{-\frac{\alpha L}{22}-jk_n\frac{L}{2}}}{1-x_1x_2y_1y_2E_0E_{0L}e^{-\frac{\alpha}{2}L-jk_nL}} \tag{5.16}$$

$$E_3 = x_2y_2E_0E_1e^{-\frac{\alpha L}{22}-jk_n\frac{L}{2}} + jx_2\sqrt{\kappa_2}E_{con} \tag{5.17}$$

$$E_4 = x_2y_2E_0E_{0L}E_1e^{-\frac{\alpha}{2}L-jk_nL} + jx_2\sqrt{\kappa_2}E_{0L}E_{con}e^{-\frac{\alpha L}{22}-jk_n\frac{L}{2}} \tag{5.18}$$

From Eqs.(5.3), (5.5), and (5.16)–(5.18), the output optical field of the through port (E_{t1}) can be expressed as:

$$E_{t1} = x_1y_1E_{in} + \begin{pmatrix} jx_1x_2y_2\sqrt{\kappa_1}E_0E_{0L}E_1 \\ -x_1x_2\sqrt{\kappa_1\kappa_2}E_{0L}E_{i2} \end{pmatrix} e^{-\frac{\alpha L}{22}-jk_n\frac{L}{2}} \tag{5.19}$$

The output power at the through port (P_{t1}) is written by

$$P_{t1} = (E_{t1}) \cdot (E_{t1})^* = |E_{t1}|^2 \tag{5.20}$$

Similarly, from Eqs. (5.5), (5.6), and (5.16)–(5.18), the output optical field of the drop port (E_{d1}) is given by

$$E_{d1} = x_2 y_2 E_{con} + jx_2\sqrt{\kappa_2} E_0 E_1 e^{-\frac{\alpha L}{22} - jk_n \frac{L}{2}} \tag{5.21}$$

The output power at the drop port (P_{d1}) is expressed by

$$P_{d1} = (E_{d1}) \cdot (E_{d1})^* = |E_{d1}|^2 \tag{5.22}$$

The add/drop optical filter device with the appropriate parameters is shown in Fig. 5.2. The electric field detected at the through port is given by [111]

$$E_{t2} = E_{t1} \left\{ \frac{-\sqrt{1-\kappa_4} e^{-\frac{\alpha}{2} L_b - jk_n L_b} + \sqrt{1-\kappa_4}}{1-\sqrt{1-\kappa_4}\sqrt{1-\kappa_5} e^{-\frac{\alpha}{2} L_b - jk_n L_b}} \right\} \tag{5.23}$$

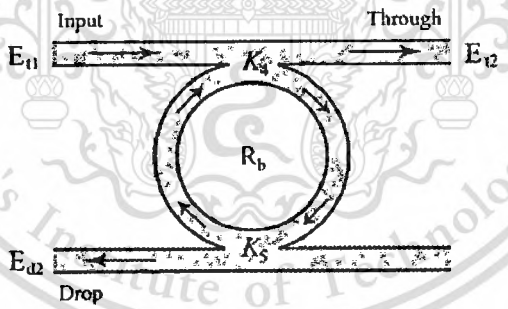

Fig. 5.2 Schematic diagram of the add/drop filter.

Where $L_b = 2\pi R_b$, R_b is the radius of the add/drop optical filter as shown in Fig. 5.2 The output power at the drop port (P_{t2}) is expressed by

$$P_{t2} = (E_{t2}) \cdot (E_{t2})^* = |E_{t2}|^2 \tag{5.24}$$

The electric field detected at the drop port is given by

$$E_{d2} = E_{t1}\left\{\frac{-\sqrt{\kappa_4\kappa_5}e^{-\frac{\alpha L_b}{2}\frac{}{2}-jk_n\frac{L_b}{2}}}{1-\sqrt{1-\kappa_4}\sqrt{1-\kappa_5}e^{-\frac{\alpha}{2}L_b-jk_nL_b}}\right\} \quad (5.25)$$

The output power at the drop port (P_{d2}) is expressed by

$$P_{d2} = (E_{d2}).(E_{d2})^* = |E_{d2}|^2 \quad (5.26)$$

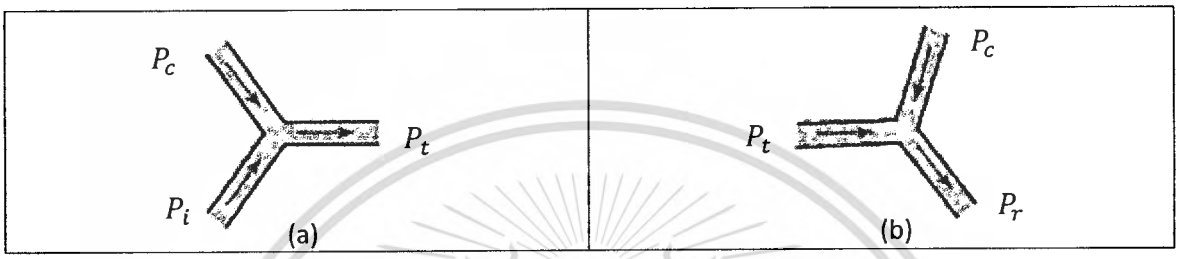

Fig. 5.3 Schematic diagram of (a) Optical Power Modulator and (b) Demodulator.

The proposed system uses the Optical Power Modulator as shown in Fig. 5.3a to combine (modulate) the signal power of the input signal with the signal power of the noiselike signal. For simplification, considering the signal power of the output signal (P_t) which is equal to the signal power of the input signal (P_i) plus the signal power of the noiselike signal (P_c), the signal power detected at the output is given by [112]

$$P_t = P_i + P_c \quad (5.27)$$

The Optical Power Demodulator as shown in Fig. 5.3b is used to demodulate the original input signal from the received signal. For simplification, considering the signal power of the output signal (P_r) which is equal to the signal power of the received signal (P_t) minus the signal power of the noiselike signal (P_c), the signal power detected at the output is given by [112]

$$P_r = P_t - P_c \quad (5.28)$$

5.3 The system design

Fig. 5.4 shows the schematic diagram of the proposed optical cryptography system, where PA refers to the PANDA ring resonator, AD1-AD4 are the add/drop filters, OPM is the Optical Power Modulator and OPD is the Optical Power Demodulator. The transmitter part consists of PA, AD1, AD2 and OPM. For the noiselike signal generation, the bright soliton pulse (E_{in}) and dark soliton pulse (E_{con}) are input to the PA at the input and control ports, respectively. The output signal (E_{t1}) obtained at the through port of the PA is the noiselike signal which is then sent to the receiver for the noise synchronization as shown in Fig. 5.4. The noiselike signal is later input to the AD1 in order to form the secret key (E_{t2}) at the through port of AD1, and then the secret key (E_{t2}) is input to the AD2 in order to generate the encryption and decryption keys at the through and drop ports of the AD2, respectively. Finally the OPM encrypts the information signal using the encryption key.

The receiver part consists of AD3 and AD4 and OPD. The synchronized noiselike signal (E_{t1}) is similarly input to the AD3, and then the secret key (E_{t2}) obtained at the through port is sent to the AD4 in order to generate the decryption and encryption keys at the through and drop ports of the AD4, respectively. Finally the OPD decrypts the ciphertext using the decryption key.

Our proposed system can be claimed as a new optical cryptography technique, which the transmitted information signal can be converted to the noiselike signal using the additive masking approach prior to sending it to the receiver. Furthermore, the higher security communication can be achieved by frequently changing the noiselike signal.

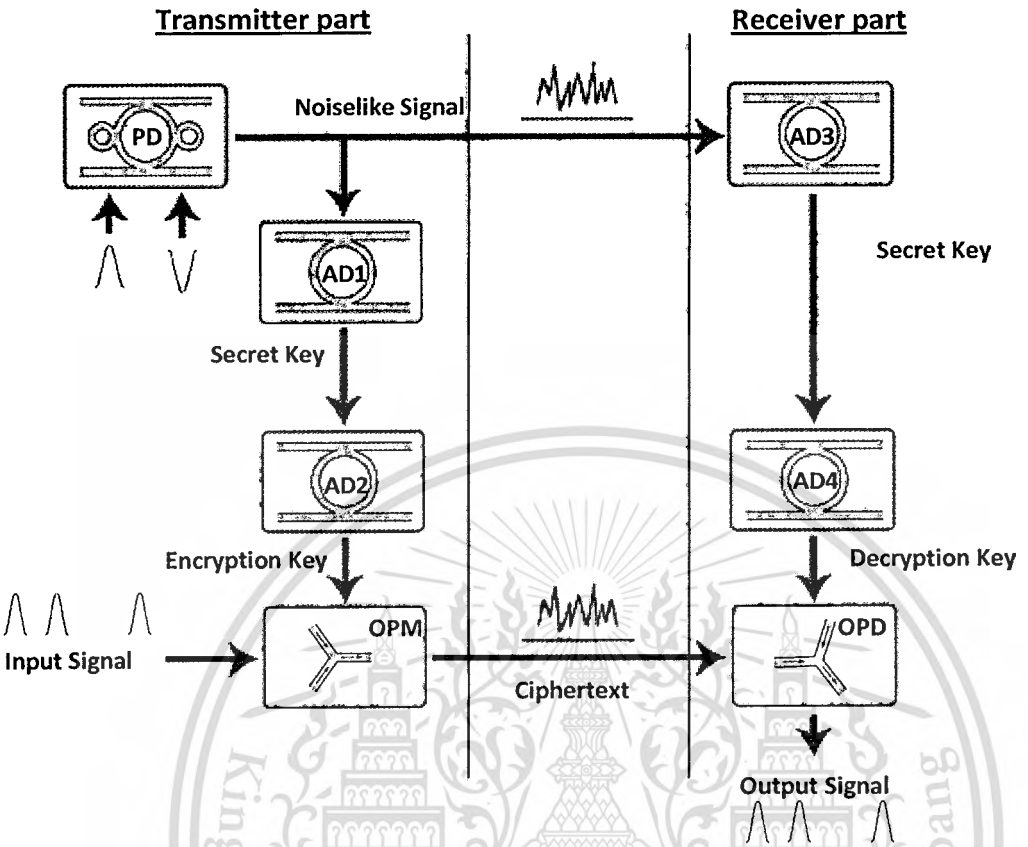

Fig. 5.4 Schematic diagram of the proposed optical cryptography system.

5.3.1 Noiselike Signal Generation

In the simulation of the noiselike signal generation, the used parameters of the PANDA ring resonator are fixed as shown in Table 5.1 [113]. In order to confirm that the noiselike signal generation is possible to be fabricated [14], only the practical device parameters are used in the simulation. Additionally, the simulation results of the noiselike signal generation are at the center wavelength (λ_0) 1.55 μm which is the most popular center wavelength used in the optical communication.

Table 5.1 The used parameters of the PANDA ring resonator.

Parameters of PANDA ring resonator	Value
Material type	InPGaAsP/InP
Linear refractive index : n_0	3.4
Nonlinear refractive index : n_2	2×10^{-15}
Ring radius of the center ring : R_{ad}	200 μm
Ring radius of the right ring : R_r	100 μm
Ring radius of the left ring : R_l	100 μm
Coupling coefficient : κ_0, κ_1, κ_2, and κ_3	0.2
Coupling loss : γ_0, γ_1, γ_2, and γ_3	0.15
Attenuation coefficient (α) of the center ring	50
Attenuation coefficient (α) of the right ring	100
Attenuation Coefficient (α) of the left ring	100
Effective core area : A_{eff}	0.25×10^{-12}

Table 5.2 shows the characteristic of the input dark and bright soliton pulses.

Parameters	Bright Soliton	Dark Soliton
Signal power	1 W	1.5 W
Center wavelength	1.55 μm	1.55 μm
Full Width Half Maximum (FWHM)	115 nm	8 nm

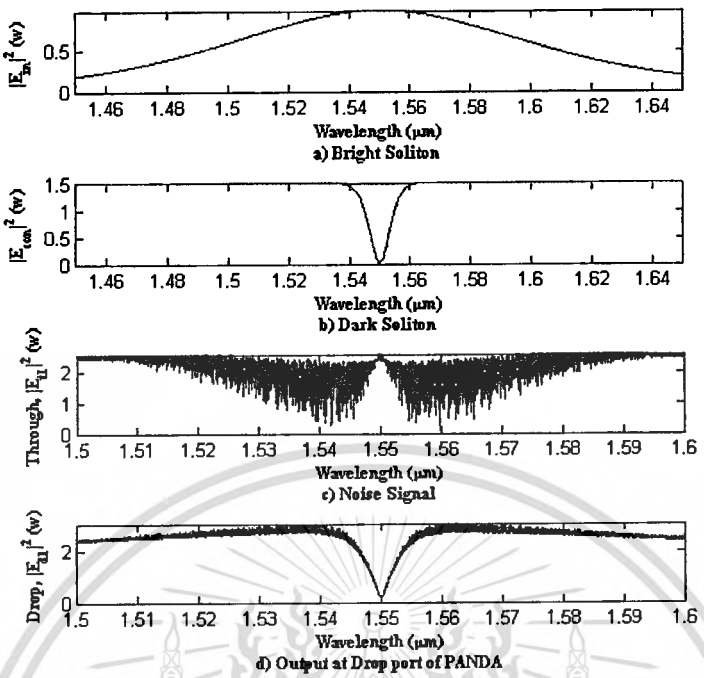

Fig. 5.5 shows the simulation results of the noiselike signal generation module.

Fig. 5.5 shows the simulation results of the noiselike signal generation part. Fig. 5.5(a) shows the bright soliton pulse with 1 W peak power that is continuously input to the PANDA ring resonator at the input port. Fig. 5.5(b) shows the dark soliton pulse with 1.5 W peak power that is continuously input to the PANDA ring resonator at the control port. Fig. 5.5(c) shows the output power at the through port which is the noiselike signal continuously generated from the dynamic behavior of the dark-bright soliton propagation and collision within the PANDA ring resonator. The obtained noiselike signal is then sent to the receiver, also known as the noise synchronization, in which the receiver is now synchronized with the transmitter. The noiselike signal is next used as the input signal for the secret key generation part in the next step. The peak power of the output signals at the through port and drop port is increased to 2.3 and 2.5 W, respectively which they are larger than the input soliton pulses due to the optical nonlinear (Kerr) effects. Fig. 5.5(d) shows the output power at the drop port.

5.3.2 Secret Key Generation

The same noiselike signal is input to the AD1 at the transmitter part and AD3 at the receiver part causing the same secret key is generated on both sides. Both AD1 and AD3 generate the secret key at the through port. Fig. 5.6 shows the simulation results of the secret key generation part where the used parameters are fixed to be as shown in the Table 5.3. Fig. 5.6(a) shows the noiselike signal received at the input port, Fig. 5.6(b)

shows the output power at the through port of the AD1 and AD3 which is the secret key. Fig. 5.6(c) shows the output power at the drop port of the AD1 and AD3 which will not be used any more in this thesis.

Table 5.3 The used parameters for the Add/drop filters : AD1 and AD3

Parameters of the AD1 and AD3	Value
Refractive Index : n	3.4
Ring radius : R	100 μm
Coupling coefficient : κ_1 , and κ_2	0.2
Attenuation coefficient : α	100

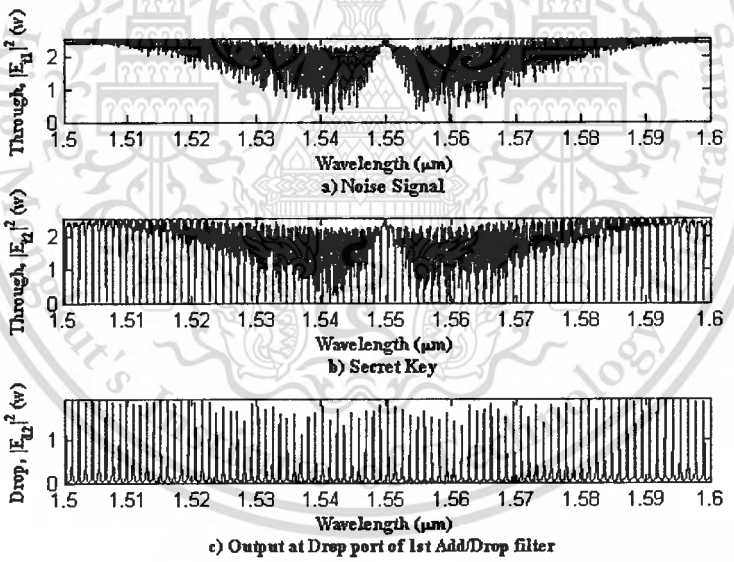

Fig. 5.6 shows the simulation results of the secret key generation module.

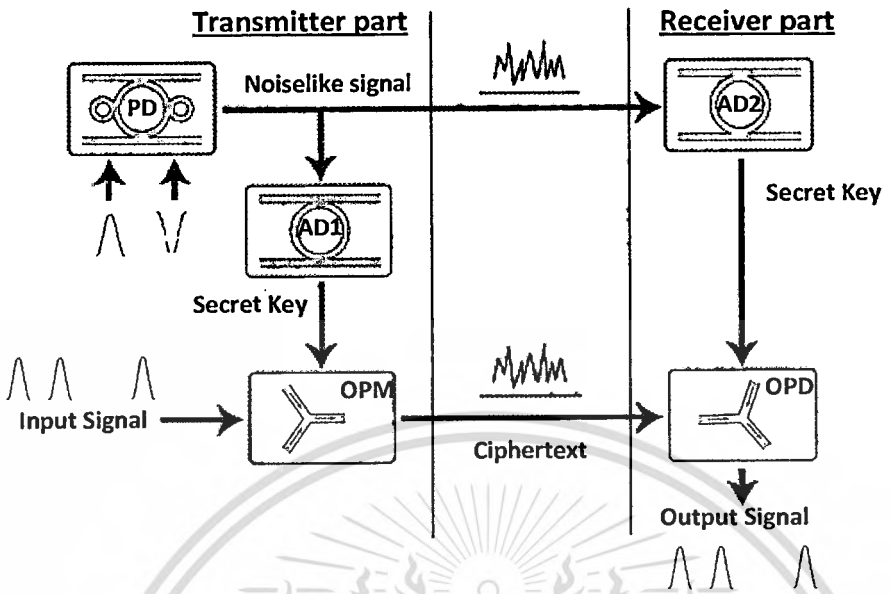

Fig. 5.7 shows a simple cryptography system.

We can simply mask the input information signal by the secret key generated from the AD1 as shown in Fig. 5.7 which its ciphertext is shown in Fig. 5.8 (c) , but in this case both transmitter and receiver have to use the same key (same secret key) to encrypt and decrypt the information signal. For the higher security, in the final design, the transmitter and receiver will use the different encryption keys which will be described later on the next section.

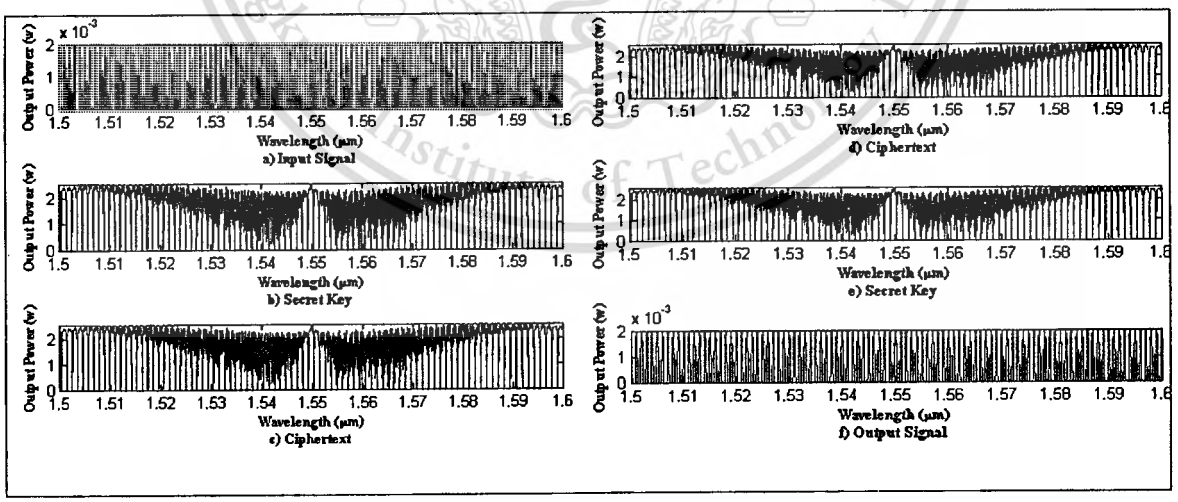

Fig. 5.8 shows the information signal masked by the secret key.

5.3.3 Encryption and Decryption Keys generation

The secret key obtained from the previous step is input to the AD2 and AD4 for generating the encryption and decryption keys. In the transmitter part, the encryption and decryption keys are generated at the through and drop ports of the AD2 respectively. On the other hand, for the receiver part, the encryption key is generated at the drop port and decryption key is generated at the through port of the AD4. Finally the OPM uses the encryption key to encrypt the information signal by using the additive masking approach and OPD uses the decryption key to decrypt the information signal which now the secure communication is performed. The receiver will use the different encryption key from the transmitter to encrypt its information signal prior to sending it to the transmitter which the transmitter can recover the information signal of the receiver by using its decryption key. The Table 5.4 shows the used parameters of the AD2 and AD4.

The proposed cryptography system is designed to secure the information sent over the Dense Wavelength-Division Multiplexing (DWDM). The DWDM involves sending a large number of closely spaced optical signals over a single fiber. Standards developed by the ITU (International Telecommunications Union) [114] define the exact optical wavelength used for DWDM applications. The standard channel spacing is 200 GHz and 100 GHz which relates to the optical wavelength as follows: A spacing of 200 GHz corresponds to about 1.6 nm, and 100 GHz corresponds to about 0.8 nm channel spacing. For simplification and easy-to- analyze, we will use the channel spacing 1 nm in our simulation which is in the range of 0.8 and 1.6 nm. We will also demonstrate in the next chapter that our proposed cryptography system can secure (bury) the information even the channel spacing is bigger or smaller than 1 nm. The Table 5.5 shows the characteristic of the input information signal used in the simulation.

Table 5.4 The used parameters for the Add/drop filters : AD2 and AD4.

Parameters of the AD2 and AD4	Value
Refractive Index : n	3.4
Ring radius : R	300 μm
Coupling coefficient : κ_1 , and κ_2	0.1
Attenuation coefficient : α	0

Table 5.5 shows the characteristic of the input information signal used in the simulation.

Parameters	Value
Signal Power	0.002 W
Channel spacing	1 nm
Full Width at Half Maximum (FWHM)	0.4 nm

Fig. 5.9I. shows the encryption and decryption keys of the transmitter and Fig 5.9II shows the decryption and encryption keys of the receiver. Fig. 5.9I(a) and II(a) are the secret key. Fig. 5.9I(b) and II(c) show the encryption keys of the transmitter and receiver, respectively. Fig. 5.9I(c) and II(b) show the decryption key of the transmitter and receiver, respectively.

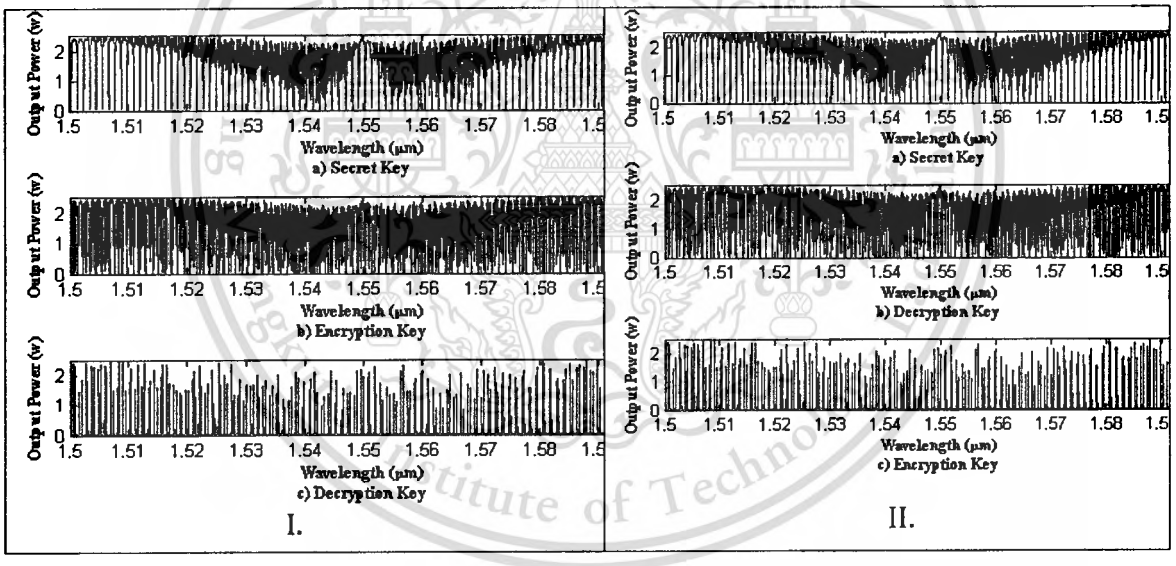

Fig. 5.9 shows the encryption and decryption keys of both sides.

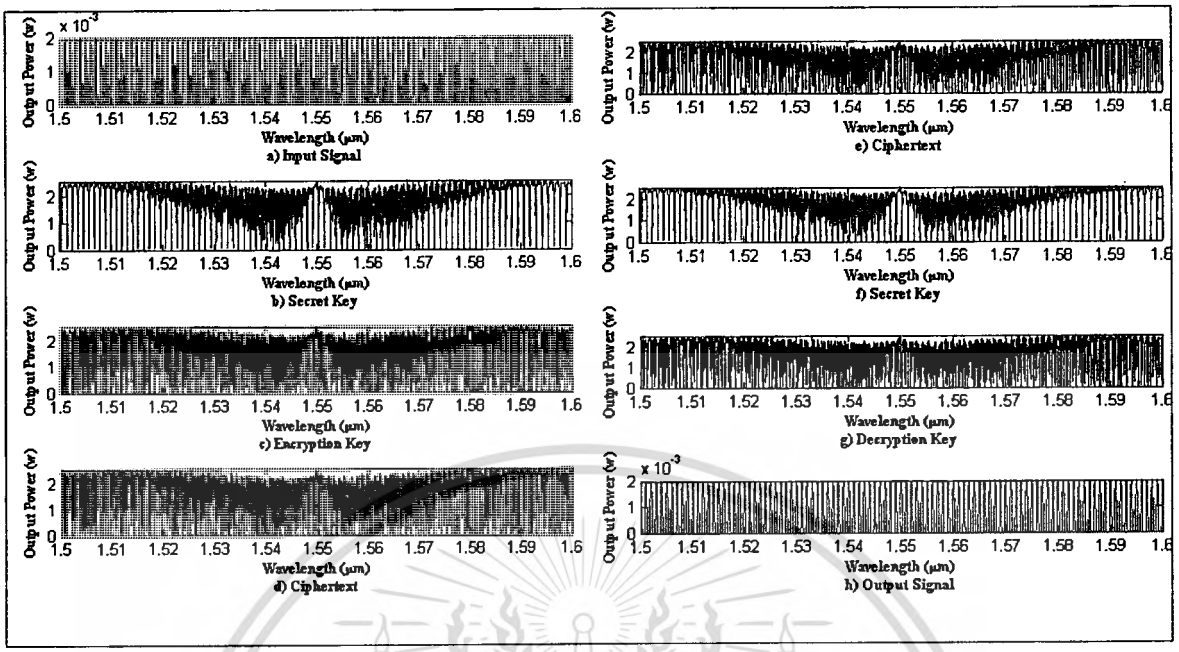

Fig. 5.10 shows the secure communication from the transmitter to the receiver.

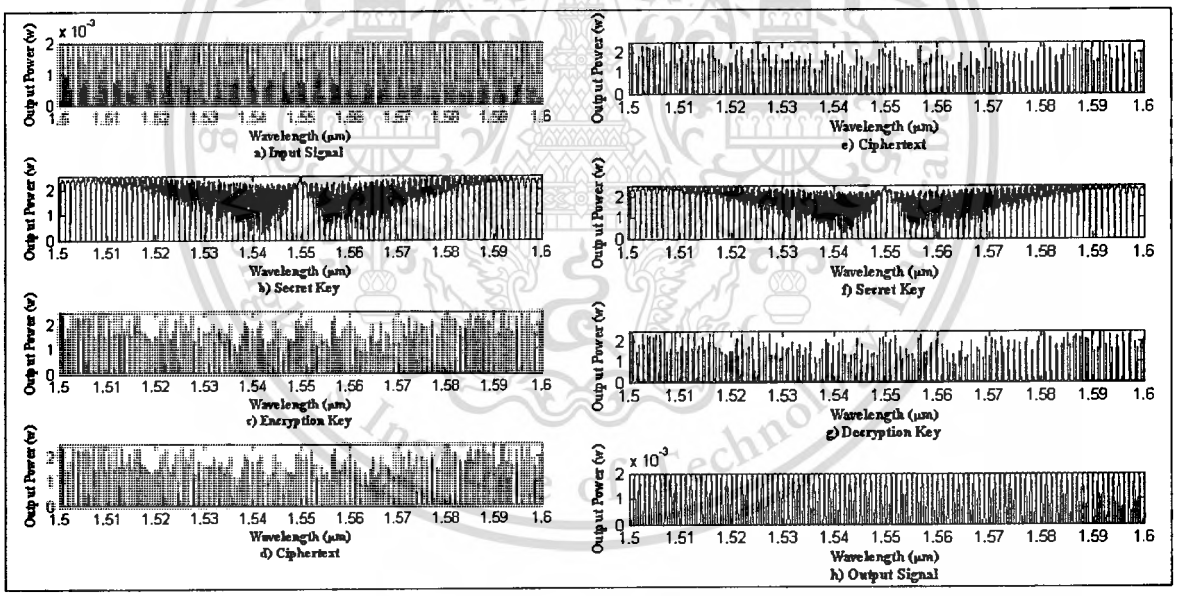

Fig. 5.11 shows the secure communication from the receiver to the transmitter.

Fig. 5.10 and Fig 5.11 show the overall simulation results of the secure communication between the transmitter and receiver. Fig. 5.10(d) shows the ciphertext generated by the transmitter using its encryption key (Fig. 5.10(c)) , the receiver uses its decryption key as shown in Fig. 5.10(g) to recover the original information signal. Similarly, Fig. 5.11(d) shows the ciphertext generated by the receiver using its encryption

key (Fig. 5.11(c)) , the transmitter uses its decryption key as shown in Fig. 5.11(g) to decrypt the ciphertext. The output signals are shown in Fig. 5.10(h) and Fig. 5.11(h).

CHAPTER 6

MATHEMATICAL SIMULATION

6.1 Mathematical simulation

In order to evaluate the proposed optical cryptography system, the following experiments are conducted.

1. Changing the channel spacing.
2. Generating the new noiselike signal.
3. Secret key mismatches.
4. Decryption key mismatches.
5. Changing the power (intensity) of the input pulses.
6. Changing the input pulses.
7. Rekeying at every time T.
8. Decrypting the ciphertext by the old decryption key after rekeying.

We simulate the proposed optical cryptography system using MathLAB program, the simulation results of all experiments are also presented as below in detail.

6.1.1 Experiment 1 – Changing the channel spacing.

Our proposed cryptography system is designed to secure the information sent over the DWDM, so we generally use the channel spacing equal to 1 nm for the simulations as mentioned in the previous chapter, however, it is possible to use the channel spacing wider or narrower than 1 nm as well in some specific systems. This experiment is conducted to demonstrate that our proposed system is not affected by the change of the channel spacing, it still can bury the input information signal into the noiselike signal in order to form the secure communication. In this experiment, we conduct two tests (Test 1 and Test 2). Test 1 uses the channel spacing = 0.5 nm and the Test 2 uses the channel spacing = 2 nm as shown in Fig. 6.1(a) and Fig. 6.2(a), respectively. Table 6.1 shows the used parameters of the PANDA ring resonator in the noiselike signal generation module. Table 6.2 shows the characteristic of the input dark and bright soliton pulses that are input to the noiselike signal generation module for the noiselike signal generation. Table 6.3 shows the used parameters of the Add/drop filters in the secret key generation module, the AD1 and AD3. Table 6.4 shows the used parameters of the Add/drop filters in the encryption-decryption keys generation module,

the AD2 and AD4. Table 6.5 shows the characteristic of the input information signal used in the Test 1 and Test 2.

Table 6.1 shows the used parameters of the PANDA ring resonator.

Parameters of PANDA ring resonator	Value
Material Type	InPGaAsP/InP
Linear refractive index : n_0	3.4
Nonlinear refractive index : n_2	2×10^{-15}
Ring radius of the center ring : R_{ad}	200 μm
Ring radius of the right ring : R_r	100 μm
Ring radius of the left ring : R_l	100 μm
Coupling coefficient : κ_0, κ_1, κ_2, and κ_3	0.2
Coupling loss : γ_0, γ_1, γ_2, and γ_3	0.15
Attenuation coefficient (α) of the center ring	50
Attenuation coefficient (α) of the right ring	100
Attenuation coefficient (α) of the left ring	100
Effective core area : A_{eff}	0.25×10^{-12}

Table 6.2 shows the characteristic of the input dark and bright soliton pulses used for the noiselike signal generation.

Parameters	Bright Soliton	Dark Soliton
Signal power	1 W	1.5 W
Center wavelength	1.55 μm	1.55 μm
Full Width Half Maximum (FWHM)	115 nm	8 nm

Table 6.3 shows the used parameters of the Add/drop filters, the AD1 and AD3.

Parameters of the AD1 and AD3	Value
Refractive Index : n	3.4
Ring radius : R	100 μm
Coupling coefficient : κ_4 , and κ_5	0.2
Attenuation coefficient : α	100

Table 6.4 shows the used parameters of the Add/drop filters, the AD2 and AD4.

Parameters of the AD2 and AD4	Value
Refractive Index : n	3.4
Ring radius : R	300 μm
Coupling coefficient : κ_4 , and κ_5	0.1
Attenuation Coefficient : α	0

Table 6.5 shows the characteristic of the input information signal used in this experiment.

Parameters	Original Value	Test 1	Test 2
Signal Power	0.002 W	0.002 W	0.002 W
Channel spacing	1 nm	0.5 nm	0.5 nm
Full Width at Half Maximum (FWHM)	0.4 nm	0.25 nm	1 nm

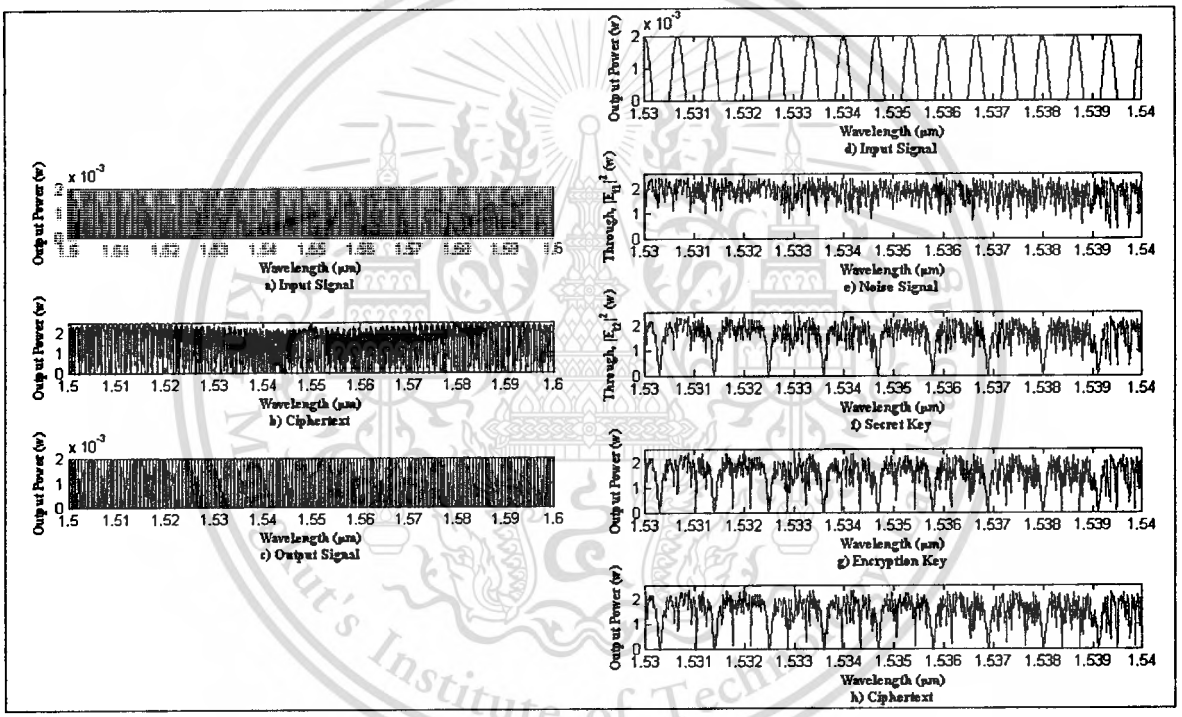

Fig. 6.1 shows the simulation results of the Test 1 where channel spacing is equal to 0.5 *n*m.

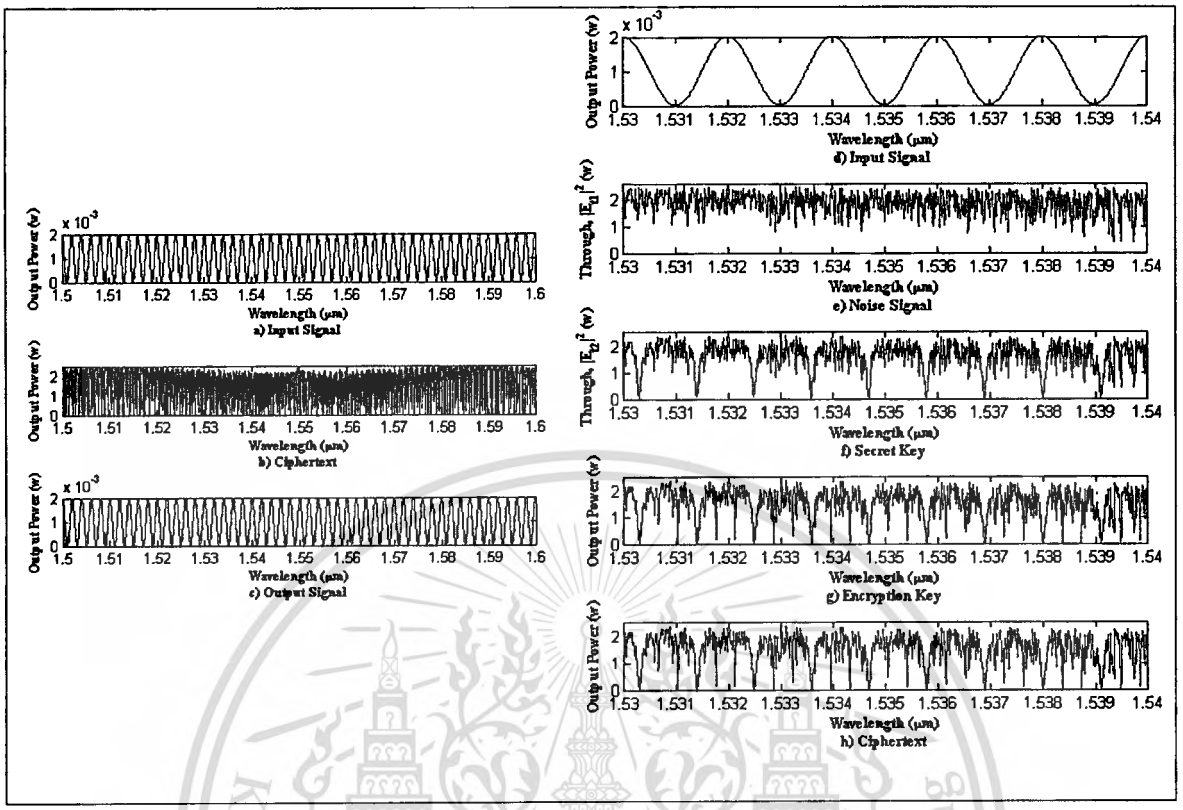

Fig. 6.2 shows the simulation results of the Test 2 where channel spacing is equal to 2 nm.

Fig 6.1 shows the simulation results of the Test 1 where the channel spacing is equal to 0.5 nm and Fig 6.2 shows the simulation results of the Test 2 where the channel spacing is equal to 2 nm. Fig. 6.1(a)-(c) and 6.2(a)-(c) show the simulation results where the wavelengths in the range of 1.5 μm to 1.6 μm which this range covers all the wavelengths generally used in the DWDM (1.528 – 1.567 μm) [115]. The input pulses with 2 mW as shown in Fig. 6.1(a) and 6.2(a) are input to all the transmission channels (pulse is ON in every channel), we use 2 mW input power because it is supported by the commercial laser [116], the higher input power can be used with our proposed cryptography system as well which will be demonstrated later in the experiment 5. The ciphertexts generated by OPM of the transmitter are random, broad and flat which look like the broadband noise signal as shown in Fig. 6.1(b) and Fig. 6.2(b), so then the secure communication is performed. The decryption module (with OPD) can recover the output signal properly as shown in the Fig. 6.1(c) and Fig. 6.2(c) , the characteristic of the output signals remains the same as the input information signals shown in Fig 6.1(a) and (c) and Fig 6.2(a) and (c), respectively. Fig. 6.1(d)-(h) and 6.2(d)-(h) show the simulation results which zoom into the wavelengths in the range of 1.53 μm to 1.54 μm in order to get

into the deeper detail. We choose these wavelengths because they are also in the range used by the DWDM (1.528 – 1.567 μm). Fig. 6.1(d) and Fig.6.2(d) show the input information signal with the channel spacing 0.5 nm and 2 nm, respectively. Fig.6.1 (e) and 6.2 (e) show the noiselike signal generated from the PANDA ring resonator in the noiselike signal generation module. Fig.6.1 (f) and 6.2 (f) show the secret key generated from the secret key generation module. Fig.6.1 (g) and 6.2 (g) show the encryption key generated from the encryption-decryption keys generation module, and Fig.6.1 (h) and 6.2 (h) show the ciphertexts generated from the OPM, respectively.

The simulation results have confirmed that the proposed cryptography system can hide the information signal even the channel spacing of the information signal are wider or narrower than 1 nm.

6.1.2 Experiment 2 – Generating the new noiselike signal

As mentioned in the previous chapter that the secret key and encryption-decryption keys are inherently derived from the noiselike signal generated from the PANDA ring resonator in the noiselike signal generation module. For the high security communication, the cryptography system must have the ability to change the key (rekey), thus the PANDA ring resonator must be capable to generate the different noiselike signals in order to obtain the different encryption-decryption keys. This experiment aims to demonstrate that the PANDA ring resonator can generate the different noiselike signals after we change the characteristics of the input dark and bright soliton pulses. We conduct three tests (Test 1, Test 2 and Test 3) in this experiment. The characteristics of the input dark and bright soliton pulses of each test are shown in Table 6.7. The used parameters of the PANDA ring resonator in the noiselike signal generation module are shown in Table 6.1. The used parameters of the Add/drop filters in the secret key generation module, the AD1 and AD3, are shown in the Table 6.3. The used parameters of the Add/drop filters in the encryption-decryption keys generation module, the AD2 and AD4, are shown in the Table 6.4. The characteristic of the input information signal used in this experiment is shown in Table 6.6, the center wavelength of the bright and dark soliton pulses used for the noiselike signal generation should be close to 1.55 μm which is in the medium of the wavelengths used by the DWDM (1.528 – 1.567 μm) and generally used for the optical communication. If the center wavelengths of both soliton pulses are shifted to the left (lower than 1.55 μm), then the center of mass fluctuation will be shifted to the left too, similarly if the center wavelengths of both soliton pulses are shifted to the right (higher than 1.55 μm) , then the center of mass fluctuation will be shifted to the right as well. The center wavelength

of the bright and dark soliton pulses is not necessary to be the same. If the center wavelength of the bright soliton pulse (e.g. 1.56 μm) is higher than the center wavelength of the dark soliton pulse (e.g. 1.55 μm), the fluctuation will be high (sharply rises and falls) at the wavelengths higher than the center wavelength of the dark soliton pulse, in other words, the mass fluctuation will be shifted to the right hand side of the center wavelength of the dark soliton pulse as shown in the Fig. 6.5(c). Similarly, If the center wavelength of the bright soliton pulse (e.g. 1.55 μm) is lower than the center wavelength of the dark soliton pulse (e.g. 1.56 μm), the fluctuation will be high at the wavelengths lower than the center wavelength of the dark soliton pulse which means the mass fluctuation will be shifted to the left hand side of the center wavelength of the dark soliton pulse as shown in the Fig. 6.7(c).The used center wavelength of both bright and dark soliton pulses should be in the range of 1.528 – 1.567 μm which this range is used by the DWDM as described previously in the experiment 1, otherwise, the power spectrum of the obtained nosielike signal will not be able to mask the information signals communicated in the DWDM due to the different ranges of the power spectrum.

Table 6.6 shows the characteristic of the input information signal.

Parameters	Value
Signal Power	0.002 W
Channel spacing	1 nm
Full Width at Half Maximum (FWHM)	0.4 nm

Table 6.7 shows the characteristics of the input bright and dark soliton pulses used for noiselike signal generation.

Test	Bright Soliton			Dark Soliton		
	Signal Power	Center Wavelength	FWHM	Signal Power	Center Wavelength	FWHM
Test 1	1 W	1.55 µm	80 nm	1 W	1.55 µm	20 nm
Test 2	1 W	1.56 µm	100 nm	2 W	1.55 µm	20 nm
Test 3	1 W	1.55 µm	90 nm	1 W	1.56 µm	14 nm

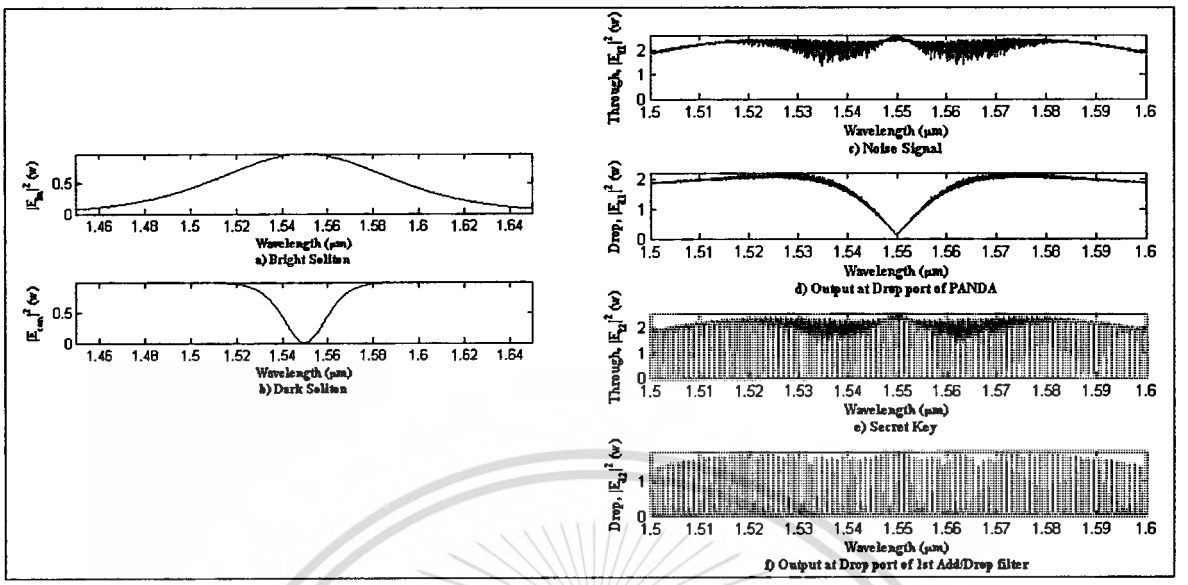

Fig. 6.3 shows the noiselike signal generation where the center wavelength of the bright and dark soliton pulses is at 1.55 μm.

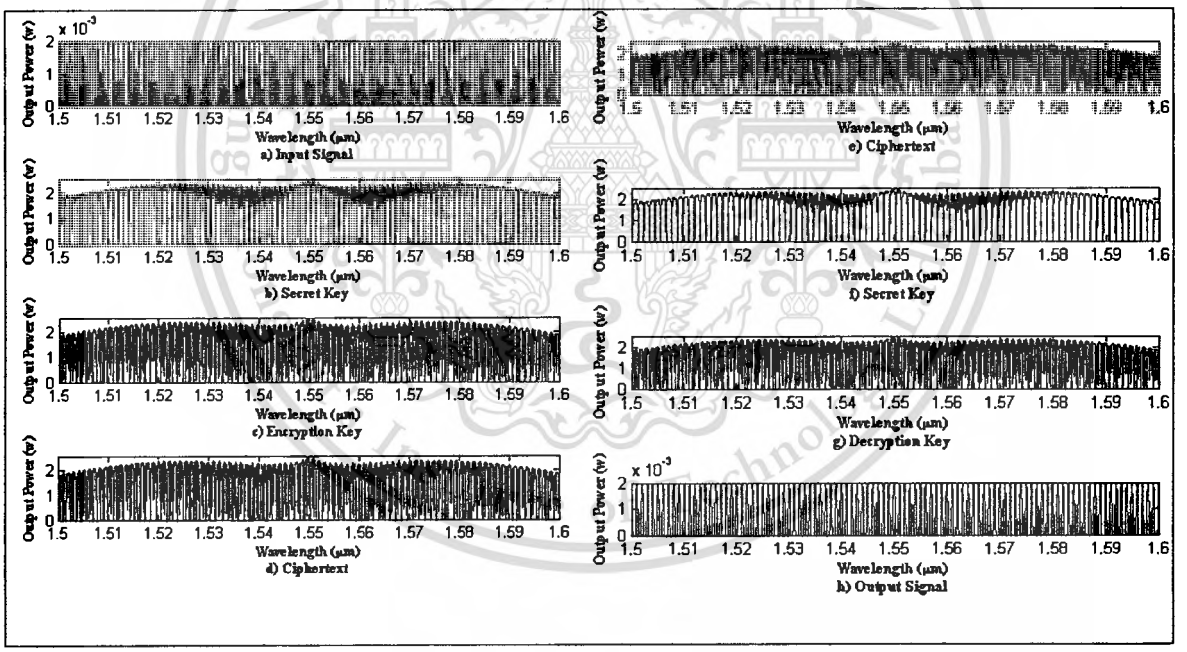

Fig. 6.4 the secret key and encryption-decryption keys are changed according to Fig. 6.3.

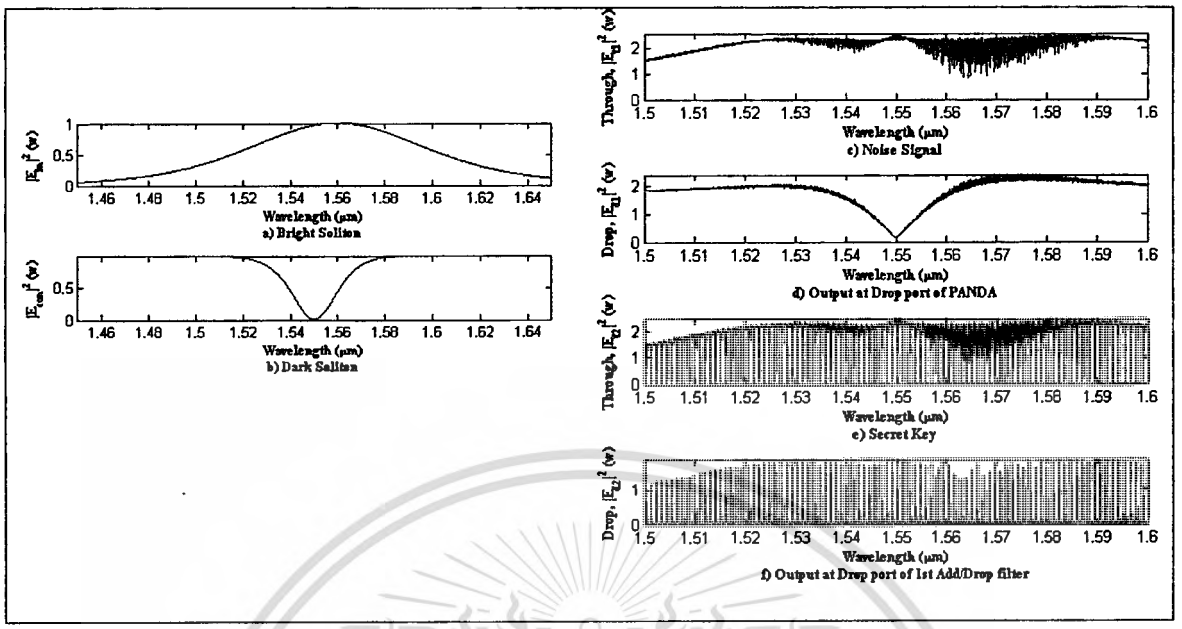

Fig. 6.5 shows the noiselike signal generation where the center wavelength of the bright and dark soliton pulses is at 1.56 μm and 1.55 μm, respectively.

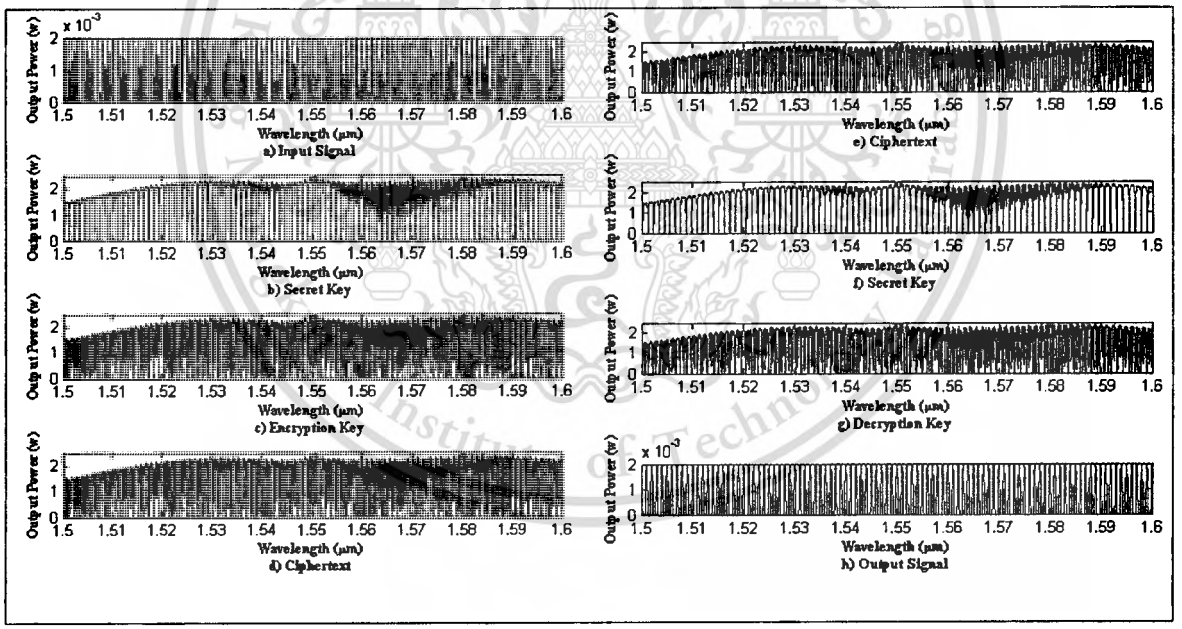

Fig. 6.6 the secret key and encryption-decryption keys are changed according to Fig. 6.5.

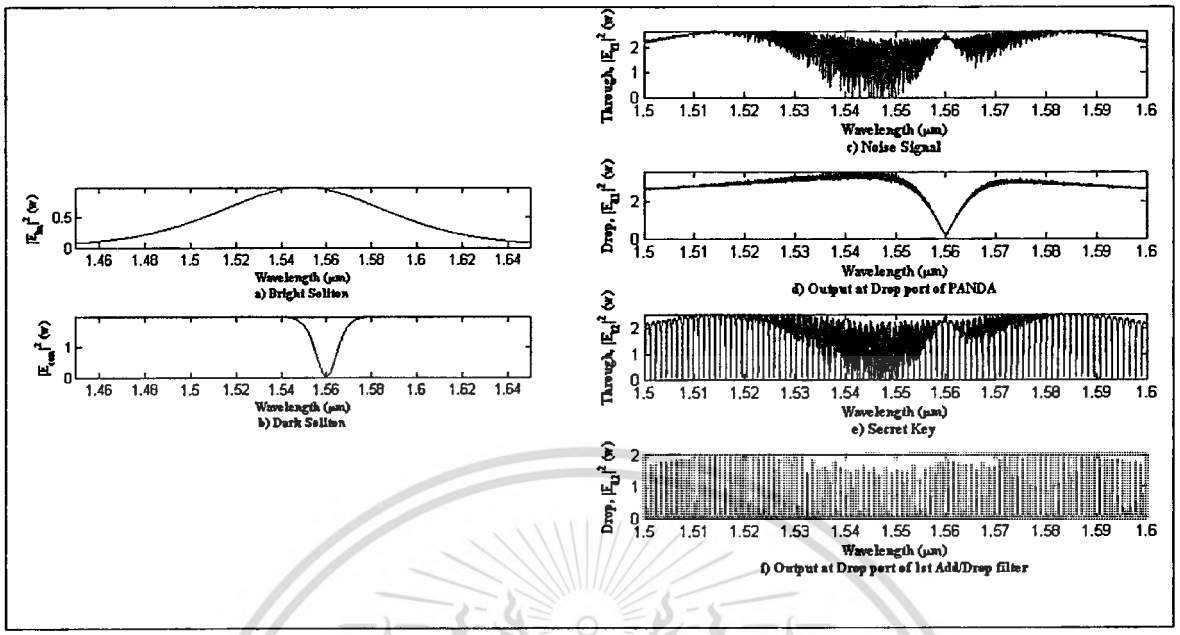

Fig. 6.7 shows the noiselike signal generation where the center wavelength of the bright and dark soliton pulses at 1.55 μm and 1.56 μm, respectively.

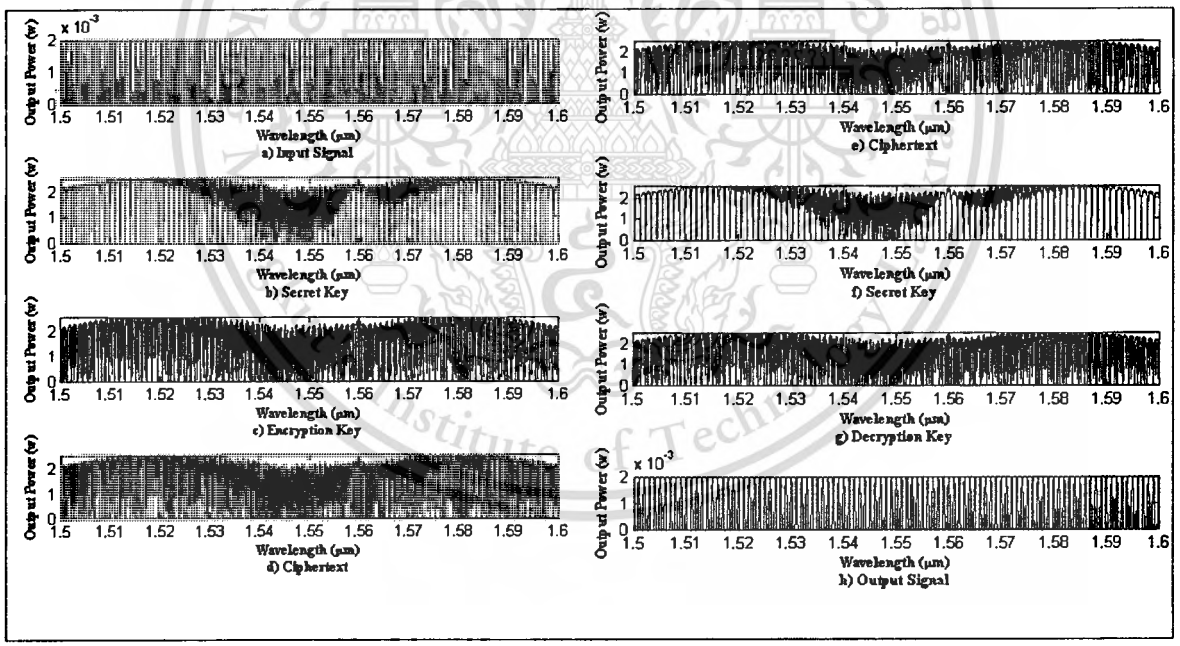

Fig. 6.8 the secret key and encryption-decryption keys are changed according to Fig. 6.7.

Fig 6.3 and 6.4 show the simulation results of the Test 1, Fig 6.5 and 6.6 show the simulation results of the Test 2, and Fig 6.7 and 6.8 show the simulation results of the Test 3, where the wavelength in the range of 1.5 to 1.6 μm .The characteristics of the input dark and bright soliton pulses used for the noiselike signal generation of the

particular test are shown in the Table 6.7. To begin with the Test 1, Fig. 6.3(a) and (b) show the bright and dark soliton pulses used for the noiselike signal generation, and Fig. 6.3(c) shows the noiselike signal generated from the noiselike signal generation module. The output signal at the drop port of the PANDA ring resonator is shown in Fig. 6.3(d) which it is not used any more by the proposed cryptography system. Fig. 6.3(e) shows the secret key generated from the secret key generation module, and Fig. 6.3(f) shows the output signal at the drop port of Add/drop filters in the secret key generation modules. Fig.6.4 (a) shows the input information signal. Fig. 6.4(b) shows the secret key generated from the secret key generation module at the transmitter. Fig. 6.4(c) shows the encryption key generated from the encryption-decryption keys generation module at the transmitter. Fig. 6.4(d) shows the ciphertext generated from the OPM at the transmitter. Fig. 6.4(e) shows the ciphertext sent to the OPD at the receiver. Fig. 6.4(f) shows the secret key generated from the secret key generation module at the receiver. Fig. 6.4(g) shows the decryption key generated from the encryption-decryption keys generation module at the receiver. Fig. 6.4(h) shows the output signal which is the same as the input information signal. Similarly, we show the simulation results of the Test 2 in Fig. 6.5 and 6.6, and the simulation results of the Test 3 in Fig. 6.7 and 6.8, where the wavelength in the range of 1.5 to 1.6 μm.

As shown in the simulation results that the proposed cryptography system has generated the different noiselike waveforms after the input dark and bright soliton pulses have been changed. The ability to generate the different noise signals and later to cause different secret keys and different encryption-decryption keys generated can confirm that our proposed system is capable to rekey which is required by the traditional cryptography system.

6.1.3 Experiment 3 – Secret key mismatches

The sensitivity to initial conditions and variation of the parameters is the key property of the noiselike communication. In this experiment, we would like to demonstrate that our proposed cryptography system has the characteristic of this property. The goal of this experiment is to show that once the eavesdropper can trap (sniff) the noislike signal, but if they use the different system parameters (in this case is the different ring radius of the AD3) from those used by the receiver's system of the proposed cryptography system, then he cannot reproduce the correct secret key and recover the original information signal. We conduct two tests (Test 1 and Test 2) in this experiment. The characteristics of the input dark and bright soliton pulses of both tests are shown in Table 6.2. The used parameters of the PANDA ring resonator in the

noiselike signal generation module are shown in Table 6.1. The used parameters of the Add/drop filters in the secret key generation module at the transmitter part, the AD1, are shown in the Table 6.3. The used parameters of the Add/drop filters in the encryption-decryption keys generation module, the AD2 and AD4, are shown in the Table 6.4. The characteristic of the input information signal used for this experiment is shown in Table 6.6. We assume that the eavesdropper has known correctly all the system parameters except the ring radius of the AD3, so in this experiment we change the ring radius of the AD3 from the one used by the proposed cryptography system as shown in Table 6.8.

Table 6.8 shows the parameters of the Add/drop filters (AD3) used in this experiment.

Parameters of the AD3	Original Value	Test 1	Test 2
Refractive index : n	3.4	3.4	3.4
Ring radius : R	100 μm	101 μm	110 μm
Coupling coefficient : κ_1 , and κ_2	0.2	0.2	0.2
Attenuation coefficient : α	100	100	100

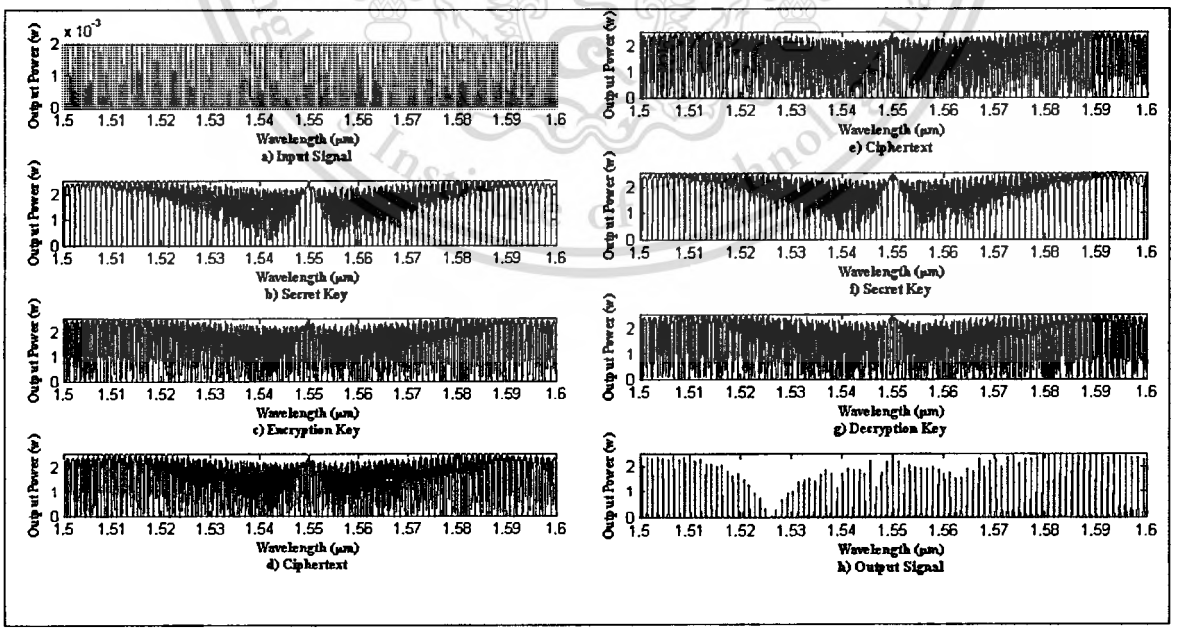

Fig 6.9 shows the simulation results where the ring radius of the AD3 is changed to 101.

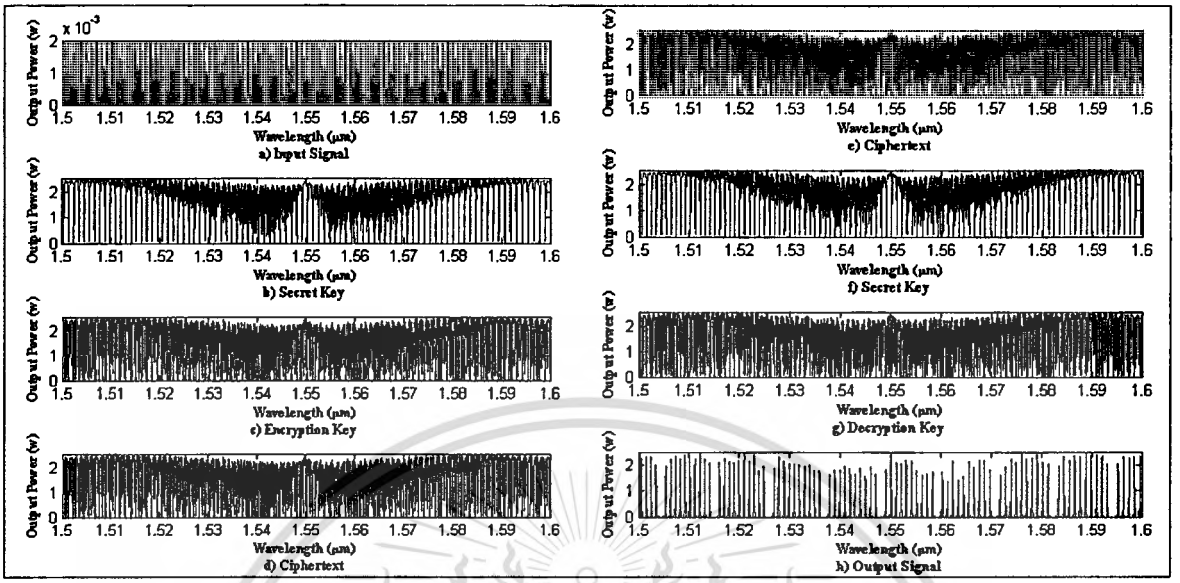

Fig 6.10 shows the simulation results where the ring radius of the AD3 is changed to 110.

Fig. 6.9 and 6.10 show the simulation results of the Test 1 and Test 2, respectively, where the wavelength in the range of 1.5 μm to 1.6 μm. Fig. 6.9(a) and 6.10(a) show the input information signal. Fig. 6.9(b) and 6.10(b) show the secret key generated from the secret key generation module at the transmitter. Fig. 6.9(c) and 6.10(c) show the encryption key generated from the encryption-decryption keys generation module at the transmitter. Fig. 6.9(d) and 6.10(d) show the ciphertext generated from the OPM at the transmitter. Fig. 6.9(e) and 6.10(e) show the ciphertext trapped by eavesdropper. Fig. 6.9(f) and 6.10(f) show the secret key generated by the eavesdropper using the values shown in the Table 6.8, in this step, as he uses the wrong ring radius of the AD3, so it causes him to generate the wrong secret key, the secret key generated from the transmitter is slightly different from the secret key generated from him as shown in Fig.6.9(b) and (f) and Fig. 6.10(b) and (f). Then Fig. 6.9(g) and 6.10(g) show the decryption key derived inherently from the secret key generated by eavesdropper which his decryption key is again slightly different from the encryption key generated by the transmitter as shown in Fig.6.9(c) and (g) and Fig. 6.10(c) and (g). Finally, Fig. 6.9(h) and 6.10(h) show the output signal which is much different from the input information signal, thus it means that the eavesdropper cannot recover the original information signal correctly.

The simulation results shown in this experiment have confirmed that our proposed cryptography system has the property of the sensitivity to initial conditions

and variation of the parameters. The small different of the ring radius of Add/drop filter used in the secret key generation module (AD3) causes the large different at the output. The wrong secret key causes the wrong decryption keys generated, making the eavesdropper cannot decrypt the ciphertext correctly.

6.1.4 Experiment 4 – Decryption key mismatches

The fourth experiment is similar to the third experiment which aims to confirm that the proposed cryptography system has the property of the sensitivity to initial conditions and variation of the parameters. In this experiment, Instead of changing the ring radius of the AD3, we make a minute change at the AD4, the rest parameters remain the same. In this experiment, we assume that the eavesdropper can trap (sniff) the noiselike signal, and reproduce exactly the correct secret key. Fortunately, he guesses wrongly the ring radius of the AD4 causing he cannot reproduce the correct decryption key, and then also cannot recover the original information. The simulation results are shown as Fig. 6.11 and 6.12. We conduct two tests (Test 1 and Test 2) in this experiment. The characteristics of the input dark and bright soliton pulses of both tests are shown in Table 6.2. The used parameters of the PANDA ring resonator in the noiselike signal generation module are shown in Table 6.1. The used parameters of the Add/drop filters in the secret key generation module, the AD1 and AD3, are shown in the Table 6.3. The used parameters of the Add/drop filters in the encryption-decryption keys generation module at the transmitter, the AD2, are shown in the Table 6.4. The characteristic of the input information signal used for this experiment is shown in Table 6.6. We assume that the eavesdropper has known correctly all the system parameters of the receiver except the ring radius of the AD4, so in this experiment we change the ring radius of AD4 from the one used by the proposed cryptography system as shown in Table 6.9.

Table 6.9 shows the parameters of the Add/drop filters (AD4) used in this experiment.

Parameters of AD4	Original Value	Test 1	Test 2
Refractive index : n	3.4	3.4	3.4
Ring radius : R	300 μm	301 μm	310 μm
Coupling coefficient : κ_1 , and κ_2	0.1	0.1	0.1
Attenuation coefficient : α	0	0	0

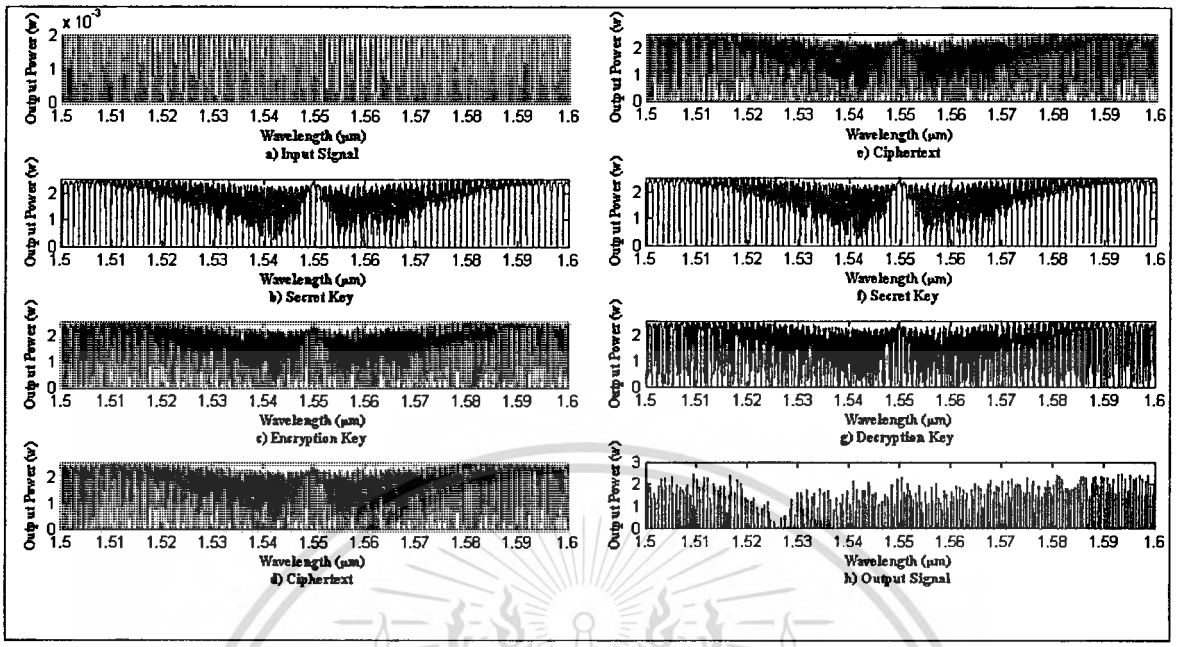

Fig 6.11 shows the simulation results where the ring radius of the AD4 is changed to 301.

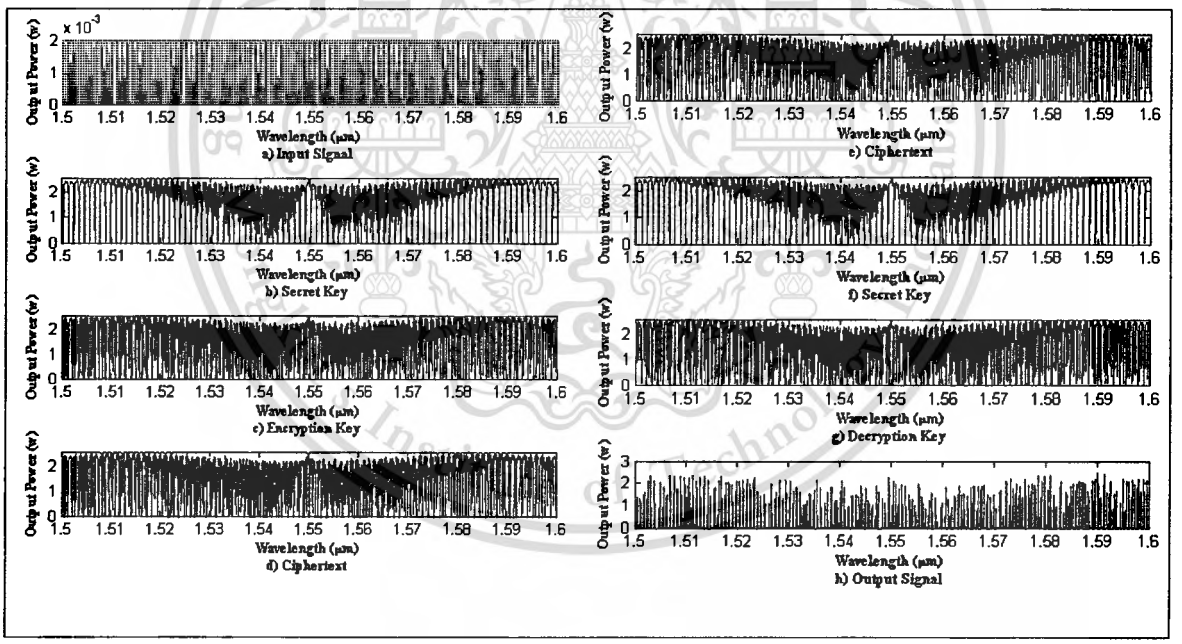

Fig. 6.12 shows the simulation results where the ring radius of the AD4 is changed to 310.

Fig. 6.11 and 6.12 show the simulation results of the Test 1 and Test 2, respectively, where the wavelength in the range of 1.5 μm to 1.6 μm. Fig. 6.11(a) and 6.12(a) show the input information signal. Fig. 6.11(b) and 6.12(b) show the secret key generated from the secret key generation module at the transmitter. Fig. 6.11(c) and

6.12(c) show the encryption key generated from the encryption-decryption keys generation module at the transmitter. Fig. 6.11(d) and 6.12(d) show the ciphertext generated from the OPM at the transmitter. Fig. 6.11(e) and 6.12(e) show the ciphertext trapped by eavesdropper. Fig. 6.9(f) and 6.10(f) show the secret key generated by the eavesdropper, as he can trap the noiselike signal and knows the used parameters of the AD3 so he can generate the secret key correctly. Fig. 6.9(g) and 6.10(g) show the decryption key generated by the eavesdropper, in this step as he uses the wrong ring radius of the AD4, so it causes him to generate the wrong decryption key as well, the encryption key generated from the transmitter is slightly different from the decryption key generated from him as shown Fig.6.11(c) and (g) and Fig. 6.12(c) and (g). Finally, Fig. 6.11(h) and 6.12(h) show the output signal which is much different from the input information signal, thus it means that the eavesdropper cannot recover the original information signal correctly.

The simulation results shown in this experiment have strongly confirmed that the proposed cryptography system really has the property of the sensitivity to initial conditions and variation of the parameters. The small different of the ring radius of Add/drop filter, the AD4, used in the encryption-decryption keys generation module causes the large different at the output. Although the eavesdropper can trap the noiselike signal and reproduce the correct secret key, but if he cannot reproduce the correct decryption key as shown in Fig. 6.11(c) and (g), and Fig. 6.12(c) and (g) , then he cannot recover the original information signal correctly as shown in Fig. 6.11(a) and (h), and Fig. 6.12(a) and (h).

6.1.5 Experiment 5 – Changing the power (intensity) of the input pulses.

The proposed cryptography system uses the additive masking technique to bury the transmitted information signals into the encryption key (derived from the noiselike signal). The power spectrum of the encryption key must be much higher than the signal power of the input information signals in order to disguise the transmitted information signals from eavesdropping. This experiment aims to show the power spectrum of the ciphertexts after doing the additive masking with the different input power. We conduct six tests (Test 1-6) in this experiment. The characteristics of the input dark and bright soliton pulses of all tests are shown in Table 6.2. The used parameters of the PANDA ring resonator in the noiselike signal generation module are shown in Table 6.1. The used parameters of the Add/drop filters in the secret key generation module, the AD1 and AD3, are shown in the Table 6.3. The used parameters of the Add/drop filters in the encryption-decryption keys generation module, the AD2 and AD4, are shown in the

Table 6.4. The signal powers of the input information signals used in this experiment are shown in Table 6.10.

Table 6.10 shows the signal power of the input information signals, and the input pulse of each channel at the wavelength between 1.53 μm and 1. 54 μm.

Test	Signal Power of the input information signal	Input pulses of the channels at the wavelength between 1.53 μm and 1. 54 μm
Test 1	0.002 W	11111111111
Test 2	0.02 W	11111111111
Test 3	0.2 W	11111111111
Test 4	0.4 W	11111111111
Test 5	1 W	10110101011
Test 6	2 W	01101010101

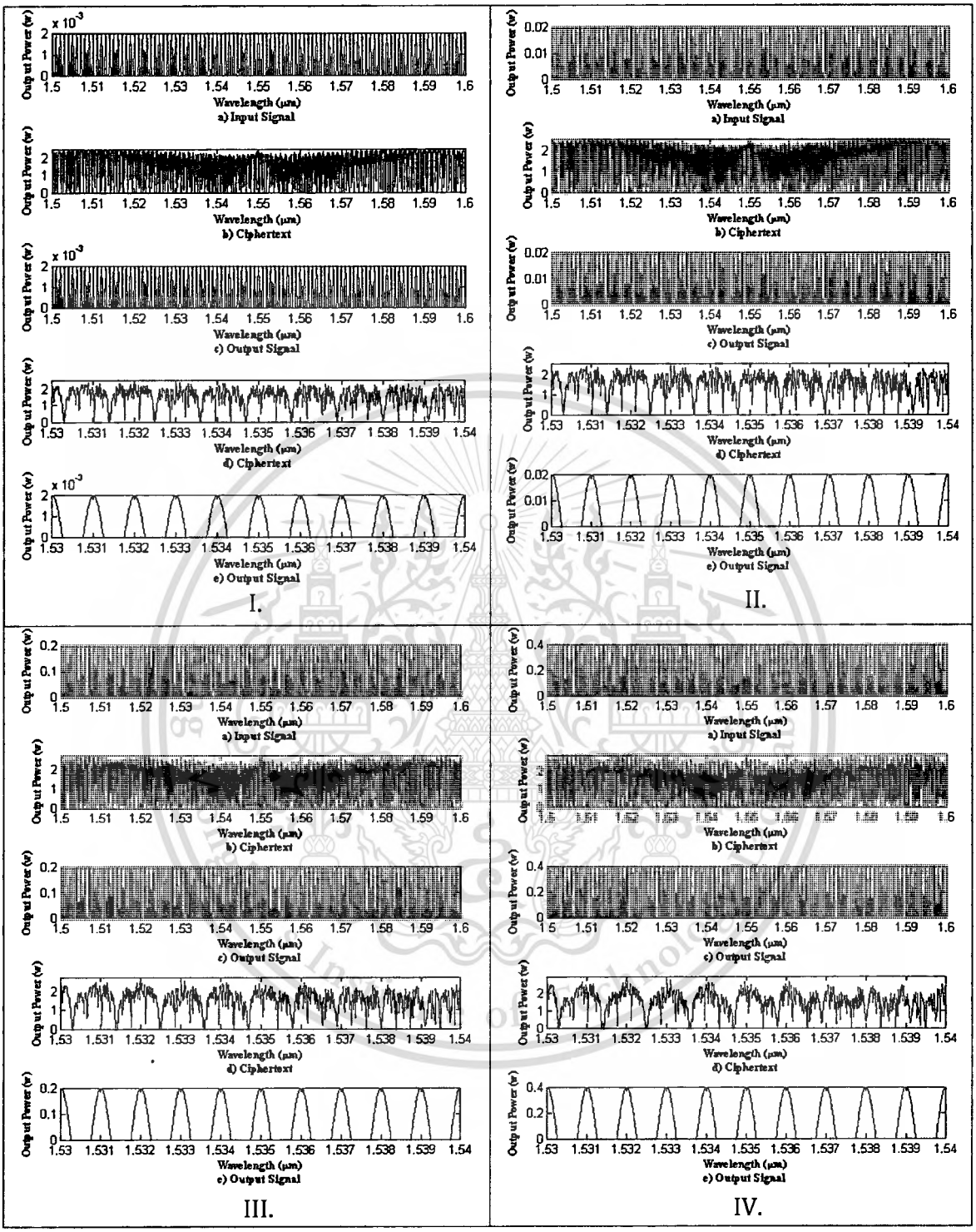

Fig 6.13 shows the ciphertext when the power (intensity) of the input pulses is changed.

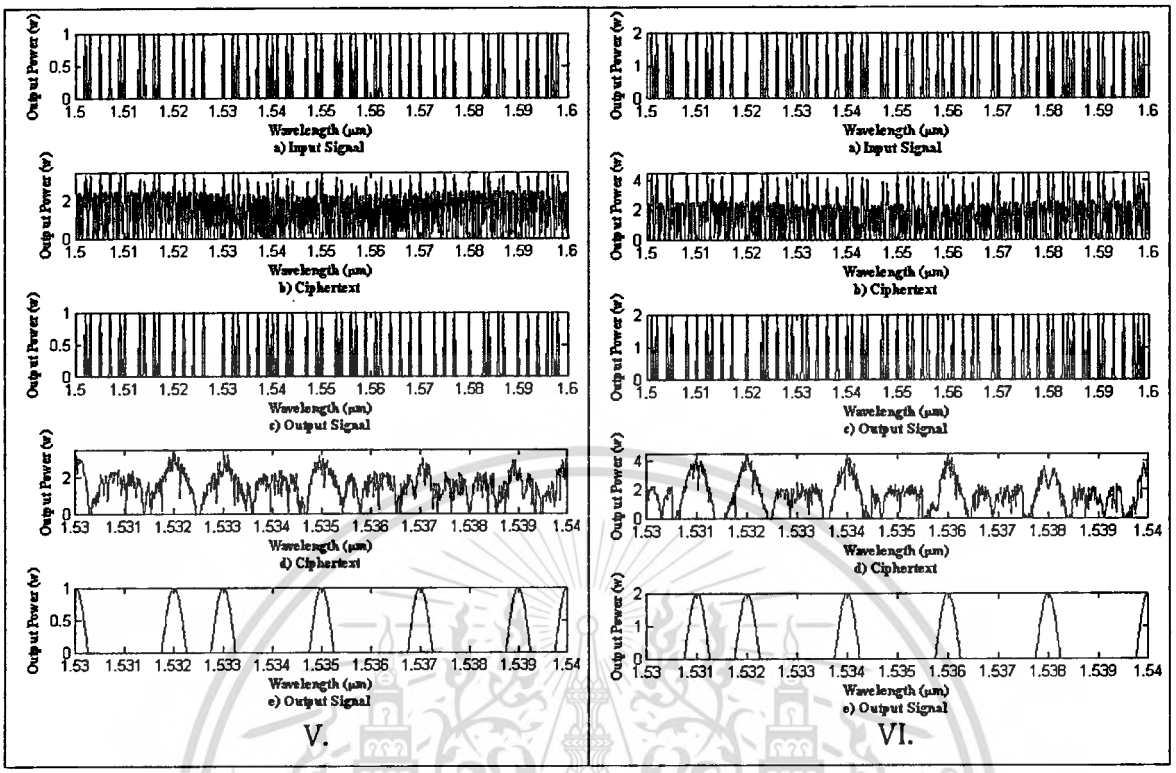

Fig 6.13 (cont.) shows the ciphertext when the power (intensity) of the input pulses is changed.

Fig. 6.13I – 6.13VI show the simulation results of the Test 1-6, respectively. To begin with the Test 1, Fig. 6.13I(a)-(c) show the simulation results at the wavelength in the range of 1.5 μm to 1.6 μm, and Fig. 6.13I(d)-(e) show the simulation results at the wavelength in the range of 1.53 μm to 1.54 μm. Fig. 6.13I(a) shows the input information signal. Fig. 6.13I(b) shows the ciphertext generated from the OPM at the transmitter. Fig. 6.13I(c) shows the output signal in the result of the decryption by the OPD at the receiver. Fig. 6.13I(d) and Fig. 6.13I(e) show the ciphertext and the output signal, respectively, where the wavelength in the range of 1.53 μm to 1.54 μm. Similar to the Test 1, the five simulation graphs are presented in particular test since Test 2 until Test 6. In particular test, we change the signal power of the input information signal to the values shown in the Table 6.10.

The simulation results have shown that If the signal power of the encryption key is much higher than the signal power of the information signal (more than or equal to 10x), then it can completely hide the information signals making the eavesdropper cannot detect the presence of the information signals as shown in the Fig.6.13I-III which the signal power of encryption key is 1000x, 500x, and 10x higher than the signal power

of the input information signal, respectively. Moreover, we have also demonstrated that if the signal power of the encryption key is not much higher than the signal power of the information signals (less than 10x), 5x, 2x and 1x as shown in Fig. 6.13IV-VI, respectively, then the eavesdropper can easily detect the presence of the information signal.

6.1.6 Experiment 6 – Changing the input pulses.

In the real communication over DWDM, usually all the transmission channels may not convey the pulse at the same time. At every time T some channels may be in ON state (1) and some channels may be in OFF state (0). This experiment aims to demonstrate how the ciphertexts look like if only some transmission channels are conveying the pulses. We conduct six tests (Test 1-6) in this experiment for time T_1 to T_6 , respectively. The characteristics of the input dark and bright soliton pulses of all tests are shown in Table 6.2. The used parameters of the PANDA ring resonator in the noiselike signal generation module are shown in Table 6.1. The used parameters of the Add/drop filters in the secret key generation module, the AD1 and AD3, are shown in the Table 6.3. The used parameters of the Add/drop filters in the encryption-decryption keys generation module, the AD2 and AD4, are shown in the Table 6.4. The characteristic of the input information signal used for this experiment is shown in Table 6.6. Lastly, the input pulses of all the channels are shown in the Table 6.11, where their wavelength between 1.53 μm and 1.54 μm.

Table 6.11 shows the input pulses of all the channels where its wavelength between 1.53 μm and 1.54 μm.

Test	Input pulses of the channels where the wavelength between 1.53 μm and 1. 54 μm
Test 1	11111111111
Test 2	11111111111
Test 3	11111111111
Test 4	11111111111
Test 5	10110101011
Test 6	01101010101

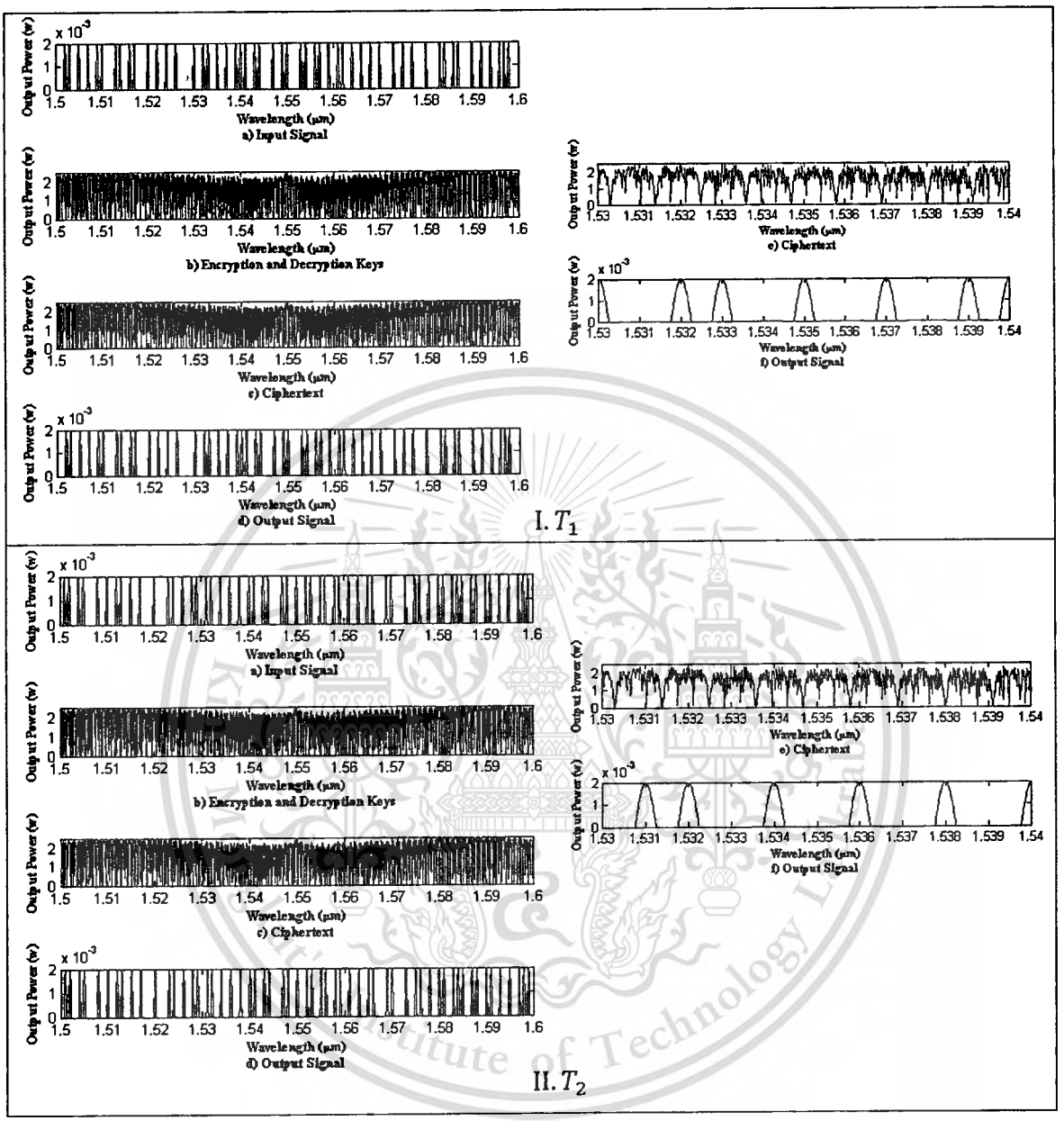

Fig. 6.14 shows the simulation results at the time T_i $(1 \leq i \leq 6)$.

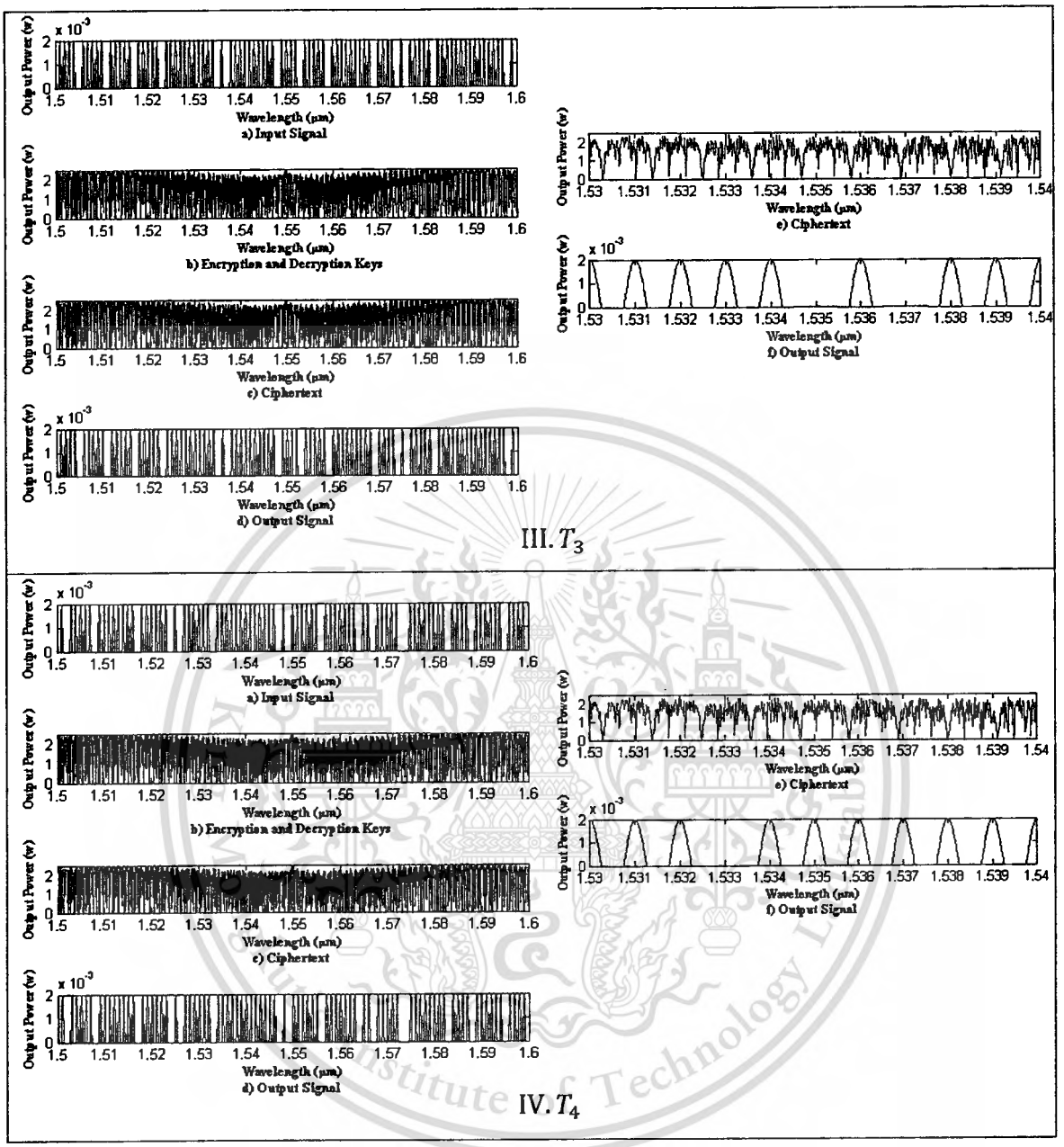

Fig. 6.14 (cont.) shows the simulation results at the time T_i $(1 \leq i \leq 6)$.

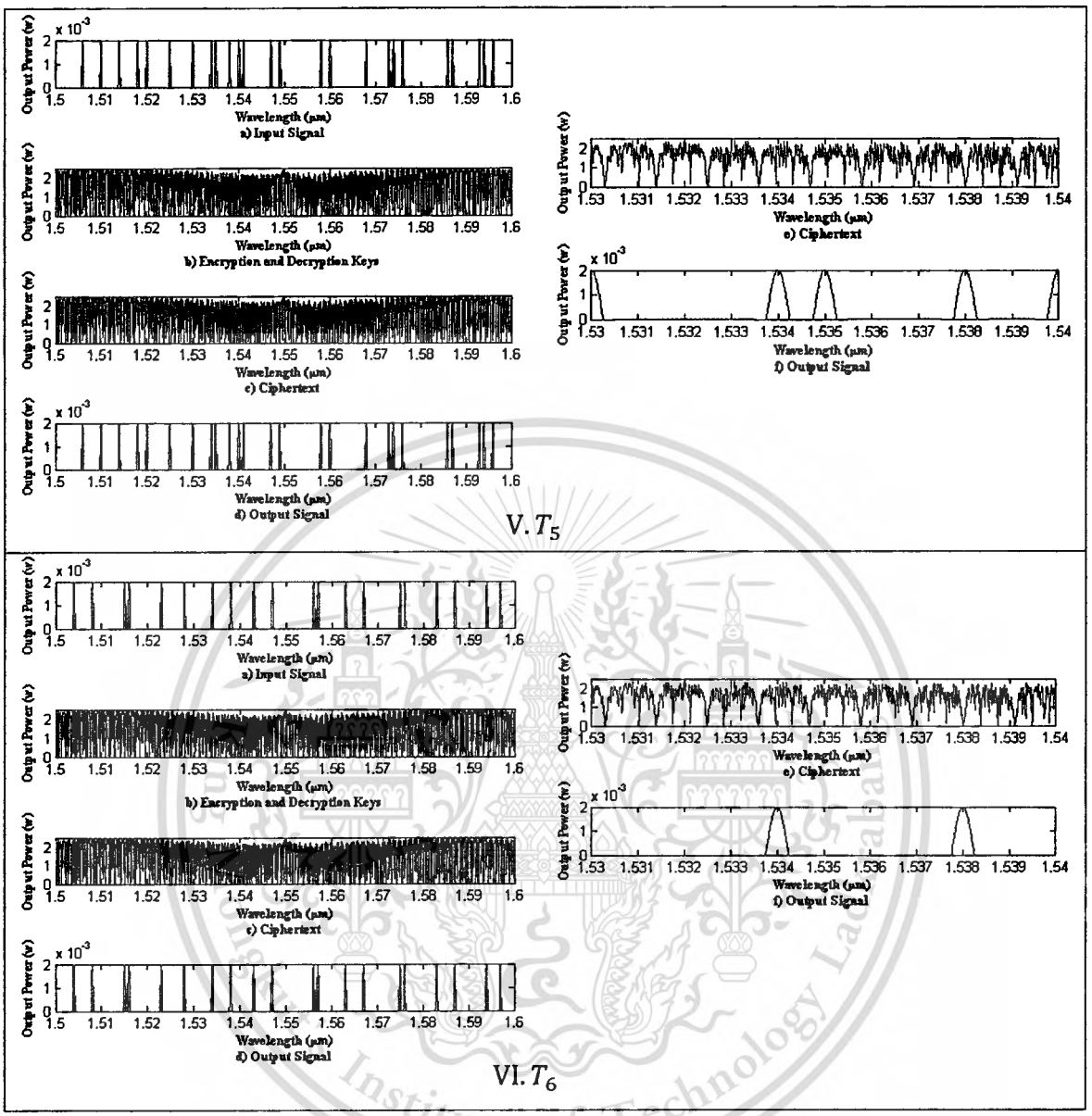

Fig. 6.14 (cont.) shows the simulation results at the time T_i $(1 \leq i \leq 6)$.

Fig. 6.14I–VI show the simulation results of the Test 1-6, respectively. To begin with the Test 1, Fig. 6.14I(a)-(d) show the simulation results at the wavelength in the range of 1.5 μm to 1.6 μm, and Fig. 6.14I(e)-(f) show the simulation results at the wavelength in the range of 1.53 μm to 1.54 μm. Fig. 6.14I(a) shows the input information signal. Fig. 6.14I(b) shows the encryption and decryption keys generated from the encryption-decryption keys generation module at the transmitter and receiver , respectively. Fig. 6.14I(c) shows the ciphertext generated from the OPM at the transmitter prior to sending it to the OPD at the receiver. Fig. 6.14I(d) shows the output

signal in the result of the decryption by the OPD at the receiver. Fig. 6.14I(e) and Fig. 6.14I(f) show the ciphertext and the output signal, respectively, at the wavelength in the range of 1.53 μm to 1.54 μm. Similar to the Test 1, six simulation graphs are presented in particular test since Test 2 until Test 6 as shown in the Fig. 6.14II-VI, respectively. In particular test, we change the state of the input pulses as shown in the Table 6.11.

The simulation results have shown that the ciphertexts look like the same in every time T, the power spectrums of all the ciphertexts are random, broad and flat which look like the broadband noise signal. Therefore, it confirms that our proposed cryptography system has the property of the noiselike broadband spread spectrum even some channels are ON and some channels are OFF.

6.1.7 Experiment 7 – Rekeying at every time T.

The ability to rekey is very important for the traditional cryptography system, it helps to protect the entire ciphertext not to get decrypted by the eavesdropper in case he can reproduce any decryption key. In addition to the demonstration in the second experiment, this experiment aims to demonstrate that our proposed cryptography system is capable to rekey the new encryption and decryption keys at every time $T_i(\ 1 \leq i \leq 6)$ and at both the transmitter and receiver parts. The ciphertexts of both transmitter and receiver, after rekeying, will be also shown at the simulation results, the benefit of the rekeying will be demonstrated in the next experiment. This experiment shows the communication on both ways (transmitter to receiver, and receiver to transmitter). We conduct six tests on each way for time T_1 to T_6 , respectively. Test 1-6 are conducted for the communication from the transmitter to the receiver, and Test 7-12 are conducted for the communication from the receiver to the transmitter. The used parameters of the PANDA ring resonator in the noiselike signal generation module are shown in Table 6.1. The used parameters of the Add/drop filters in the secret key generation module, the AD1 and AD3, are shown in the Table 6.3. The used parameters of the Add/drop filters in the encryption-decryption keys generation module, the AD2 and AD4, are shown in the Table 6.4. The characteristic of the input information signal used for this experiment is shown in Table 6.6. Lastly, the characteristics of the input dark-bright soliton pulses and the input pulses used in this experiment are shown in the Table 6.12. As described in the experiment 2, the center wavelength of the dark and bright soliton pulses should be close to 1.55 μm in order to keep the center of mass fluctuation in the medium of the wavelengths used by the DWDM. Thus the used center wavelength of the dark and bright soliton pulses in this experiment is 1.55 μm or 1.56 μm. Moreover, the signal power of the dark soliton pulse and the Full Width at Half

Maximum (FWHM) of the bright soliton pulse also effect the fluctuation of the noiselike signal, if the signal power of the dark soliton pulse is higher, e.g. 2W at the time T_2, T_4, and T_5 , then the encryption key derived inherently from the noiselike signal generated from the PANDA ring resonator has a higher fluctuation (sharply rises and falls) too as shown in the Fig. 6.15II(b), 6.15IV(b), and 6.15V(b) , respectively. FWHM is the difference between the wavelengths (frequencies) on either side of a spectral measured at half of its maximum (peak). The FWHM of the bright soliton pulse should be wider than 50nm in order to keep the width of the fluctuation to cover all the wavelengths used in the DWDM. The narrow bright soliton pulse causes no interference at the wavelengths beyond both edges of the pulse due to there is no signal transmitted resulting in there are no fluctuation occurred on those wavelengths.

Table 6.12 shows the characteristics of the input dark-bright soliton pulses, and the input pulses used in this experiment.

Time	Input Bright Soliton			Input Dark Soliton			Input Pulses
	Signal Power	Center Wavelength	FWHM	Signal Power	Center Wavelength	FWHM	
Time T_1	1 W	1.55 μm	80 nm	1 W	1.55 μm	20 nm	10110101011
Time T_2	1 W	1.55 μm	180 nm	2 W	1.55 μm	7 nm	01101010101
Time T_3	1 W	1.56 μm	100 nm	1 W	1.55 μm	20 nm	11111010111
Time T_4	1 W	1.55 μm	90 nm	2 W	1.56 μm	14 nm	11101111111
Time T_5	1 W	1.55 μm	120 nm	2 W	1.55 μm	4 nm	10001100101
Time T_6	1 W	1.55 μm	120 nm	1 W	1.55 μm	85 nm	00001000100

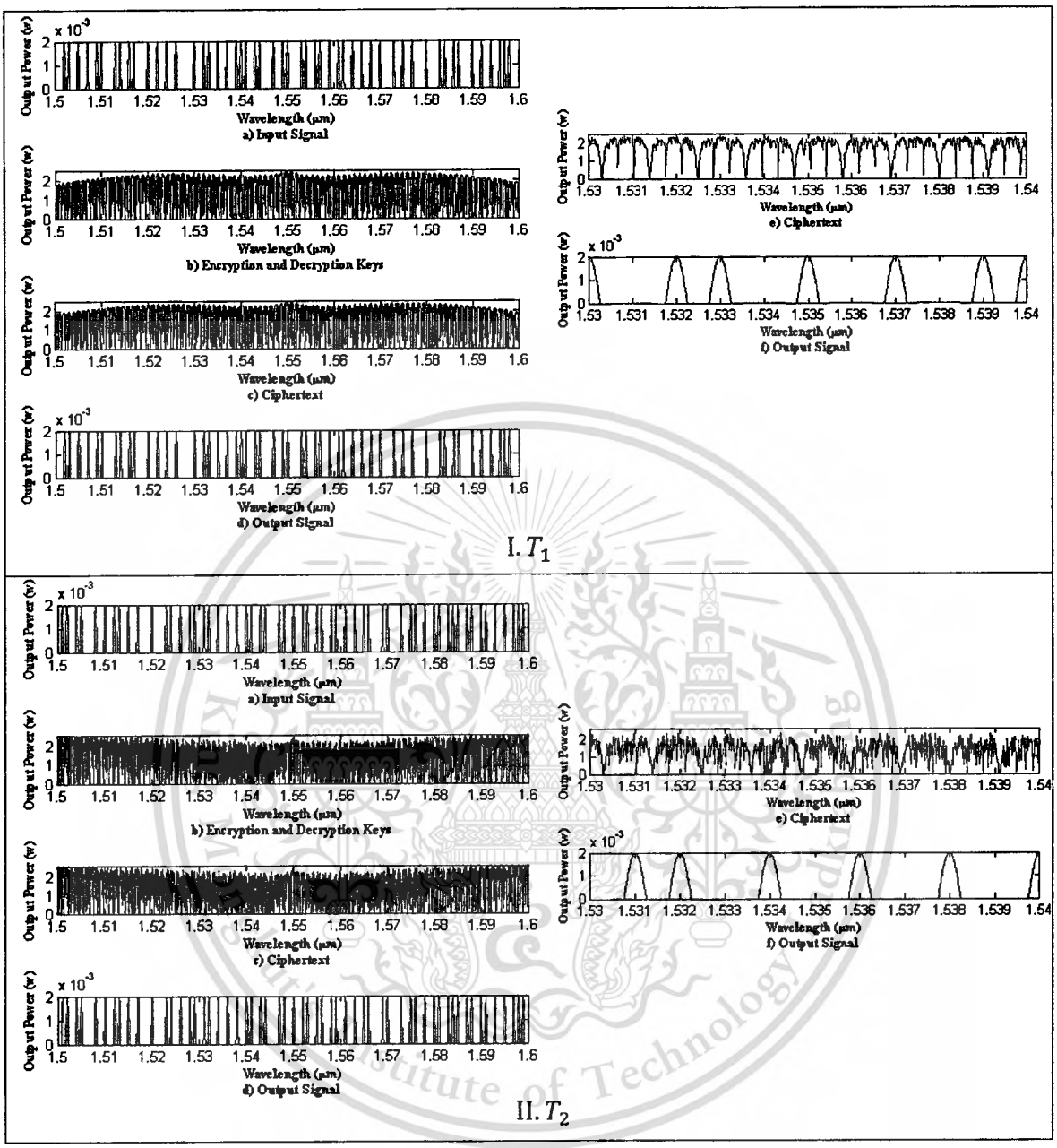

Fig. 6.15 shows the simulation results at the time T_i $(1 \leq i \leq 6)$ where the encryption key of the transmitter is changed at every time T.

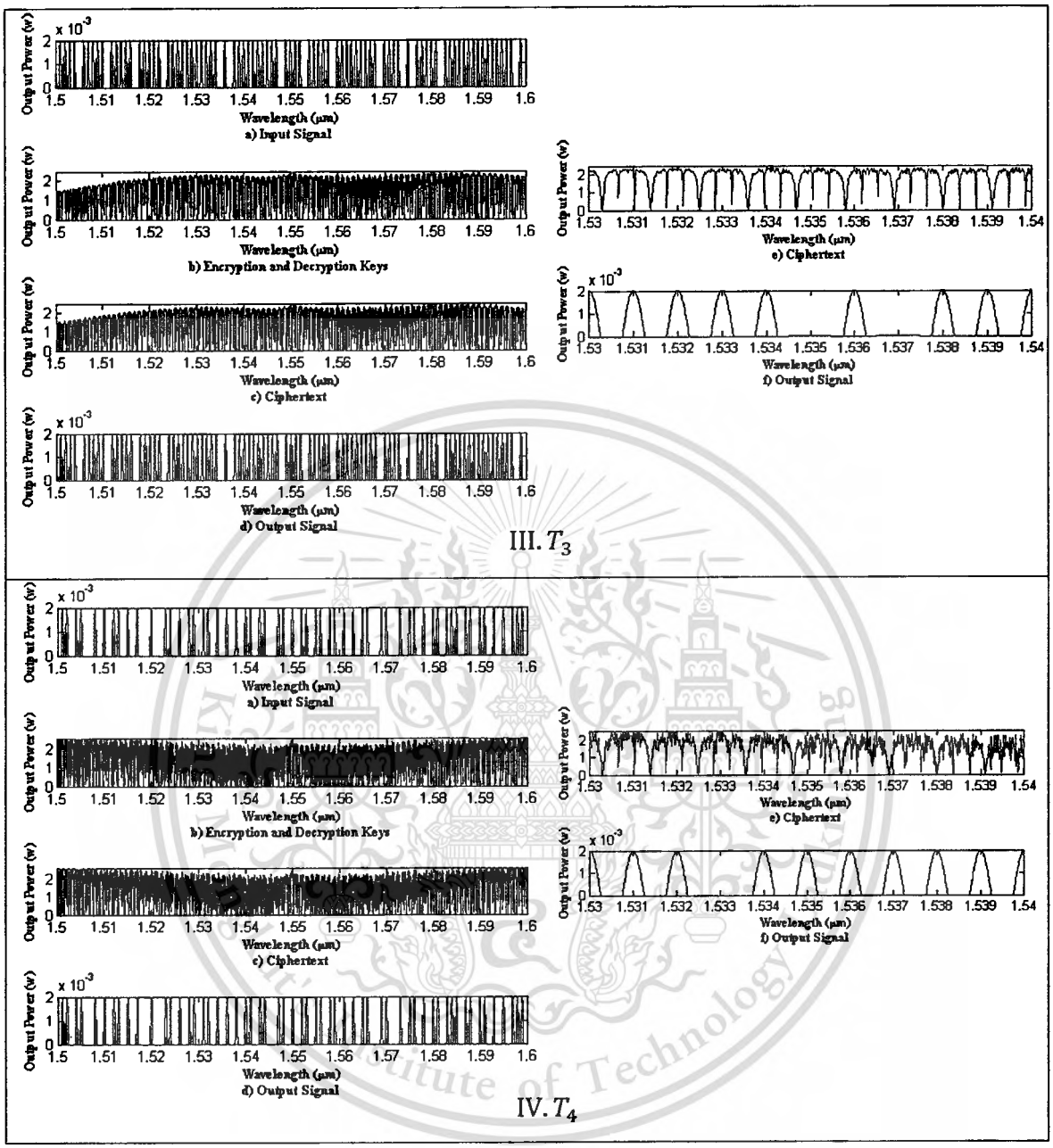

Fig. 6.15 (cont.) shows the simulation results at the time T_i $(1 \leq i \leq 6)$ where the encryption key of the transmitter is changed at every time T.

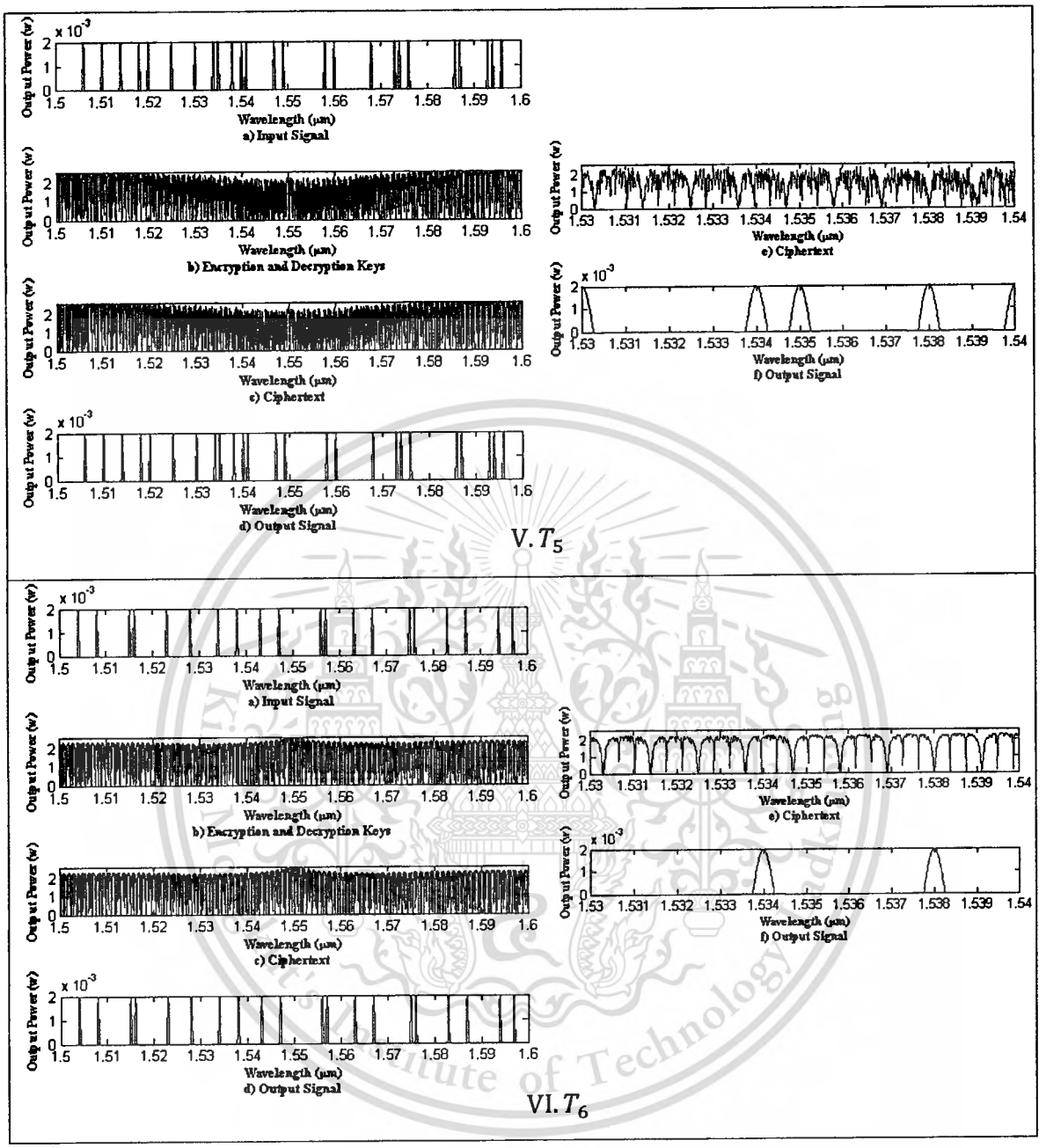

Fig. 6.15 (cont.) shows the simulation results at the time T_i $(1 \leq i \leq 6)$ where the encryption key of the transmitter is changed at every time T.

Fig. 6.15I–VI show the simulation results of the Test 1-6, respectively. To begin with the Test 1, Fig. 6.15I(a)-(d) show the simulation results at the wavelength in the range of 1.5 μm to 1.6 μm, and Fig. 6.15I(e)-(f) show the simulation results at the wavelength in the range of 1.53 μm to 1.54 μm. Fig. 6.15I(a) shows the input information signal. Fig. 6.14I(b) shows the encryption and decryption keys generated from the

encryption-decryption keys generation module at the transmitter and receiver , respectively. Fig. 6.15I(c) shows the ciphertext generated from the OPM at the transmitter prior to sending it to the OPD at the receiver. Fig. 6.15I(d) shows the output signal in the result of the decryption by the OPD at the receiver. Fig. 6.15I(e) and Fig. 6.15I(f) show the ciphertext and the output signal, respectively, at the wavelength in the range of 1.53 μm to 1.54 μm. Similar to the Test 1, six simulation graphs are presented in particular test since Test 2 until Test 6 as shown in the Fig. 6.15II-VI, respectively. In particular test, we change the characteristics of the input dark-bright soliton pulses as shown in the Table 6.12 in order to generate the new noiselike signal , new secret keys , and finally new encryption and decryption keys, respectively.

The simulation results have confirmed that our proposed cryptography system has the mechanism to create the new encryption key at the transmitter and the new decryption key at the receiver, so that we can use this mechanism to rekey at every time T in order to leverage the security of the communication. This mechanism can help to protect the entire ciphertext not to get decrypted by the eavesdropper, in case he can reproduce any decryption key, only some portions of the ciphertext can be decrypted by his decryption key. The eavesdropper will not be able to decrypt the ciphertext any more if the encryption key is changed (rekey).

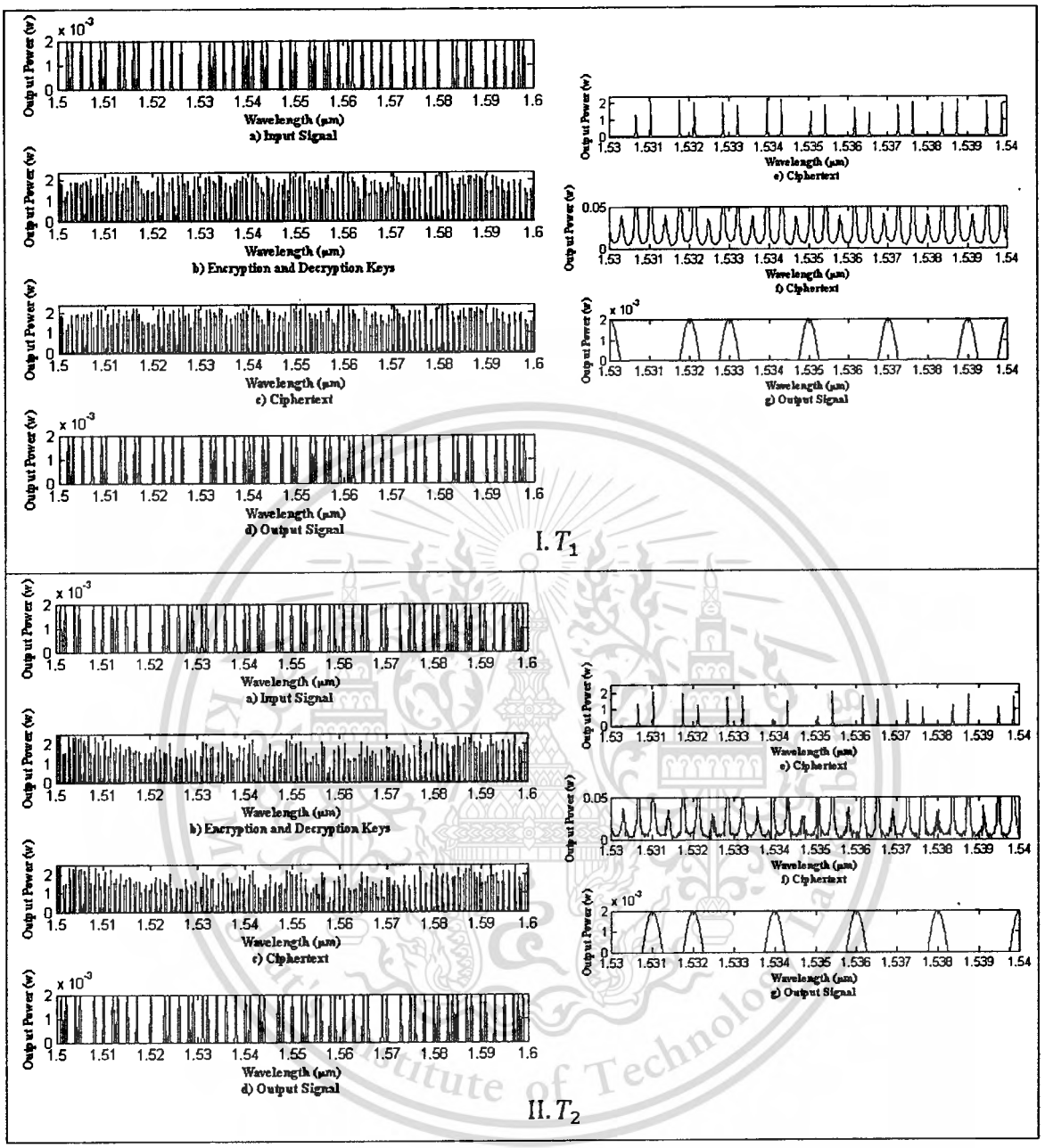

Fig. 6.16 shows the simulation results at the time T_i $(1 \leq i \leq 6)$ where the encryption key of the receiver is changed at every time T.

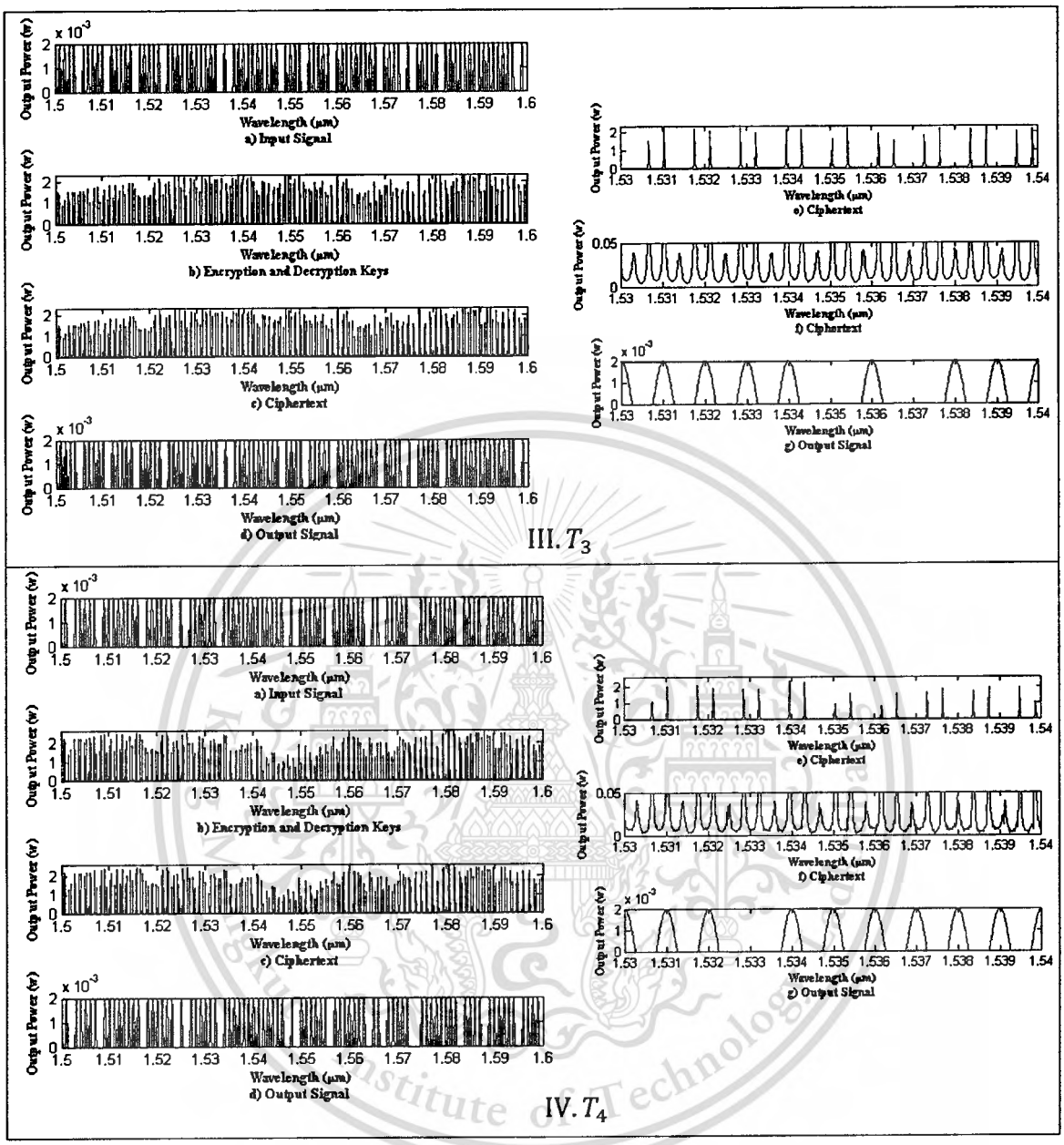

Fig. 6.16 (cont.) shows the simulation results at the time T_i $(1 \leq i \leq 6)$ where the encryption key of the receiver is changed at every time T.

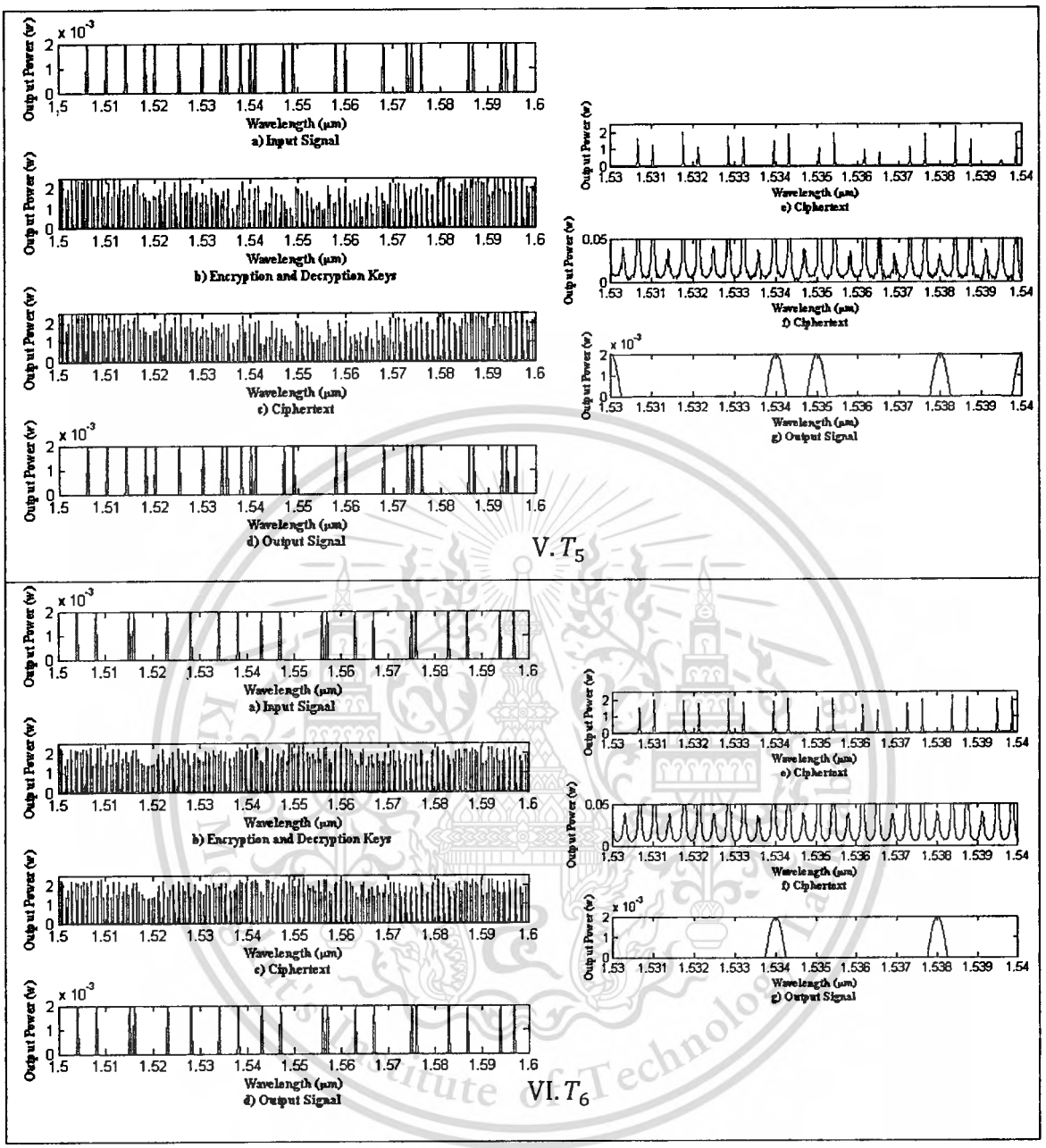

Fig. 6.16 (cont.) shows the simulation results at the time T_i $(1 \leq i \leq 6)$ where the encryption key of the receiver is changed at every time T.

Fig. 6.16I–VI show the simulation results of the Test 7-12, respectively. To begin with the Test 7, Fig. 6.16I(a)-(d) show the simulation results at the wavelength in the range of 1.5 μm to 1.6 μm, and Fig. 6.16I(e)-(g) show the simulation results at the wavelength in the range of 1.53 μm to 1.54 μm. Fig. 6.16I(a) shows the input information signal. Fig. 6.16I(b) shows the encryption and decryption keys generated from the

encryption-decryption keys generation module at the receiver and transmitter , respectively. Fig. 6.16I(c) shows the ciphertext generated from the OPM at the receiver prior to sending it to the OPD at the transmitter. Fig. 6.16I(d) shows the output signal in the result of the decryption by the OPD at the transmitter. Fig. 6.16I(e), 6.16I(f) and 6.16I(g) show the ciphertext at maximum 2W, the ciphertext at maximum 0.05W, and the output signal, respectively, at the wavelength in the range of 1.53 μm to 1.54 μm. Similar to the Test 7, seven simulation graphs are presented in particular test since Test 8 until Test 12. In particular test, we change the characteristics of the input dark and bright soliton pulses as shown in the Table 6.12 in order to generate the new noiselike signal , new secret keys , and finally new encryption and decryption keys, respectively.

The simulation results have confirmed that our proposed cryptography system has the mechanism to create the new encryption and decryption keys for both the transmitter and receiver. This can be done by changing the characteristic of the input bright and dark soliton pulses, resulting in the PANDA ring resonator generates the new noiselike signal. Then both transmitter and receiver can create the new secret and encryption-decryption keys, respectively, from that new noiselike signal. As shown in the simulation results, the rekey process can be done at every time T which means that the transmitter and receiver can create the new encryption and decryption keys at every time T too. This mechanism can help to protect the entire ciphertext not to get decrypted by the eavesdropper, in case he can reproduce any decryption key, only some portions of the ciphertext can be decrypted by his decryption key, he will not be able to decrypt the ciphertext any more if the encryption key is changed (rekey).

6.1.8 Experiment 8 – Decrypting the ciphertext by the old decryption key after rekeying

As demonstrated in the seventh experiment, the rekeying leverages the security of the cryptography system in which it protects the entire information not get decrypted by the eavesdropper even any decryption key is known. In this last experiment, it aims to demonstrate that, after rekeying, the old decryption key cannot be used to decrypt the ciphertexts. We conduct two tests (Test 1 and Test 2) in this experiment. The used parameters of the PANDA ring resonator in the noiselike signal generation module are shown in Table 6.1. The used parameters of the Add/drop filters in the secret key generation module, the AD1 and AD3, are shown in the Table 6.3. The used parameters of the Add/drop filters in the encryption-decryption keys generation module, the AD2 and AD4, are shown in the Table 6.4. The characteristic of the input information signal used for this experiment is shown in Table 6.6. We have described in the experiment 2

and 7 how the noiselike signal is changed according to the change of the parameters of the bright and dark soliton pulses. This experiment would like to demonstrate that the old decryption key cannot be used to decrypt the ciphertext generated from the new encryption key, in order to do so, we have to generate the different noiselike signals for the transmitter and eavesdropper. The table 6.13 shows the characteristics of the bright and dark soliton pulses used to generate the noiselike signal for the eavesdropper which the secret and decryption keys derived inherently from the noiselike signal generated by the eavesdropper are assumed as the old keys. On the other hand, the table 6.14 shows the characteristics of the bright and dark soliton pulses used to generate the noiselike signal for the transmitter which the secret and encryption keys derived inherently from the noiselike signal generated by the transmitter are assumed as the new keys. In the Test 1, we would like to have the noiselike signal of the eavesdropper to be higher fluctuation than the transmitter so the signal power of its dark soliton pulse is set to 2W (as described in the experiment 7). Vice versus in the Test 2, we would like to have the noiselike signal of the transmitter to be higher fluctuation than the eavesdropper so the signal power of its dark soliton pulses is set to 2W.

Table 6.13 shows the characteristics of the old bright and dark soliton pulses used for the noiselike signal generation at the eavesdropper in the Test 1 and Test 2.

Test	Old Bright Soliton			Old Dark Soliton		
	Signal Power	Center Wavelength	FWHM	Signal Power	Center Wavelength	FWHM
Test 1	1 W	1.55 μm	180 nm	2 W	1.55 μm	7nm
Test 2	1 W	1.56 μm	100 nm	1 W	1.55 μm	20 nm

Table 6.14 shows the characteristics of the new bright and dark soliton pulses used for the noiselike signal generation at the transmitter in the Test 1 and Test 2.

Test	New Bright Soliton			New Dark Soliton		
	Signal Power	Center Wavelength	FWHM	Signal Power	Center Wavelength	FWHM
Test 1	1 W	1.55 μm	80 nm	1 W	1.55 μm	20 nm
Test 2	1 W	1.55 μm	90 nm	2 W	1.56 μm	14 nm

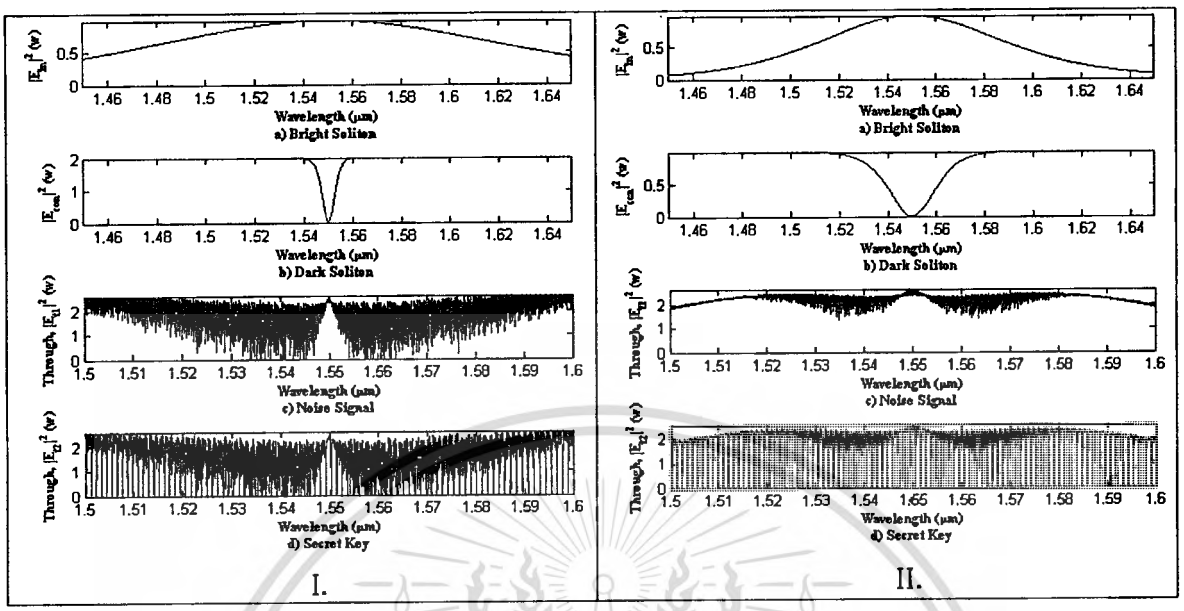

Fig. 6.17 compares the old (eavesdropper) and new (transmitter) noiselike signals used in the Test 1.

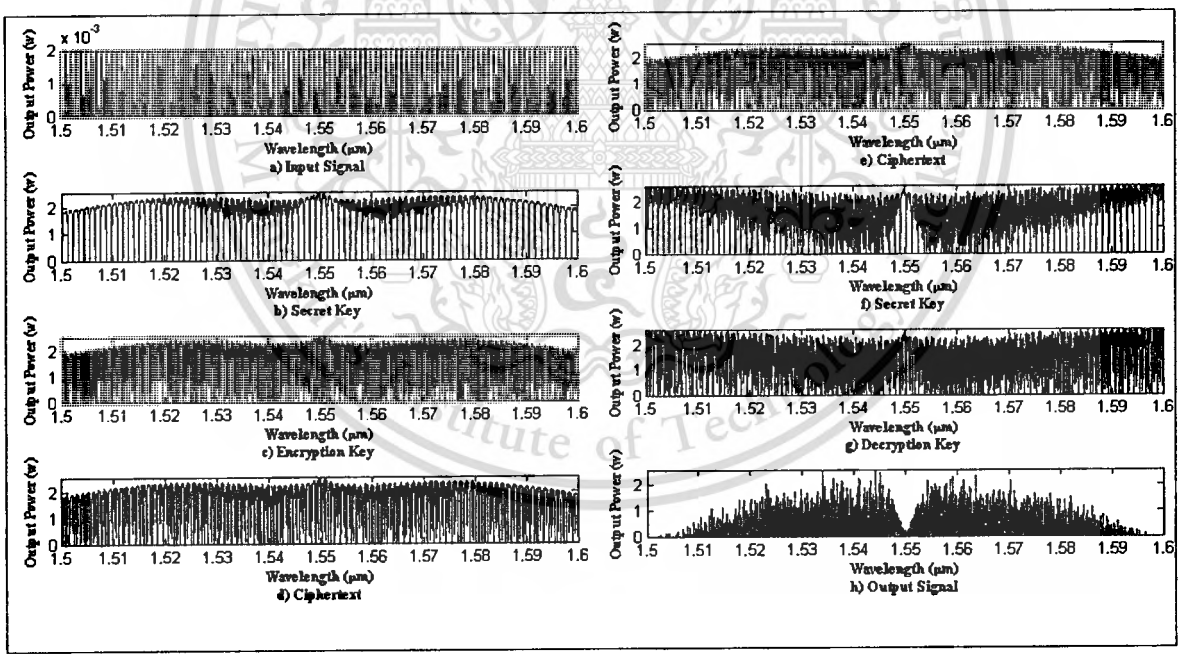

Fig. 6.18 shows the simulation results of the Test 1 after the transmitter has changed the encryption key.

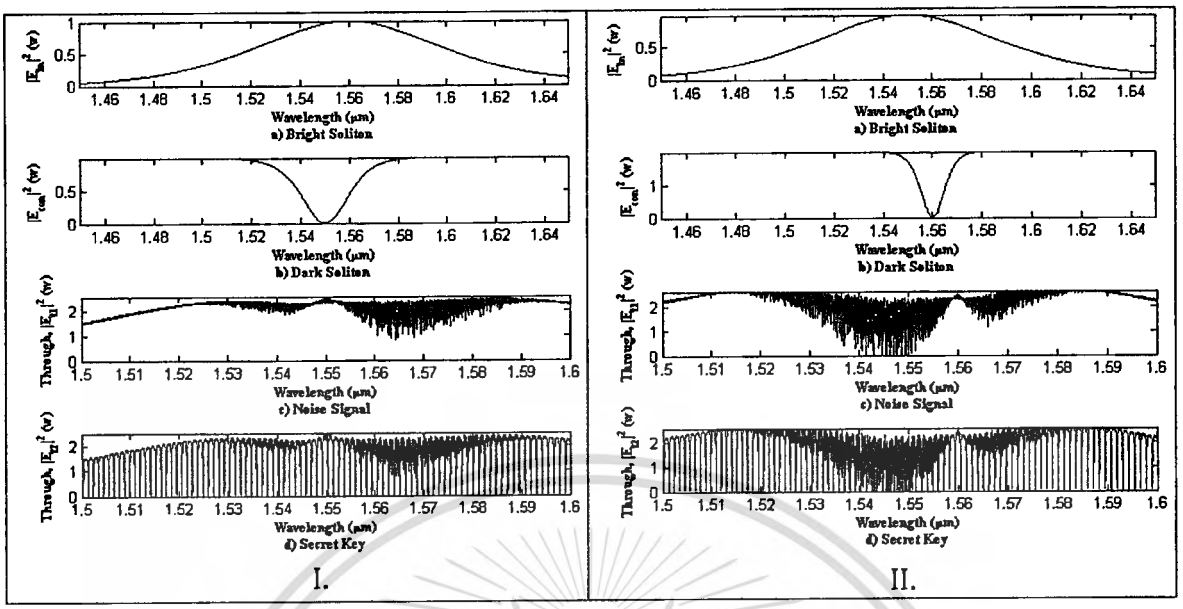

Fig. 6.19 compares the old (eavesdropper) and new (transmitter) noiselike signals used in the Test 2.

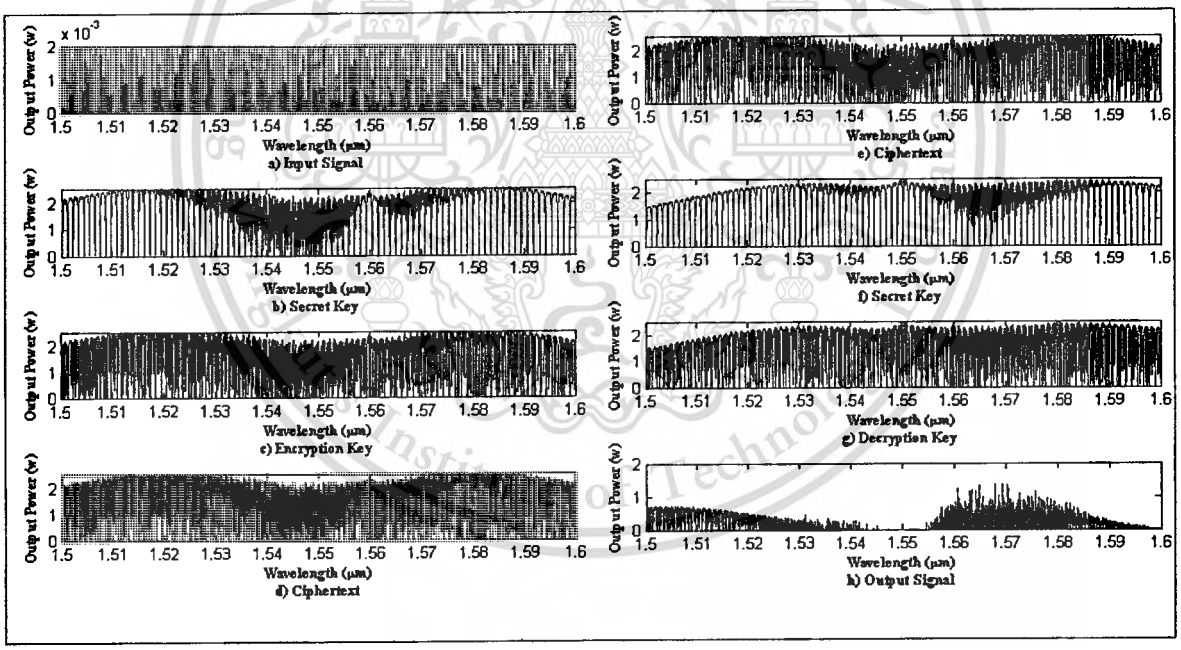

Fig. 6.20 shows the simulation results of the Test 2 after the transmitter has changed the encryption key.

Fig. 6.17 and 6.18 show the simulation results of the Test 1, and Fig. 6.19 and 6.20 show the simulation results of the Test 2, where the wavelength in the range of 1.5 to 1.6 μm. To begin with the Test 1, Fig. 6.17I(a) and I(b) show the old input bright and old input dark soliton pulses, respectively, and Fig. 6.17II(a) and II(b) show the new

input bright and new input dark soliton pulses, respectively, where the characteristics of all the bright and dark soliton pulses used in the Test 1 are shown in the Table 6.13 and 6.14. Fig. 6.17I(c) and Fig. 6.17I(d) show the old noiselike signal generated from the old bright and dark soliton pulses, and the old secret key generated from the old noiselike signal, respectively. Fig. 6.17II(c) and Fig. 6.17II(d) show the new noiselike signal generated from the new bright and dark soliton pulses, and the new secret key generated from the new noiselike signal, respectively. Fig.6.18 (a) shows the input information signal. Fig. 6.18(b) shows the new secret key. Fig. 6.18(c) shows the new encryption key generated from the new secret key. Fig. 6.18(d) shows the ciphertext in the result of the encryption used the new encryption key. Fig. 6.18(e) shows the ciphertext received by the eavesdropper. Fig. 6.18(f) shows the old secret key. Fig. 6.18(g) shows the old decryption key generated from the old secret key. Fig. 6.18(h) shows the output signal which it can be seen that the eavesdropper cannot recover the original information signal after the transmitter changes the keys. Similarly, we show the simulation results of the Test 2 in Fig. 6.19 and 6.20. The characteristics of the bright and dark soliton pulses used in the Test 2 are shown in the Table 6.13 and 6.14 too.

The simulation results have confirmed that after the transmitter changes the encryption key (rekey), then the old decryption key is not applicable to decrypt the ciphertext. This strongly confirms that even the eavesdropper can trap the noiselike signal and reproduce the correct secret and decryption keys, he still cannot decrypt the entire ciphertext if we continuously change the keys.

6.2 Technical Discussion

6.2.1 Limitation of the proposed cryptography system

The transmitter part consists of one PANDA ring resonator and two Add/drop filters (AD1 and AD2), the AD1 is used for the secret key generation, and the AD2 is used for the encryption key generation. The receiver part consists of two Add/drop filters (AD3 and AD4), the AD3 is used for the secret key generation and the AD4 is used for the decryption key generation. In order to recover the original information signal correctly at the receiver, the AD3 of the receiver must be identical to the AD1 of the transmitter as well as the AD4 of the receiver must be identical to the AD2 of the transmitter. The Table 5.6 in the previous chapter shows the used parameters of the Add/Drop filters at the receiver part (AD3 and AD4) including the refractive index (n) , the ring radius(R), the

coupling coefficient (κ_4 and κ_5) and the attenuation coefficient (α). The limits of error of these parameters due to improper fabrication will be investigated here. The simulation results shown in the Fig. 6.21-6.39 illustrate that If the receiver would like to recover the information signal correctly, the fabrication errors of the AD3 and AD4 at the receiver must be in a very limited range as shown in the Table 6.15 and 6.16, respectively.

We also measure the delay time taken in every module as well as the total delay times of the transmitter and receiver parts which they have been shown in Table 6.17 that the delay time of each module, the total delay time of the transmitter and the total delay of the receiver each is very minimum, and Fig. 6.40-6.44 show where those values come from.

Table 6.15 shows the limitation of the Add/drop filter, the AD3.

Parameters of AD3	System's Values	Limitation
Reflective index : n	3.4	$3.3999998 \leq n \leq 3.4000002$
Ring radius : R	100 μm	$99.999994 \leq R \leq 100.000008$ μm
Coupling coefficient : κ_4	0.2	$0.199 \leq \kappa_4 \leq 0.201$
Coupling coefficient: κ_5	0.2	$0.199 \leq \kappa_5 \leq 0.201$
Attenuation coefficient : α	100	$97 \leq \alpha \leq 103$

Table 6.16 shows the limitation of the Add/drop filter, the AD4.

Parameters of AD4	System's Values	Limitation
Reflective index : n	3.4	$3.3999999 \leq n \leq 3.4000001$
Ring radius : R	300 μm	$299.99999 \leq R \leq 300.00001$ μm
Coupling coefficient : κ_4	0.1	$0.080 \leq \kappa_4 \leq 0.101$
Coupling coefficient: κ_5	0.1	$0.080 \leq \kappa_5 \leq 0.101$
Attenuation coefficient : α	0	$0 \leq \alpha \leq 1$

Table 6.17 shows the delay time of the particular module .

Module	Transmitter (delay time in seconds)	Receiver (delay time in seconds)
Noiselike signal generation	14.23466667 ps	
Secret key generation	7.11733333 ps	7.11733333 ps
Encryption-decryption key generation	21.35200000 ps	21.35200000 ps
Total Delay	42.70400000 ps	28.46933333 ps

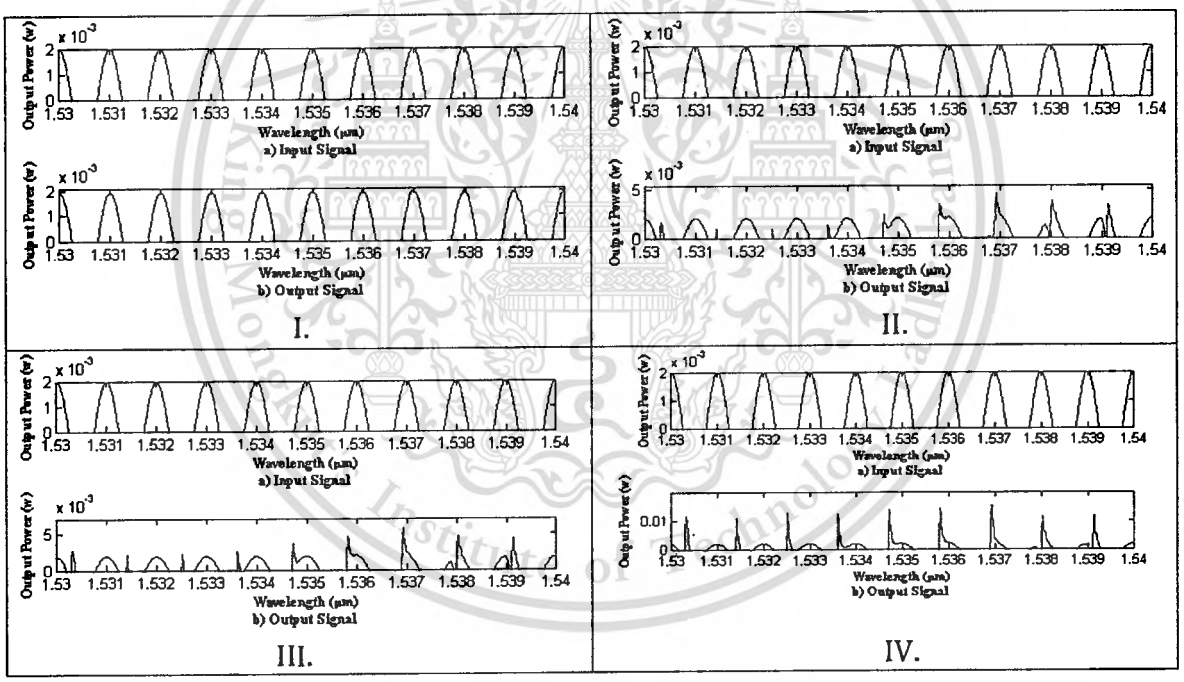

Fig. 6.21 compares the input information signal and the output signal when the *n* of the AD3 is changed, I) *n*=3.40000001, II) *n*=3.4000002, III) *n*=3.4000003 , and IV) *n* = 3.400001.

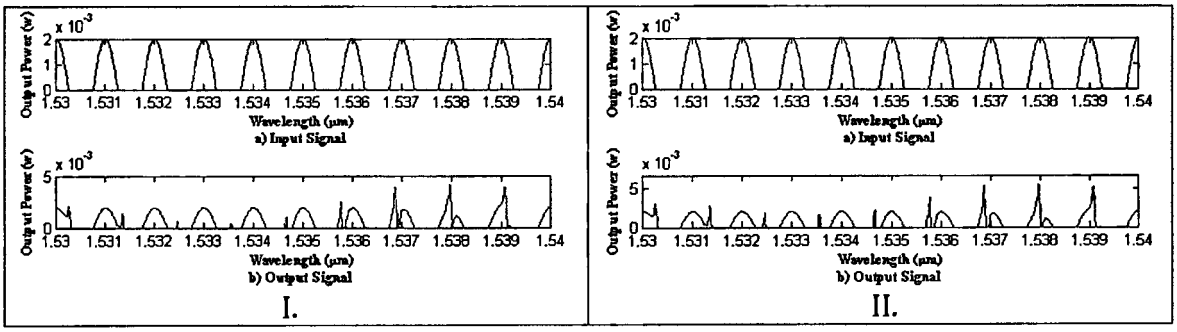

Fig. 6.22 compares the input information signal and the output signal when the *n* of the AD3 is changed, I) *n*=3.3999998, and II) *n*=3.3999997.

Fig. 6.21I, 6.21II and 6.22I show that if the refractive index (*n*) of the AD3 is *n*=3.40000001, *n*=3.4000002 and *n* = 3.3999998, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.21III and 6.22II show that if the refractive index (*n*) of the AD3 is *n* = 3.4000003, and *n* = 3.3999997, respectively, then the output signals begin to become different from the input information signals. Lastly, Fig. 6.21IV shows that if the refractive index (*n*) of the AD3 is *n* = 3.400001, then the output signals are much different from the input information signals. Thus the refractive index (*n*) of the AD3 must be in the range between 3.3999998 and 3.4000002 ($3.3999998 \leq n \leq 3.4000002$).

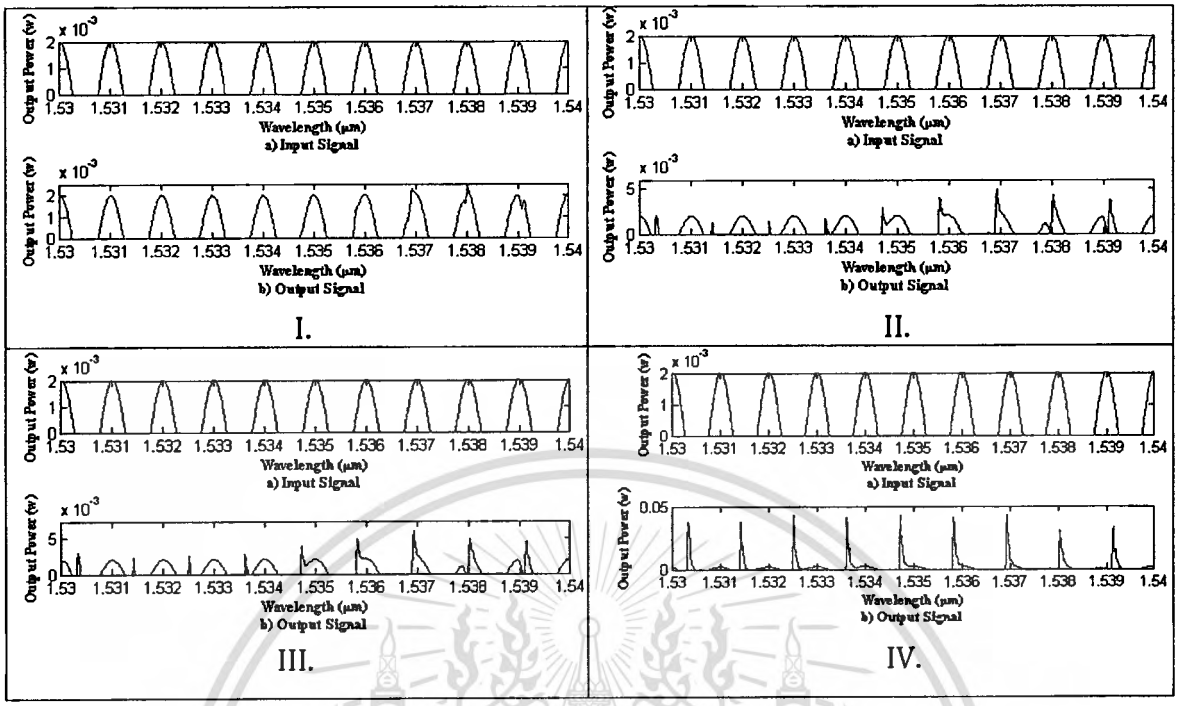

Fig. 6.23 compares the input information signal and the output signal when the *R* of the AD3 is changed, I) *R*=100.000001, II) *R*=100.000008, III) *R*=100.000009, and IV) *R*=100.00009.

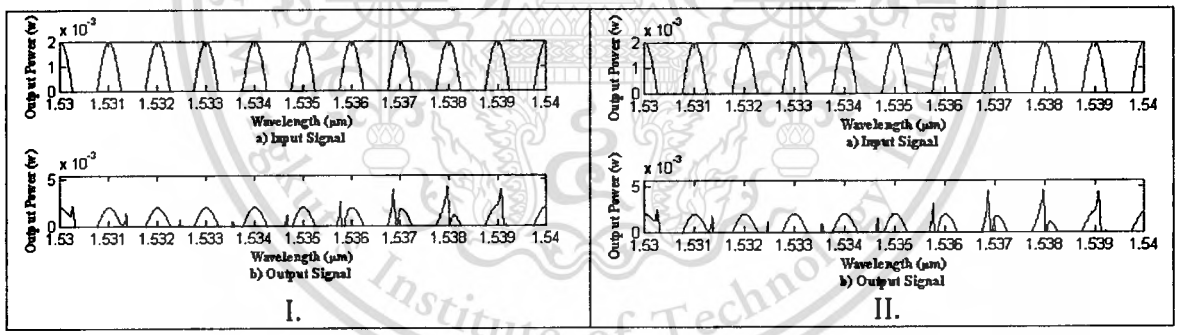

Fig. 6.24 compares the input information signal and the output signal when the *R* of the AD3 is changed, I) *R*=99.999994 ,and II) *R*=99.999993.

Fig. 6.23I, 6.23II and 6.24I show that if the ring radius (*R*) of the AD3 is *R*=100.000001, *R*=100.000008, and *R*=99.999994, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.23III and 6.24II show that if the ring radius (*R*) of the AD3 is *R*=100.000009, and *R*=99.999993, respectively, then the output signals begin to become different from the input information signals. Lastly, Fig. 6.23IV shows that if the ring radius (*R*) of the AD3 is

R=100.00009, then the output signals are much different from the input information signals. Thus the ring radius (R) of the AD3 must be in the range between 99.999994 μm and 100.000008 μm (99.999994≤ R ≤100.000008).

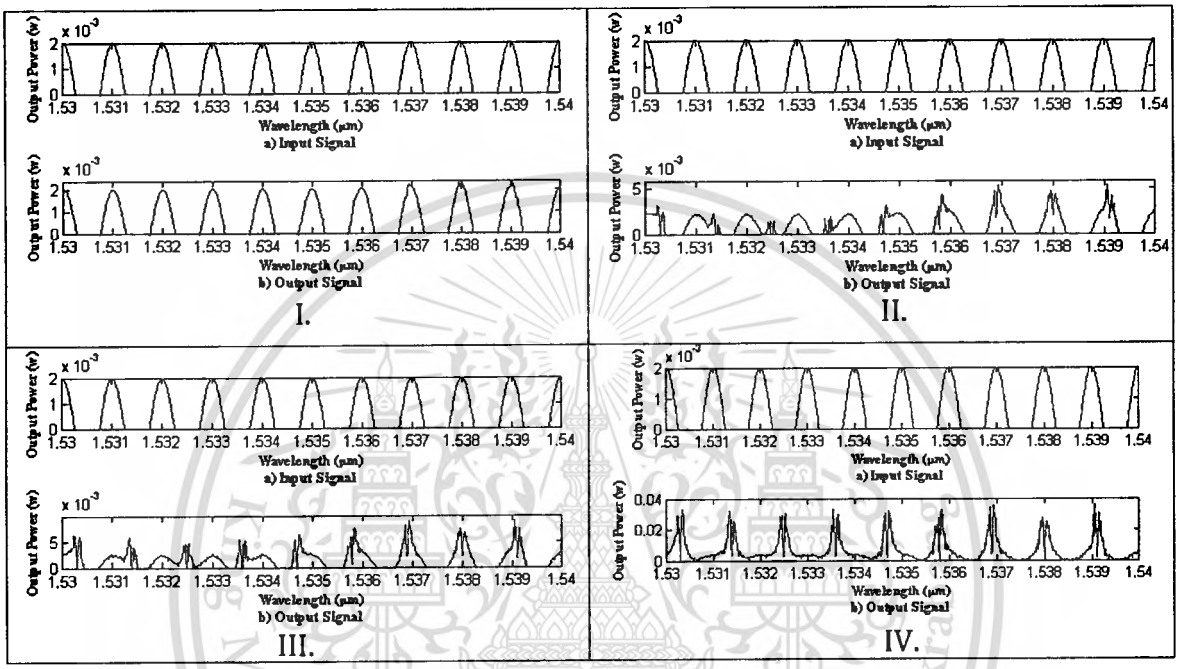

Fig. 6.25 compares the input information signal and the output signal when the κ_4 of the AD3 is changed, I) κ_4 = 0.2001, II) κ_4 = 0.201, III) κ_4= 0.202, and IV) κ_4= 0.21.

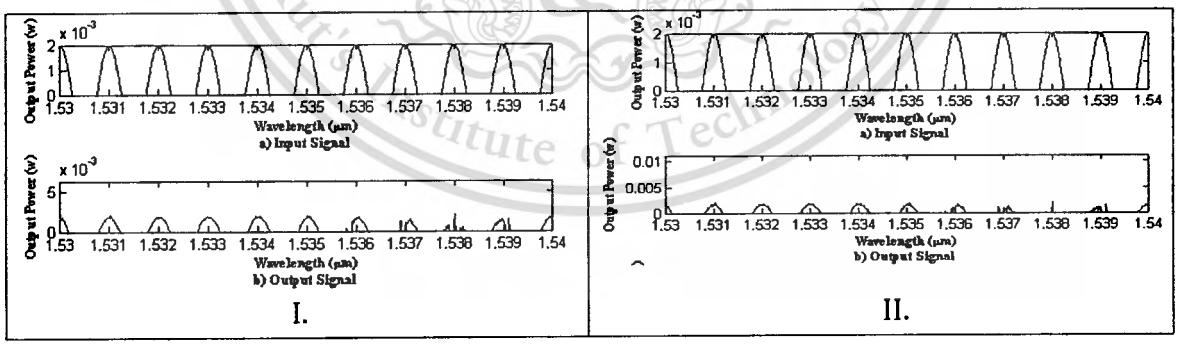

Fig. 6.26 compares the input information signal and the output signal when the κ_4 of the AD3 is changed, I) κ_4 =0.199, and II) κ_4 =0.198.

Fig. 6.25I, 6.25II and 6.26I show that if the coupling coefficient (κ_4) of the AD3 is κ_4 = 0.2001, κ_4 = 0.201, and κ_4 =0.199, respectively, then the output signals are still

recognizable when compare with the input information signals. Fig. 6.25III and 6.26II show that if the coupling coefficient (κ_4) of the AD3 is κ_4= 0.202, and κ_4 =0.198, respectively, then the output signals begin to become different from the input information signals. Lastly, Fig. 6.25IV shows that if the coupling coefficient (κ_4) of the AD3 is κ_4= 0.21, then the output signals are much different from the input information signals. Thus the coupling coefficient (κ_4) of the AD3 must be in the range between 0.199 and 0.201 ($0.199 \leq \kappa_4 \leq 0.201$).

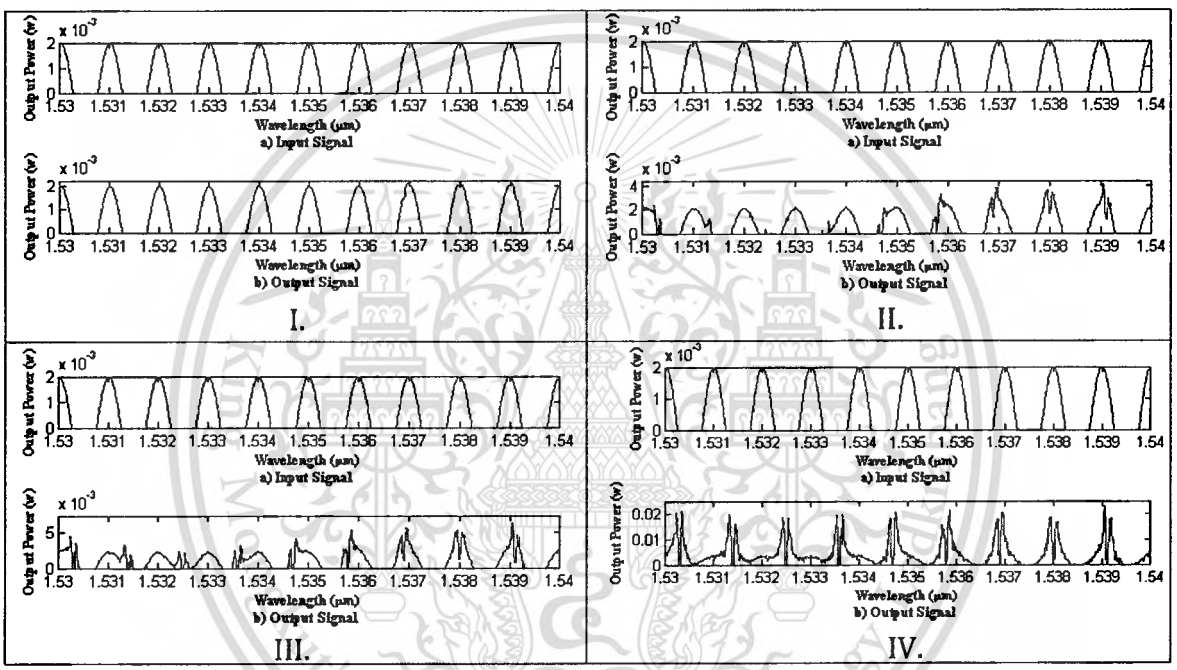

Fig. 6.27 compares the input information signal and the output signal when the κ_5 of the AD3 is changed, I) κ_5=0.2001, II) κ_5=0.201, III) κ_5= 0.202, and IV) κ_5=0.21.

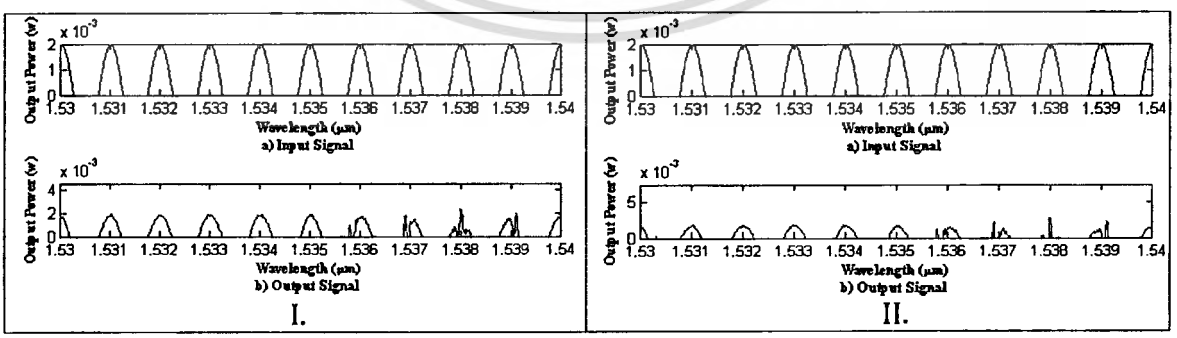

Fig. 6.28 compares the input information signal and the output signal when the κ_5 of the AD3 is changed, I) κ_5= 0.199, and II) κ_5= 0.198.

Fig. 6.27I, 6.27II and 6.28I show that if the coupling coefficient (κ_5) of the AD3 is κ_5 = 0.2001, κ_5 = 0.201, and κ_5 =0.199, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.27III and 6.28II show that if the coupling coefficient (κ_5) of the AD3 is κ_5= 0.202, and κ_5 =0.198, respectively, then the output signals begin to become different from the input information signals. Lastly, Fig. 6.27IV shows that if the coupling coefficient (κ_5) of the AD3 is κ_5= 0.21, then the output signals are much different from the input information signals. Thus the coupling coefficient (κ_5) of the AD3 must be in the range between 0.199 and 0.201 ($0.199 \leq \kappa_5 \leq 0.201$).

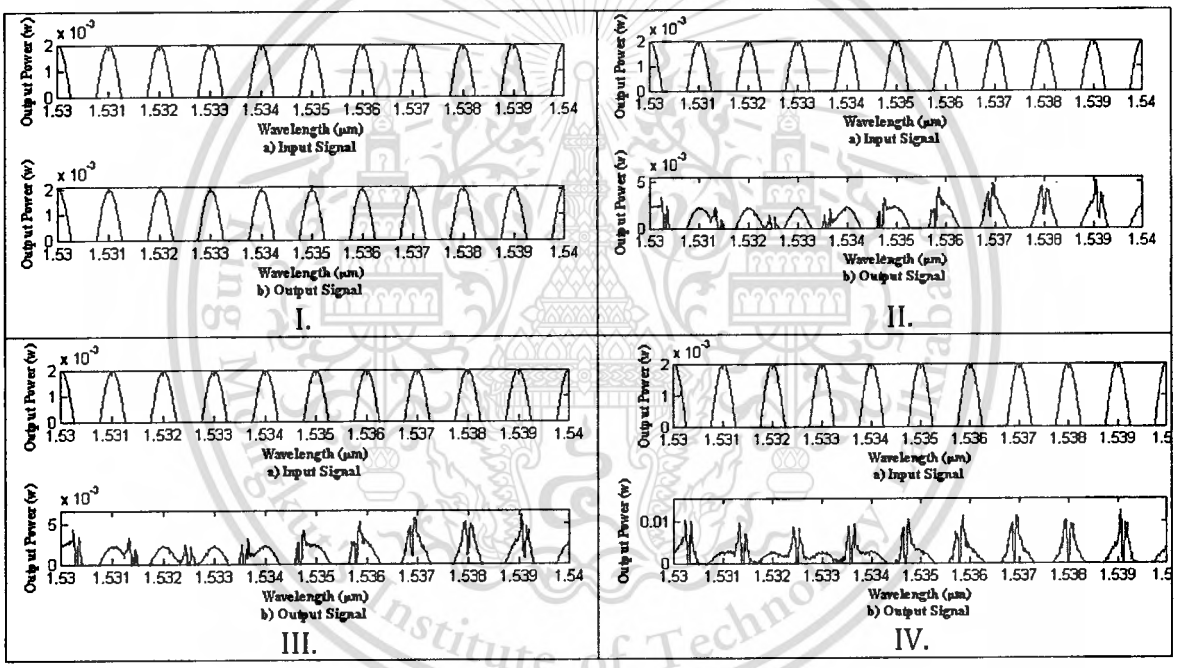

Fig. 6.29 compares the input information signal and the output signal when the α of the AD3 is changed, I) α = 100.1, II) α = 103, III) α = 104, and IV) α = 110.

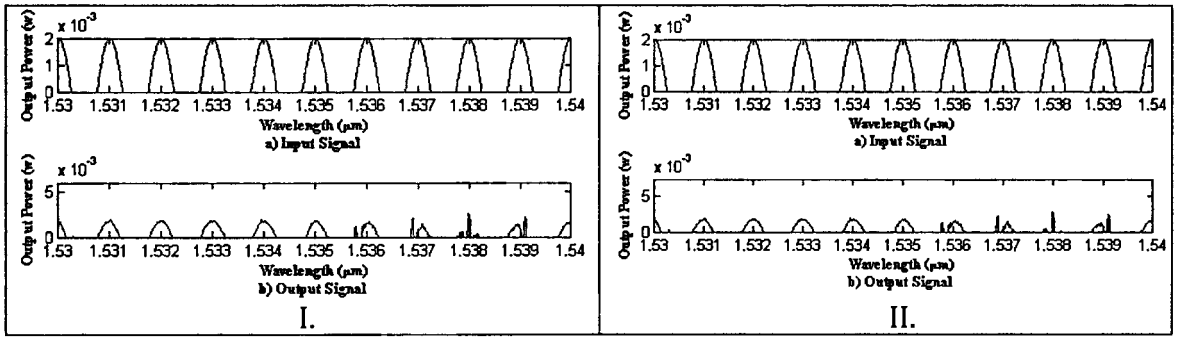

Fig. 6.30 compares the input information signal and the output signal when the α of the AD3 is changed, I) α = 97, and II) α = 96.

Fig. 6.29I, 6.29II and 6.30I show that if the attenuation coefficient (α) of the AD3 is α = 100.1, α = 103, and α = 97, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.29III and 6.30II show that if the attenuation coefficient (α) of the AD3 is α = 104, and α = 96, respectively, then the output signals begin to become different from the input information signals. Lastly, Fig. 6.29IV shows that if the attenuation coefficient (α) of the AD3 is α = 110, then the output signals are much different from the input information signals. Thus the attenuation coefficient (α) of the AD3 must be in the range between 97 and 103 ($97 \leq \alpha \leq 103$).

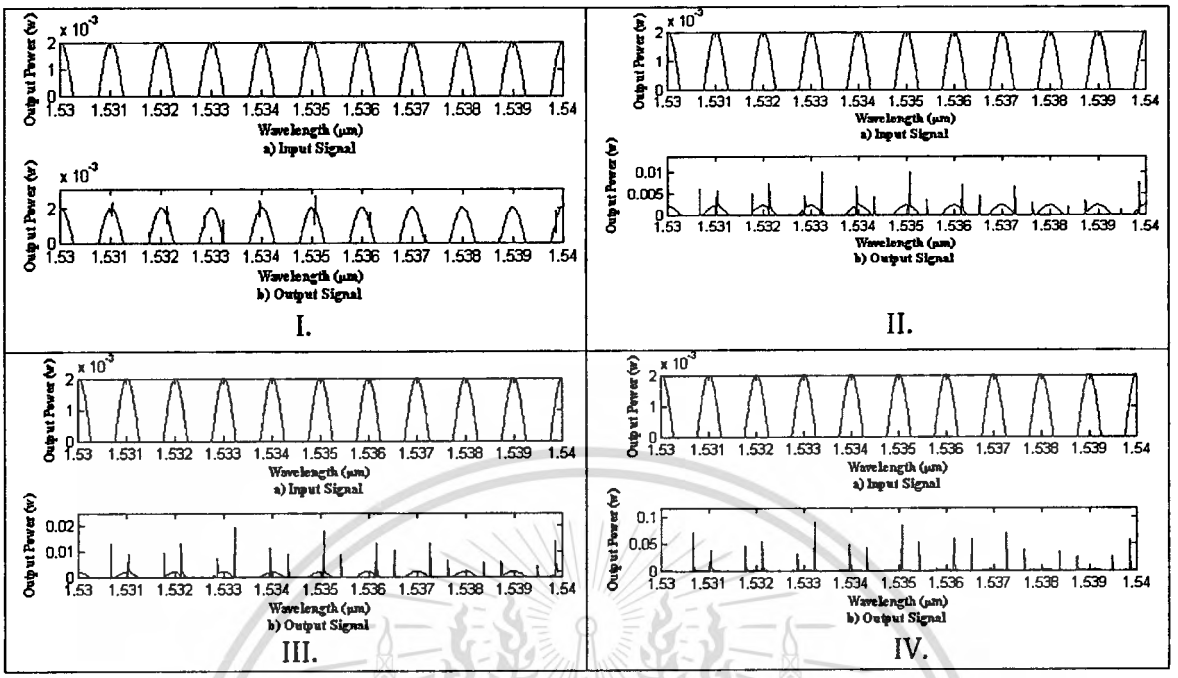

Fig. 6.31 compares the input information signal and the output signal when the *n* of the AD4 is changed, I) *n*=3.40000001, II) *n* =3.4000001, III) *n*=3.4000002, and IV) *n*= 3.400001.

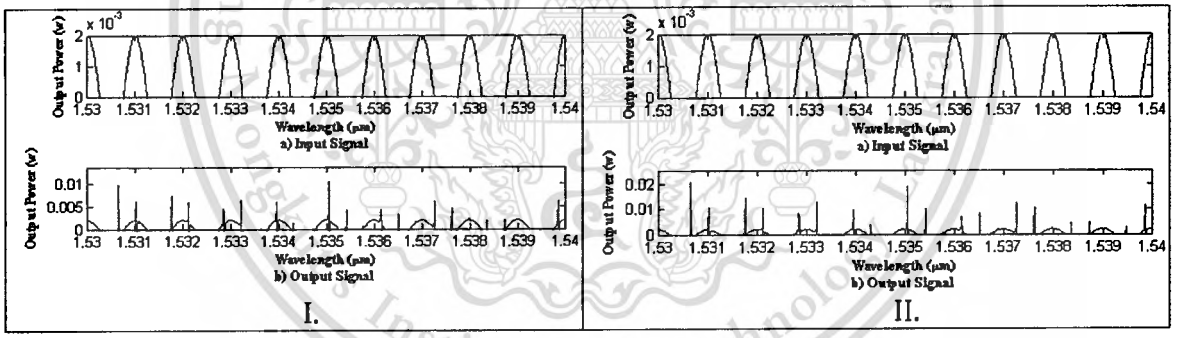

Fig. 6.32 compares the input information signal and the output signal when the *n* of the AD4 is changed, I) *n*=3.3999999,and II) *n*=3.3999998.

Fig. 6.31I, 6.31II and 6.32I show that if the refractive index (*n*) of the AD4 is *n*=3.40000001, *n*=3.4000001 and *n*=3.3999999, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.31III and 6.32II show that if the refractive index (*n*) of the AD4 is *n* = 3.4000002, and *n*= 3.3999998, respectively, then the output signals begin to become different from the input information signals. Lastly, Fig. 6.31IV shows that if the refractive index (*n*) of the AD4 is *n* = 3.400001, then the output signals are much different from the input information

signals. Thus the refractive index (n) of the AD4 must be in the range between 3.3999999 and 3.4000001 ($3.3999999 \leq n \leq 3.4000001$).

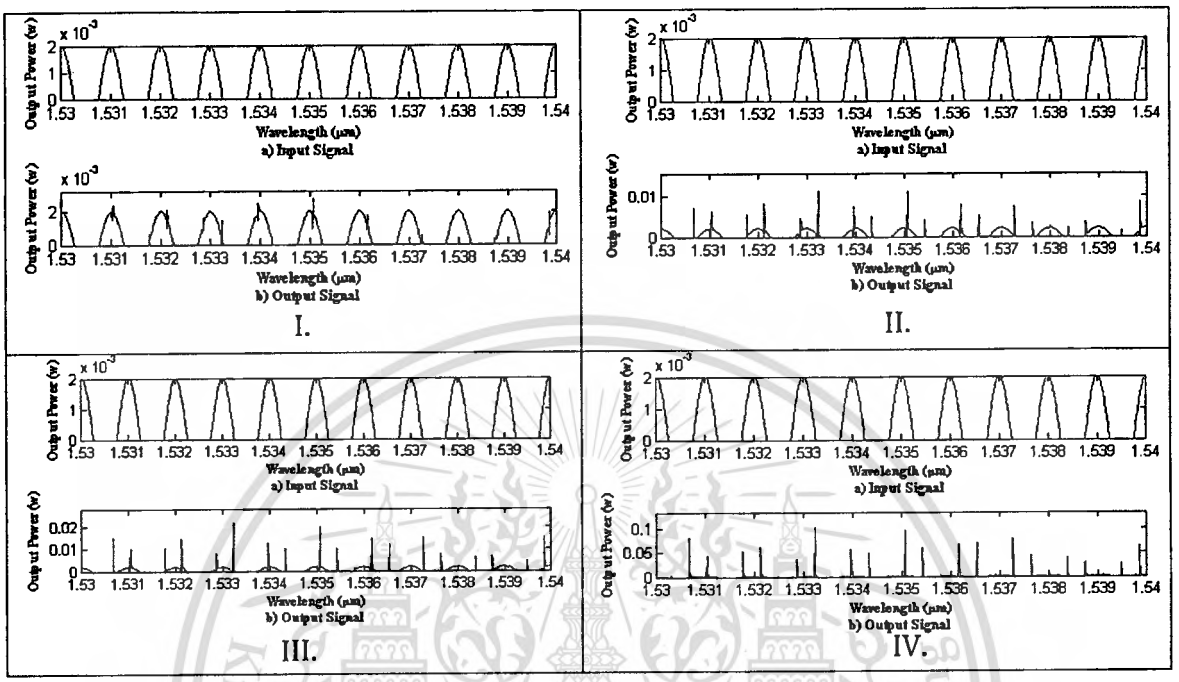

Fig. 6.33 compares the input information signal and the output signal when the R of the AD4 is changed, I) R =300.000001, II) R =300.00001, III) R =300.00002, and IV) R =300.0001.

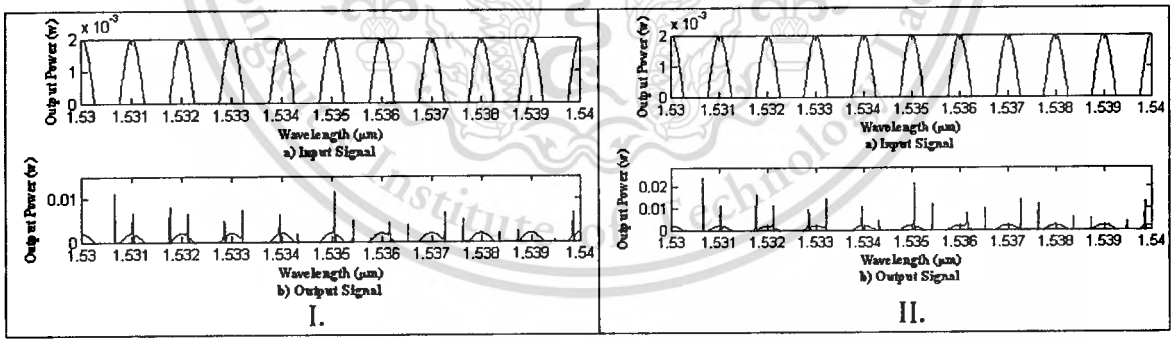

Fig. 6.34 compares the input information signal and the output signal when the R of the AD4 is changed, I) R=299.99999, and II) R=299.99998.

Fig. 6.33I, 6.33II and 6.34I show that if the ring radius (R) of the AD4 is R=300.000001, R=300.00001, and R=299.99999, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.33III and 6.34II show that if the ring radius (R) of the AD4 is R=300.00002, and R=299.99998, respectively,

then the output signals begin to become different from the input information signals. Lastly, Fig. 6.33IV shows that if the ring radius (R) of the AD4 is R=300.0001, then the output signals are much different from the input information signals. Thus the ring radius (R) of the AD4 must be in the range between 299.99999 μm and 300.00001μm ($299.99999 \leq R \leq 300.00001$).

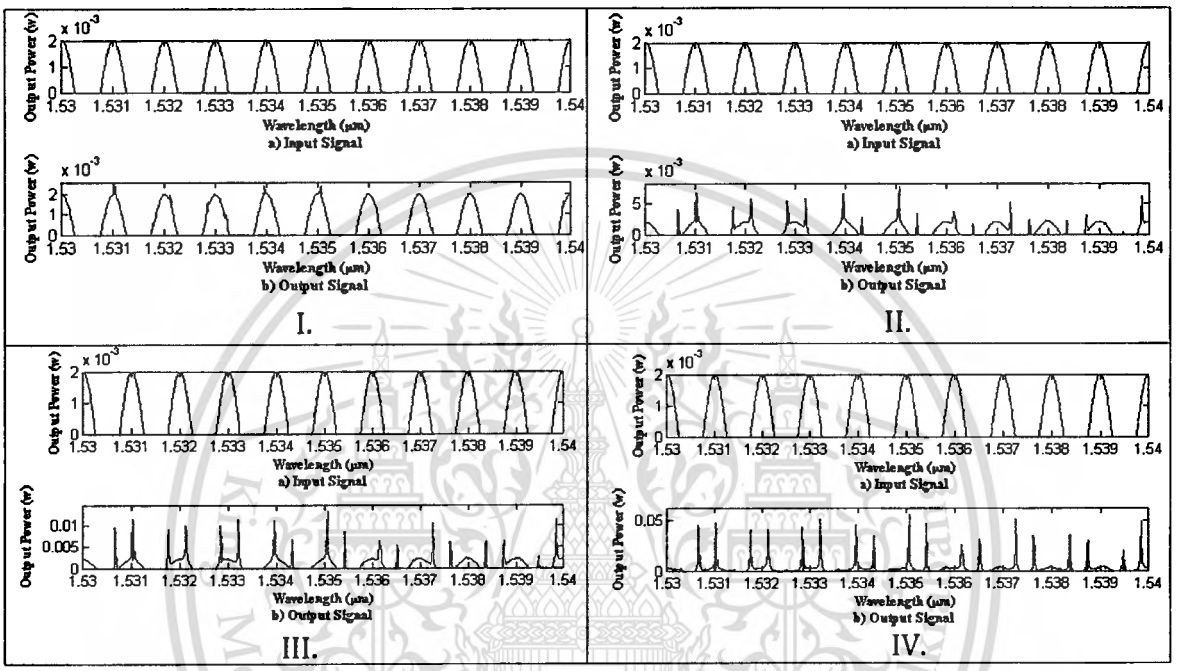

Fig. 6.35 compares the input information signal and the output signal when the κ_4 of the AD4 is changed, I) κ_4= 0.1001, II) κ_4 = 0.101, III) κ_4= 0.102 ,and IV) κ_4 = 0.11.

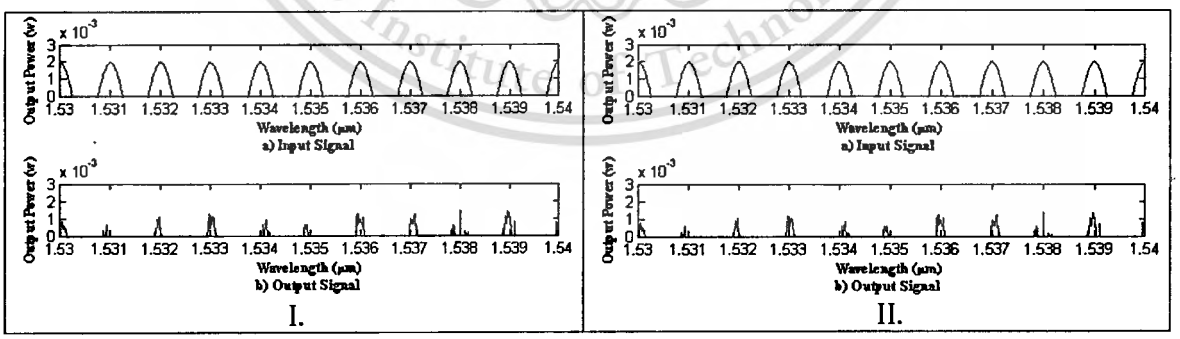

Fig. 6.36 compares the input information signal and the output signal when the κ_4 of the AD4 is changed, I) κ_4 =0.080, and II) κ_4 =0.079.

Fig. 6.35I, 6.35II and 6.36I show that if the coupling coefficient (κ_4) of the AD4 is κ_4= 0.1001, κ_4 = 0.101, and κ_4 = 0.080, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.35III and 6.36II show that if the coupling coefficient (κ_4) of the AD4 is κ_4= 0.102, and κ_4 =0.079, respectively, then the output signals begin to become different from the input information signals. Lastly, Fig. 6.35IV shows that if the coupling coefficient (κ_4) of the AD4 is κ_4= 0.11, then the output signals are much different from the input information signals. Thus the coupling coefficient (κ_4) of the AD4 must be in the range between 0.080 and 0.101 ($0.080 \leq \kappa_4 \leq 0.101$).

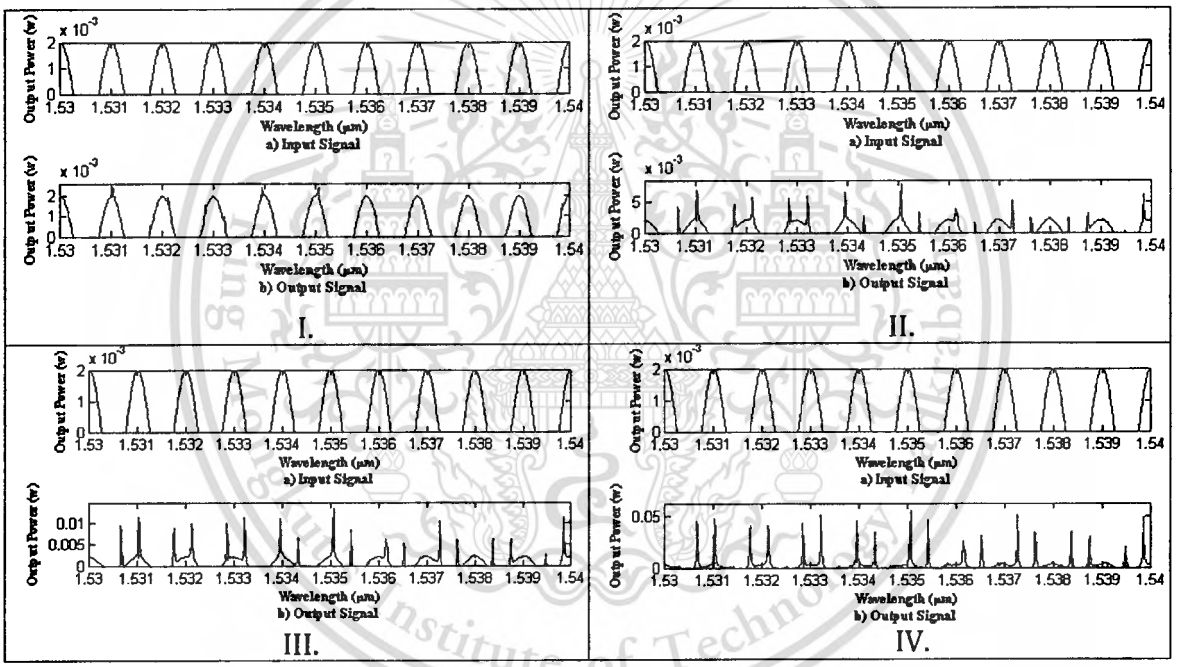

Fig. 6.37 compares the input information signal and the output signal when the κ_5 of the AD4 is changed, I) κ_5 = 0.1001, II) κ_5 = 0.101, III) κ_5 = 0.102, and IV) κ_5 = 0.11

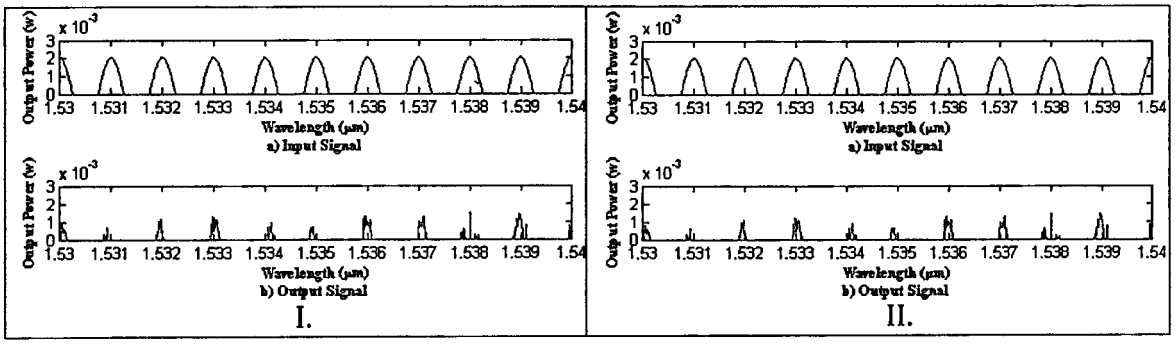

Fig. 6.38 compares the input information signal and the output signal when the κ_5 of the AD4 is changed, I) κ_5 = 0.080, and II) κ_5 = 0.079.

Fig. 6.37I, 6.37II and 6.38I show that if the coupling coefficient (κ_5) of the AD4 is κ_5 = 0.1001, κ_5 = 0.101, and κ_5 = 0.080, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.37III and 6.38II show that if the coupling coefficient (κ_5) of the AD4 is κ_5= 0.102, and κ_5 = 0.079, respectively, then the output signals begin to become different from the input information signals. Lastly, Fig. 6.37IV shows that if the coupling coefficient (κ_5) of the AD4 is κ_5= 0.11, then the output signals are much different from the input information signals. Thus the coupling coefficient (κ_5) of the AD4 must be in the range between 0.080 and 0.101 ($0.080 \leq \kappa_5 \leq 0.101$).

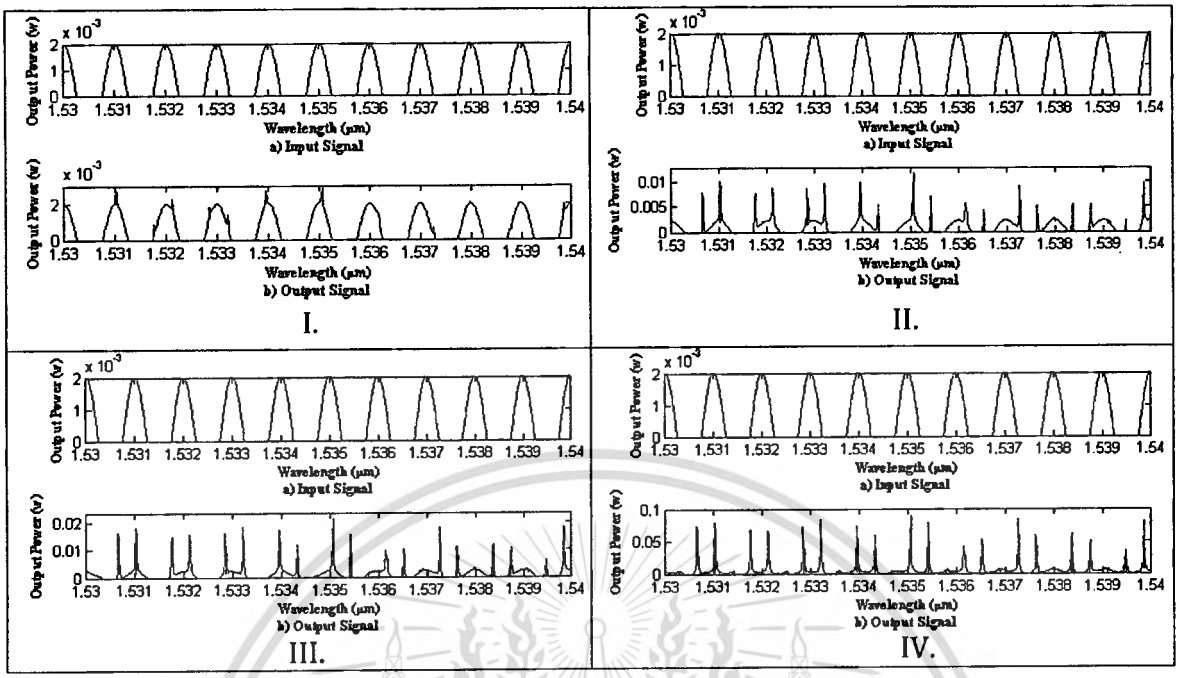

Fig. 6.39 compares the input information signal and the output signal when the α of the AD4 is changed, I) α = 0.1, II) α = 1, III) α = 2, and IV) α = 10.

Fig. 6.39I, and 6.39II show that if the attenuation coefficient (α) of the AD4 is α = 0.1, and α = 1, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.39III shows that if the attenuation coefficient (α) of the AD4 is α = 2, then the output signals begin to become different from the input information signals. Lastly, Fig. 6.39IV shows that if the attenuation coefficient of the AD4 is α = 10, then the output signals are much different from the input information signals. Thus the attenuation coefficient (α) of the AD4 must be in the range between 0 and 1 ($0 \leq \alpha \leq 1$).

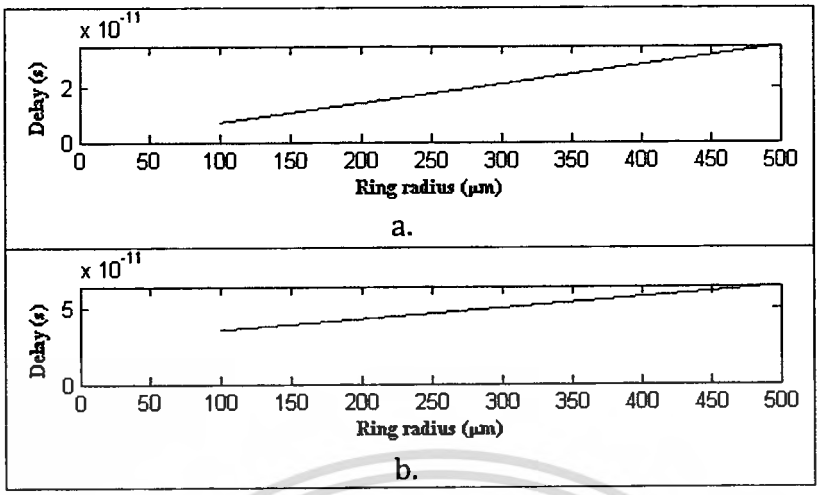

Fig. 6.40 shows the delay times of the PANDA ring resonator and the total delay times of the transmitter part.

The delay time of the PANDA ring resonator in the noiselike signal generation module is 14.23466667 ps where the radius of the center ring is 200 μm. Fig. 6.40(a) and 6.40(b) show the delay times of the PANDA ring resonator and the total delay times of the transmitter part (at particular radius), respectively, when the radius of the center ring of the PANDA ring resonator is changed in the range of 100 μm to 500 μm. It has been seen that the delay time of the PANDA ring resonator increases in proportion to the radius of its center ring.

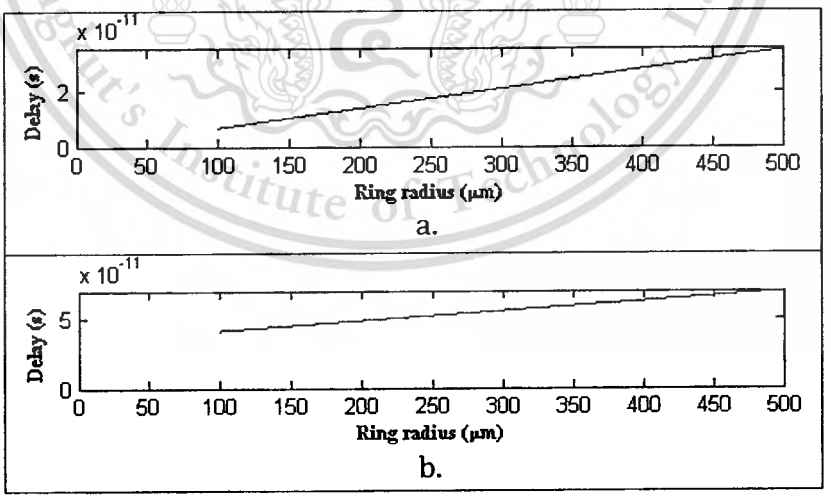

Fig. 6.41 shows the delay times of the AD1 and the total delay times of the transmitter part.

The delay time of the Add/drop filter, the AD1, in the secret key generation module at the transmitter is 7.11733333 ps where its ring radius is 100 μm. Fig. 6.41(a) and 6.41(b) show the delay times of the AD1 and the total delay times of the transmitter part (at particular ring radius of the AD1), respectively, when the ring radius of the AD1 is changed in the range of 100 μm to 500 μm. It has been seen that the delay time of the AD1 increases in proportion to its ring radius.

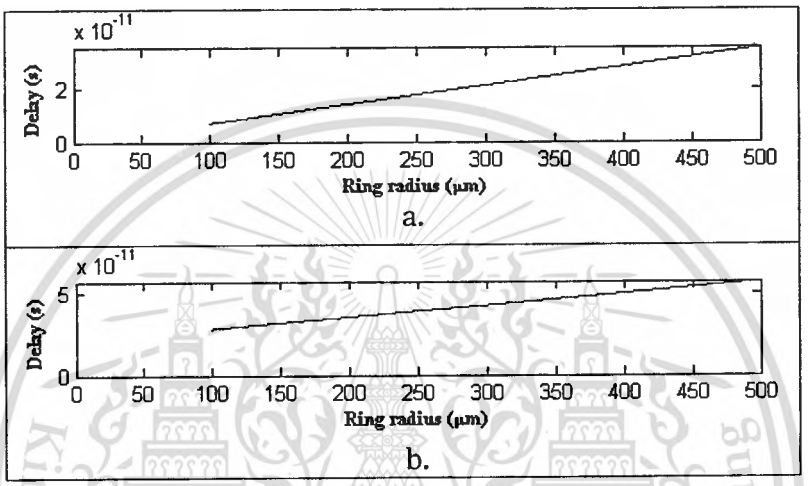

Fig. 6.42 shows the delay times of the AD2 and the total delay times of the transmitter part.

The delay time of the Add/drop filter, the AD2, in the encryption-decryption keys generation module at the transmitter is 21.35200000 ps where its ring radius is 300 μm. Fig. 6.42(a) and 6.42(b) show the delay times of the AD2 and the total delay times of the transmitter part (at particular ring radius of AD2), respectively, when the ring radius of the AD2 is changed in the range of 100 μm to 500 μm. It has been seen that the delay time of the AD2 increases in proportion to its ring radius.

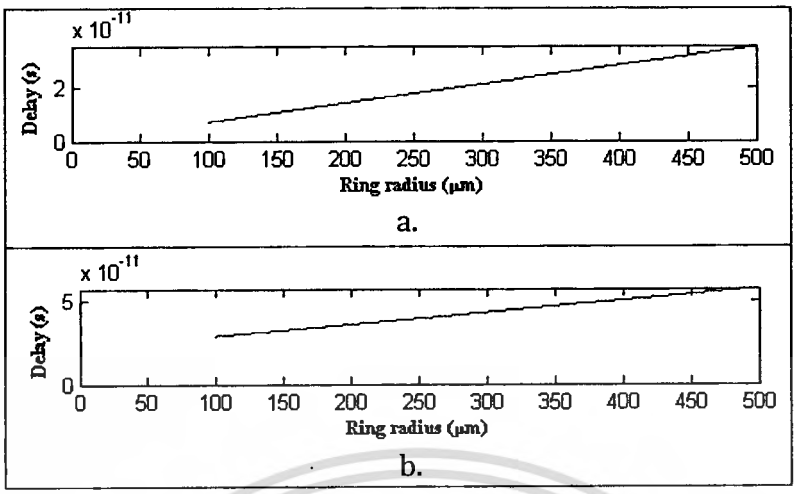

Fig. 6.43 shows the delay times of the AD3 and the total delay times of the receiver part.

The delay time of the Add/drop filter, the AD3, in the secret key generation module at the receiver is 7.11733333 ps where its ring radius is 100 μm. Fig. 6.43(a) and 6.43(b) show the delay times of the AD3 and the total delay times of the receiver part (at particular ring radius of AD3), respectively, when the ring radius of the AD3 is changed in the range of 100 μm to 500 μm. It has been seen that the delay time of the AD3 increases in proportion to its ring radius.

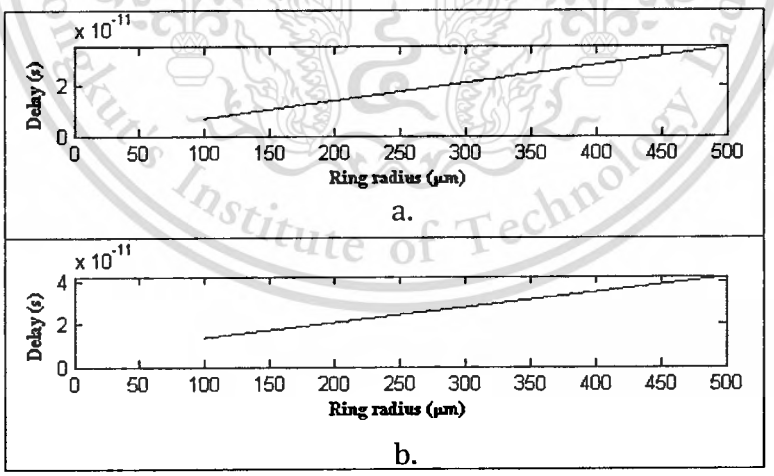

Fig. 6.44 shows the delay times of the AD4 and the total delay times of the receiver part.

The delay time of the Add/drop filter, the AD4, in the encryption-decryption keys generation module at the receiver is 21.35200000 ps where its ring radius is 300 μm. Fig.

6.44(a) and 6.44(b) show the delay times of the AD4 and the total delay times of the receiver part (at particular ring radius of AD4), respectively, when the ring radius of the AD4 is changed in the range of 100 μm to 500 μm. It has been seen that the delay time of the AD4 increases in proportion to its ring radius.

6.2.2 Security Measurement

6.2.2.1 Physical Security

In order to decrypt the cipthertext correctly, the eavesdropper must be able to trap the noiselike signal sent over the optical network which is considered very difficult. Furthermore, he must know the used parameter of both Add/drop filters used in the decryption process (the AD3 and AD4). In the previous section, we have shown the limitations of the AD3 and AD4 as illustrated in Table 6.15 and 6.16. The values beyond those shown in the Table 6.15 and 6.16 cause the receiver unable to decrypt the ciphertext or to require assistive devices. On the other hand, if the eavesdropper would like to generate the secret key and the decryption key from the noiselike signal trapped, he must build the identical Add/drop filters which all the parameters must be in the range as shown in the Table 6.15 and 6.16, otherwise, he will not be able to recover the information signal correctly even he can trap the noiselike signal. Instead of trapping the noiselike signal, the eavesdropper may generate the noiselike signal by himself using his own PANDA ring resonator as well. However, it is not easy to duplicate the PANDA ring resonator because its output is very sensitive to the variation of the parameters. If the eavesdropper would like to do so, he must duplicate the PANDA ring resonator with its values only in the range as shown in the Table 6.18, and Fig 6.45-6.64 show where those values come from.

Table 6.18 shows the limitation of the PANDA ring resonator.

Parameters of PANDA ring resonator	System's Value	Limitation
Ring radius of the center ring : R_{qd}	200 µm	$199.9997 \leq R_{qd} \leq 200.0003$ µm
Ring Radius of the right ring : R_r	100 µm	$99.9999999999999999 \leq R_r \leq 100.000000000000001$
Ring radius of the left ring : R_l	100 µm	$99.9999999999999999 \leq R_l \leq 100.000000000000001$
Refractive index (n) of the center ring.	3.4	$3.3999999 \leq n \leq 3.4000001$
Refractive index (n) of the right ring.	3.4	$3.39999999999999999 \leq n \leq 3.40000000000000001$
Refractive index (n) of the left ring.	3.4	$3.39999999999999999 \leq n \leq 3.40000000000000001$
Coupling coefficient : κ_0	0.2	$0.199999999999999999 \leq \kappa_0 \leq 0.200000000000000001$
Coupling coefficient : κ_1	0.2	$0.196 \leq \kappa_1 \leq 0.21$
Coupling coefficient : κ_2	0.2	$0.199 \leq \kappa_2 \leq 0.201$
Coupling coefficient : κ_3	0.2	$0.199999999999999999 \leq \kappa_3 \leq 0.200000000000000001$

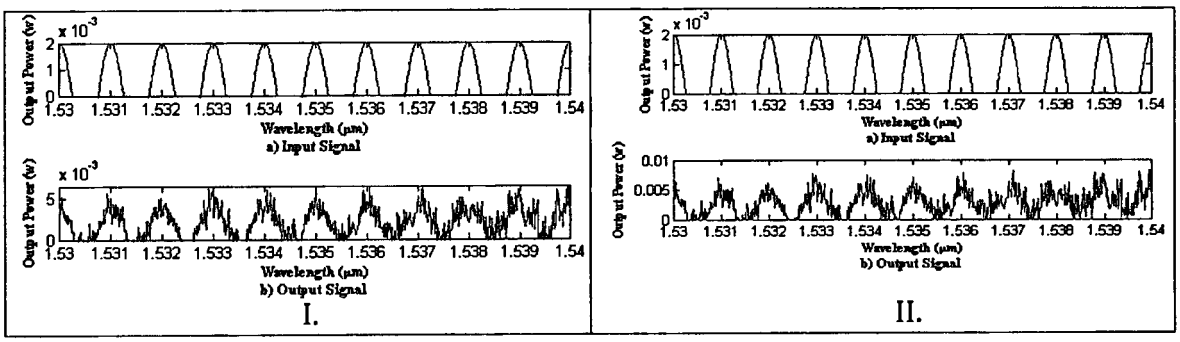

Fig. 6.45 compares the input information signal and the output signal when the R_{ad} of the PANDA ring resonator is changed, I) R_{ad} = 200.0003,and II) R_{ad} = 200.0004.

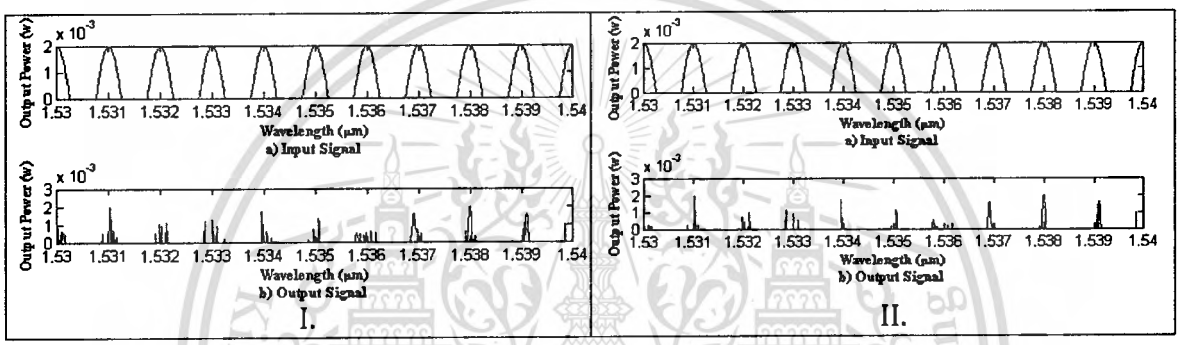

Fig. 6.46 compares the input information signal and the output signal when the R_{ad} of the PANDA ring resonator is changed, I) R_{ad} = 199.9997, and II) R_{ad} = 199.9996.

Fig. 6.45I, and 6.46I show that if the ring radius of the center ring of the PANDA ring resonator is R_{ad} = 200.0003 and R_{ad} = 199.9997, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.45II and 6.46II show that if the ring radius of the center ring of the PANDA ring resonator is R_{ad} = 200.0004 and R_{ad} = 199.9996, respectively, then the output signals begin to become different from the input information signals. Thus if the eavesdropper would like to recover the original information signals correctly, he must use the ring radius of the center ring of the PANDA ring resonator as in the range between 199.9997 μm and 200.0003 μm (199.9997≤ R_{ad} ≤200.0003).

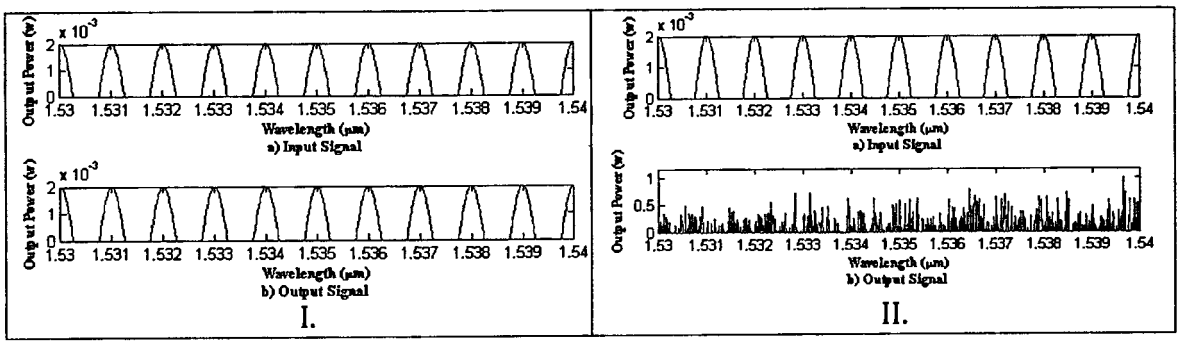

Fig. 6.47 compares the input information signal and the output signal when the R_r of the PANDA ring resonator is changed, I) R_r = 100.00000000000001,and II) R_r = 100.0000000000001.

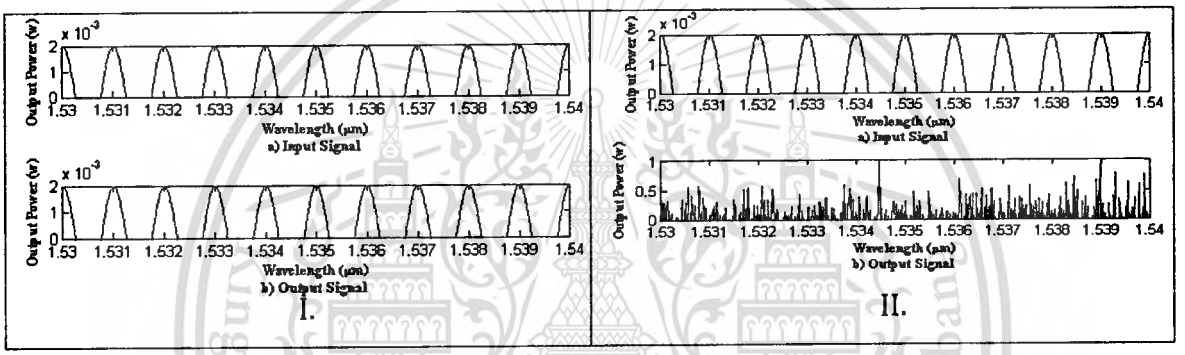

Fig. 6.48 compares the input information signal and the output signal when the R_r of the PANDA ring resonator is changed, I) R_r = 99.999999999999999,and II) R_r = 99.99999999999999.

Fig. 6.47I, and 6.48I show that if the ring radius of the right ring of the PANDA ring resonator is R_r = 100.00000000000001 and R_r = 99.999999999999999, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.47II and 6.48II show that if the ring radius of the right ring of the PANDA ring resonator is R_r = 100.0000000000001 and R_r = 99.99999999999999, respectively, then the output signals begin to become different from the input information signals. Thus if the eavesdropper would like to recover the original information signals correctly, he must use the ring radius of the right ring of the PANDA ring resonator as in the range between 99.999999999999999 μm and 100.00000000000001 μm ($99.999999999999999 \leq R_r \leq 100.00000000000001$).

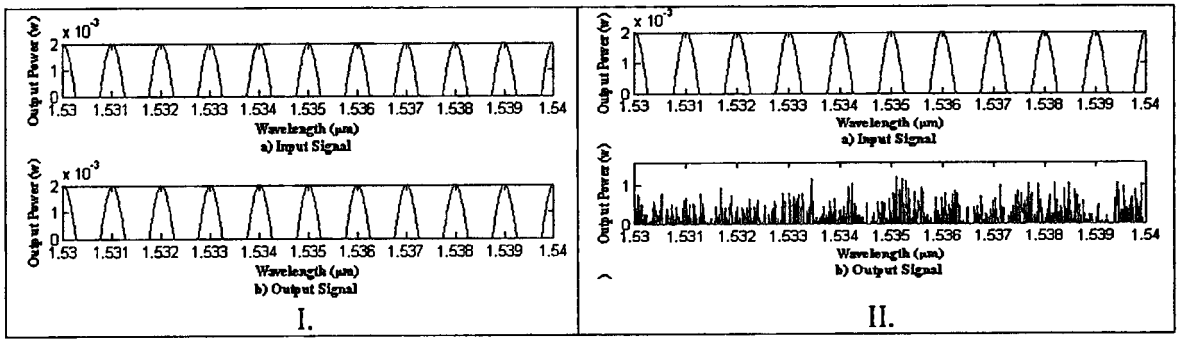

Fig. 6.49 compares the input information signal and the output signal when the R_t of the PANDA ring resonator is changed, I) R_t = 100.00000000000001, and II) R_t = 100.0000000000001.

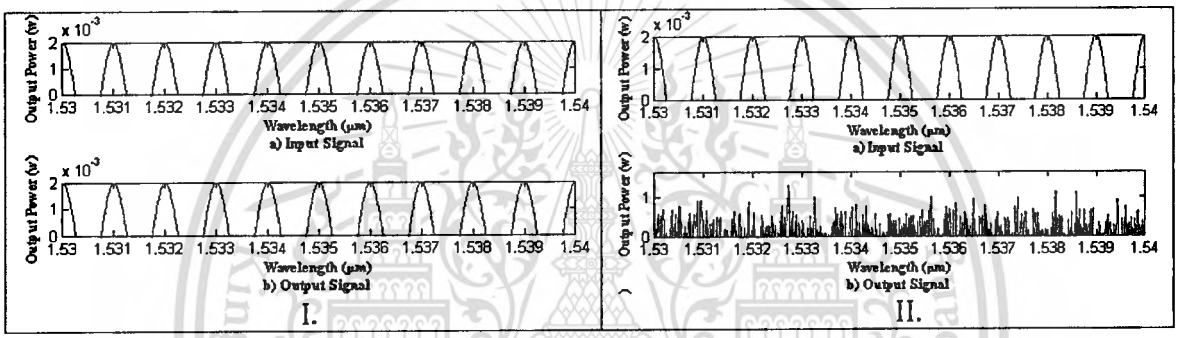

Fig. 6.50 compares the input information signal and the output signal when the R_t of the PANDA ring resonator is changed, I) R_t = 99.999999999999999, and II) R_t = 99.99999999999999.

Fig. 6.49I, and 6.50I show that if the ring radius of the left ring of the PANDA ring resonator is R_t = 100.00000000000001 and R_t = 99.999999999999999, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.49II and 6.50II show that if the ring radius of the left ring of the PANDA ring resonator is R_t = 100.0000000000001 and R_t = 99.99999999999999, respectively, then the output signals begin to become different from the input information signals. Thus if the eavesdropper would like to recover the original information signals correctly, he must use the ring radius of the left ring of the PANDA ring resonator as in the range between 99.999999999999999 μm and 100.00000000000001 μm ($99.999999999999999 \leq R_t \leq 100.00000000000001$).

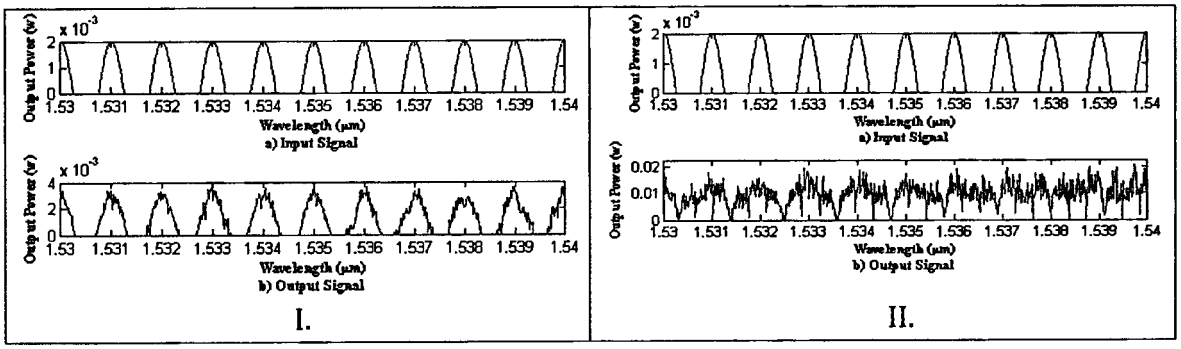

Fig. 6.51 compares the input information signal and the output signal when the refractive index (n) of the center ring of the PANDA ring resonator is changed, I) n = 3.4000001, and II) n = 3.400001.

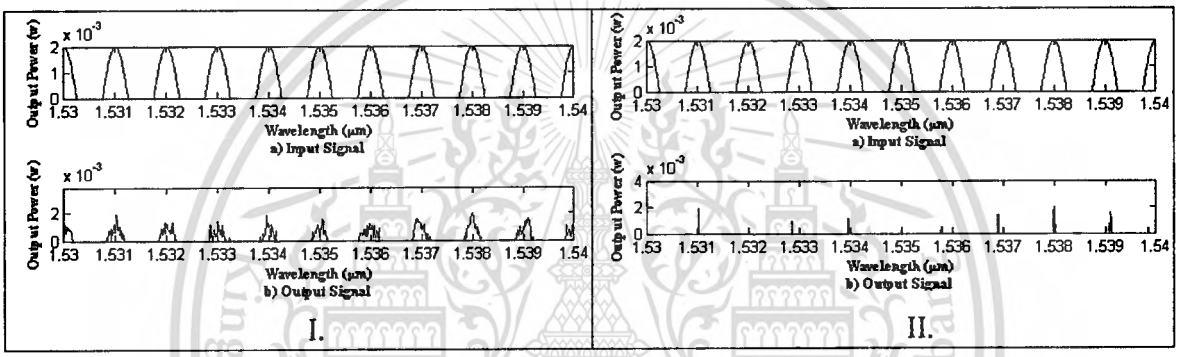

Fig. 6.52 compares the input information signal and the output signal when the refractive index (n) of the center ring of the PANDA ring resonator is changed, I) n = 3.3999999, and II) n = 3.399999.

Fig. 6.51I, and 6.52I show that if the refractive index (n) of the center ring of the PANDA ring resonator is n = 3.4000001 and n = 3.3999999, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.51II and 6.52II show that if the refractive index (n) of the center ring of the PANDA ring resonator is n = 3.400001 and n = 3.399999, respectively, then the output signals begin to become different from the input information signals. Thus if the eavesdropper would like to recover the original information signals correctly, he must use the refractive index (n) of the center ring of the PANDA ring resonator as in the range between 3.3999999 and 3.4000001 ($3.3999999 \leq n \leq 3.4000001$).

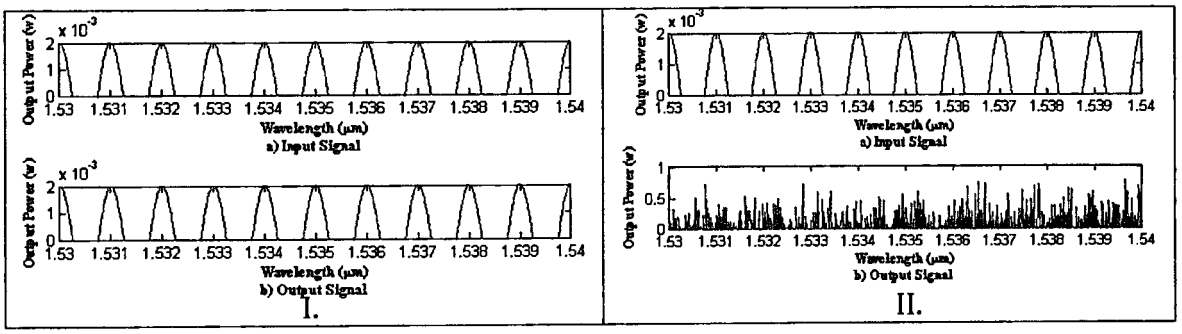

Fig. 6.53 compares the input information signal and the output signal when the refractive index (n) of the right ring of the PANDA ring resonator is changed, I) n = 3.4000000000000001, and II) n = 3.400000000000001.

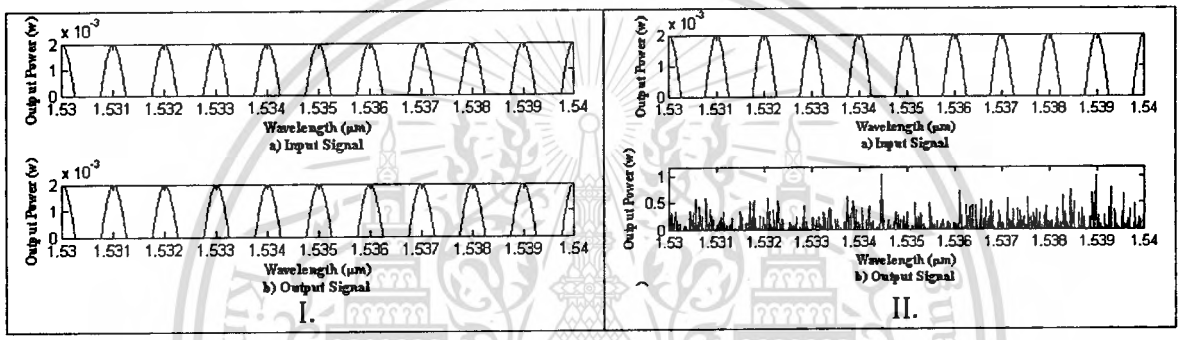

Fig. 6.54 compares the input information signal and the output signal when the refractive index (n) of the right ring of the PANDA ring resonator is changed, I) n = 3.3999999999999999, and II) n = 3.399999999999999.

Fig. 6.53I, and 6.54I show that if the refractive index (n) of the right ring of the PANDA ring resonator is n = 3.4000000000000001 and n = 3.3999999999999999, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.53II and 6.54II show that if the refractive index (n) of the right ring of the PANDA ring resonator is n = 3.400000000000001, and n = 3.399999999999999, respectively, then the output signals begin to become different from the input information signals. Thus if the eavesdropper would like to recover the original information signals correctly, he must use the refractive index (n) of the right ring of the PANDA ring resonator as in the range between 3.3999999999999999 and 3.4000000000000001 ($3.3999999999999999 \leq n \leq 3.4000000000000001$).

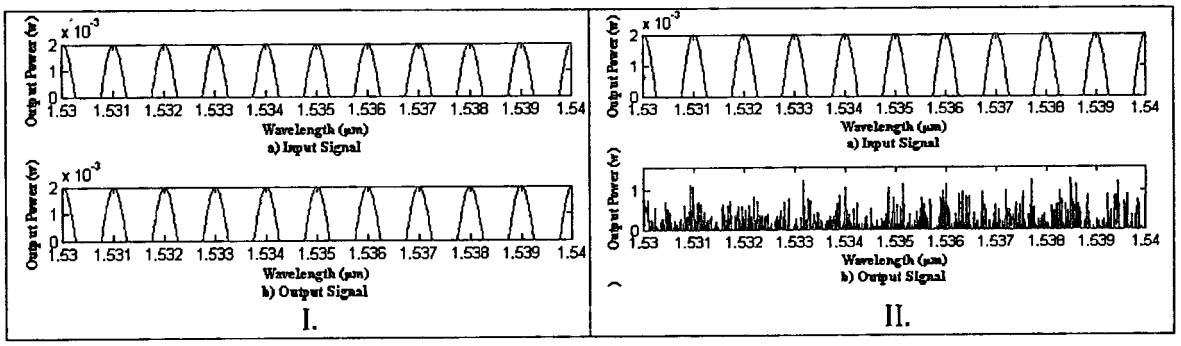

Fig. 6.55 compares the input information signal and the output signal when the refractive index (n) of the left ring of the PANDA ring resonator is changed, I) n = 3.4000000000000001, and II) n = 3.400000000000001.

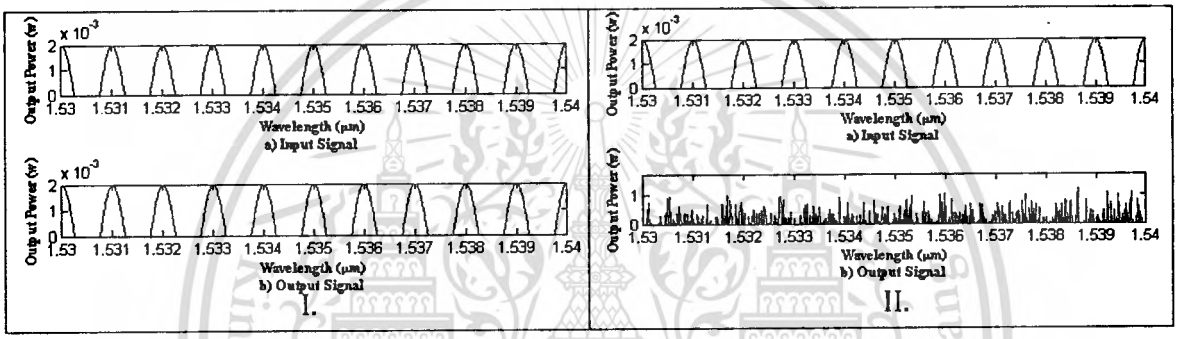

Fig. 6.56 compares the input information signal and the output signal when the refractive index (n) of the left ring of the PANDA ring resonator is changed, I) n = 3.3999999999999999, and II) n = 3.399999999999999.

Fig. 6.55I, and 6.56I show that if the refractive index (n) of the left ring of the PANDA ring resonator is n = 3.4000000000000001 and n = 3.3999999999999999, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.55II and 6.56II show that if the refractive index (n) of the left ring of the PANDA ring resonator is n = 3.400000000000001 and n = 3.399999999999999, respectively, then the output signals begin to become different from the input information signals. Thus if the eavesdropper would like to recover the original information signals correctly, he must use the refractive index (n) of the left ring of the PANDA ring resonator as in the range between 3.3999999999999999 and 3.4000000000000001 ($3.3999999999999999 \leq n \leq 3.4000000000000001$).

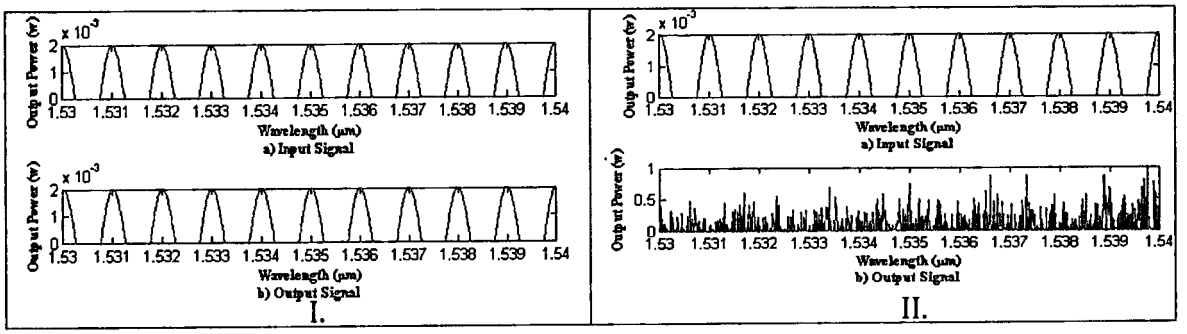

Fig. 6.57 compares the input information signal and the output signal when the κ_0 of the PANDA ring resonator is changed, I) κ_0 = 0.20000000000000001, and II) κ_0 = 0.2000000000000001.

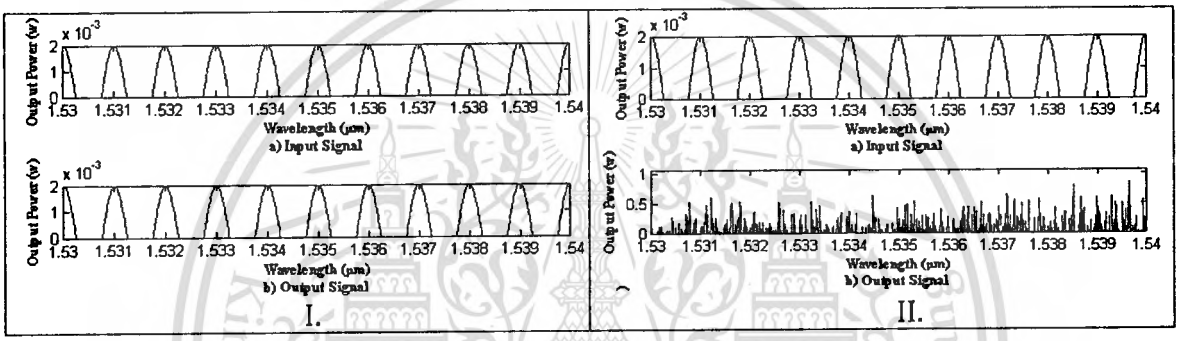

Fig. 6.58 compares the input information signal and the output signal when the κ_0 of the PANDA ring resonator is changed, I) κ_0 = 0.19999999999999999, and II) κ_0 = 0.1999999999999999.

Fig. 6.57I, and 6.58I show that if the coupling coefficient (κ_0) of the PANDA ring resonator is κ_0 = 0.20000000000000001 and κ_0 = 0.19999999999999999, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.57II and 6.58II show that if the coupling coefficient (κ_0) of the PANDA ring resonator is κ_0 = 0.2000000000000001 and κ_0 = 0.1999999999999999, respectively, then the output signals begin to become different from the input information signals. Thus if the eavesdropper would like to recover the original information signals correctly, he must use the coupling coefficient (κ_0) of the PANDA ring resonator as in the range between 0.19999999999999999 and 0.20000000000000001 ($0.19999999999999999 \leq \kappa_0 \leq 0.20000000000000001$).

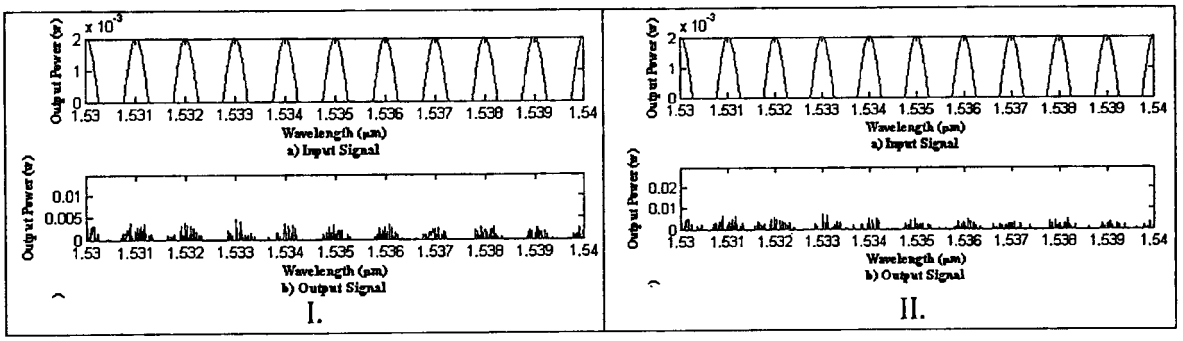

Fig. 6.59 compares the input information signal and the output signal when the κ_1 of the PANDA ring resonator is changed, I) κ_1 = 0.21, and II) κ_1 = 0.22.

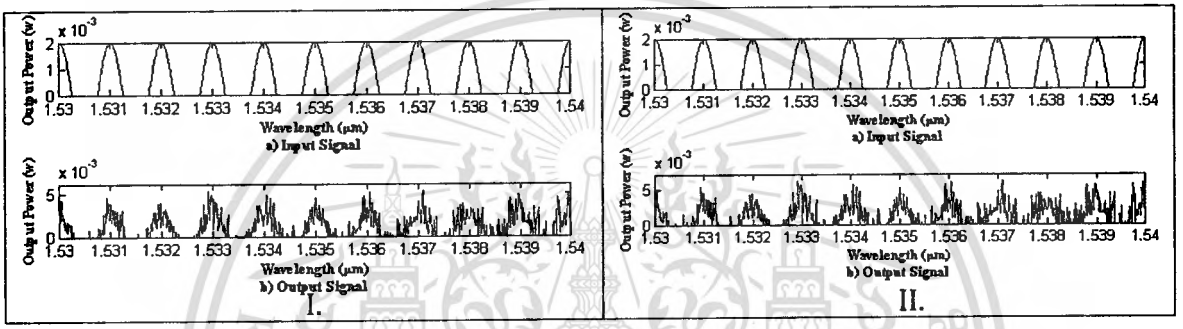

Fig. 6.60 compares the input information signal and the output signal when the κ_1 of the PANDA ring resonator is changed, I) κ_1 = 0.196, and II) κ_1 = 0.195.

Fig. 6.59I, and 6.60I show that if the coupling coefficient (κ_1) of the PANDA ring resonator is κ_1 = 0.21 and κ_1 = 0.196, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.59II and 6.60II show that if the coupling coefficient (κ_1) of the PANDA ring resonator is κ_1 = 0.22 and κ_1 = 0.195, respectively, then the output signals begin to become different from the input information signals. Thus if the eavesdropper would like to recover the original information signals correctly, he must use the coupling coefficient (κ_1) of the PANDA ring resonator as in the range between 0.196 and 0.21 ($0.196 \leq \kappa_1 \leq 0.21$).

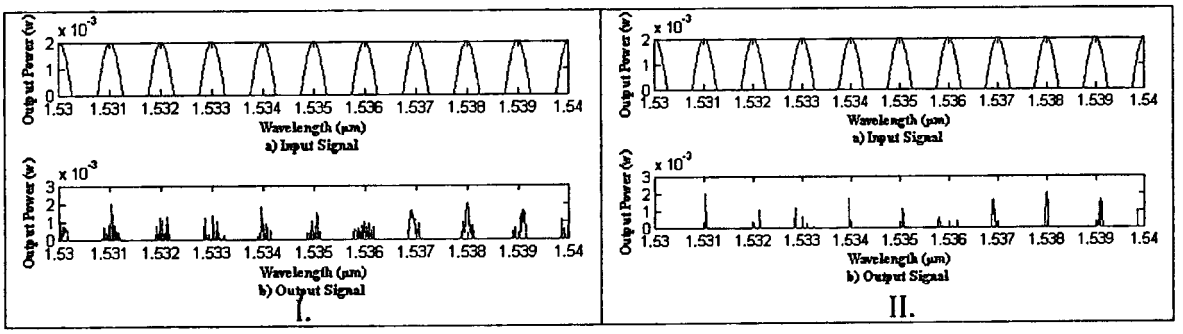

Fig. 6.61 compares the input information signal and the output signal when the κ_2 of the PANDA ring resonator is changed, I) κ_2 = 0.201, and II) κ_2 = 0.202

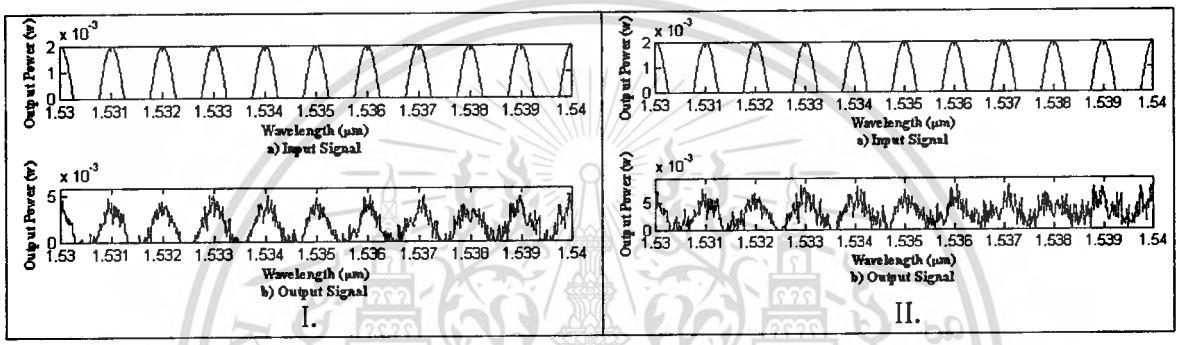

Fig. 6.62 compares the input information signal and the output signal when the κ_2 of the PANDA ring resonator is changed, I) κ_2 = 0.199, and II) κ_2 = 0.198.

Fig. 6.61I, and 6.62I show that if the coupling coefficient (κ_2) of the PANDA ring resonator is κ_2 = 0.201 and κ_2 = 0.199, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.61II and 6.62II show that if the coupling coefficient (κ_2) of the PANDA ring resonator is κ_2 = 0.202 and κ_2 = 0.198, respectively, then the output signals begin to become different from the input information signals. Thus if the eavesdropper would like to recover the original information signals correctly, he must use the coupling coefficient (κ_2) of the PANDA ring resonator as in the range between 0.199 and 0.201 ($0.199 \leq \kappa_2 \leq 0.201$).

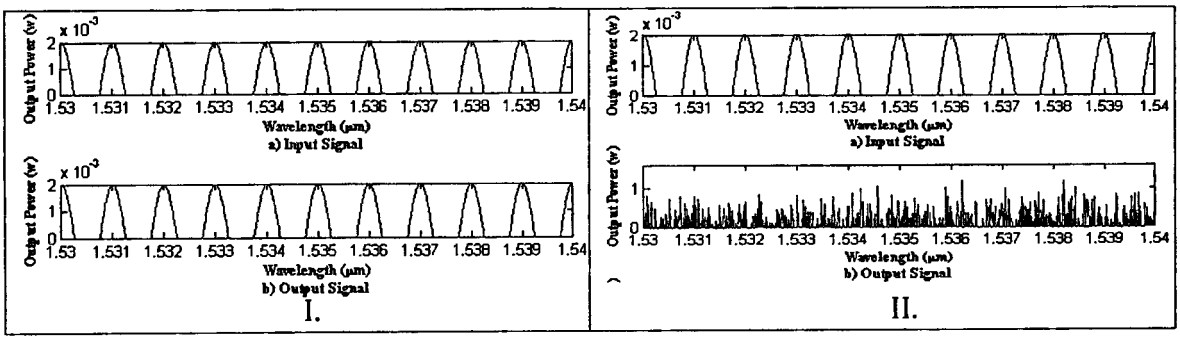

Fig. 6.63 compares the input information signal and the output signal when the κ_3 of the PANDA ring resonator is changed, I) κ_3 = 0.20000000000000001, and II) κ_3 = 0.2000000000000001.

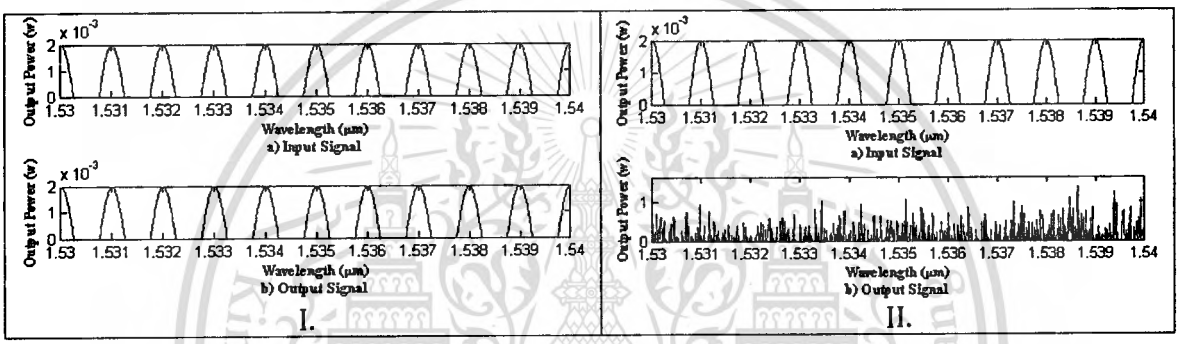

Fig. 6.64 compares the input information signal and the output signal when the κ_3 of the PANDA ring resonator is changed, I) κ_3 = 0.19999999999999999, and II) κ_3 = 0.1999999999999999.

Fig. 6.63I, and 6.64I show that if the coupling coefficient (κ_3) of the PANDA ring resonator is κ_3 = 0.20000000000000001 and κ_3 = 0.19999999999999999, respectively, then the output signals are still recognizable when compare with the input information signals. Fig. 6.63II and 6.64II show that if the coupling coefficient (κ_3) of the PANDA ring resonator is κ_3 = 0.2000000000000001 and κ_3 = 0.1999999999999999, respectively, then the output signals begin to become different from the input information signals. Thus if the eavesdropper would like to recover the original information signals correctly, he must use the coupling coefficient (κ_3) of the PANDA ring resonator as in the range between 0.19999999999999999 and 0.20000000000000001 ($0.19999999999999999 \leq \kappa_3 \leq 0.20000000000000001$).

6.2.2.2 Security of the additive masking.

We use the additive masking approach to form the noiselike communication which it has been confirmed in the experiment 2 that the cipthertexts obtained are random, broad and flat which are similar to the broadband noise (undesired signals that covers a large portion of the spectrum of interest). The additive masking approach uses the broadband noiselike signal to hide the information signal from the eavesdropper using the additive operation. With the additive masking approach, in order to bury the information signal into the noiselike signal, the signal power of the noiselike signal must be higher than the information signal at least 10x [117]. Fig 6.65I-IV show the power spectrum of the ciphertext when the signal power of the encryption key (derived inherently from the noiselike signal) is higher than the information signal, 1000x,10x, 5x and 2x ,respectively.

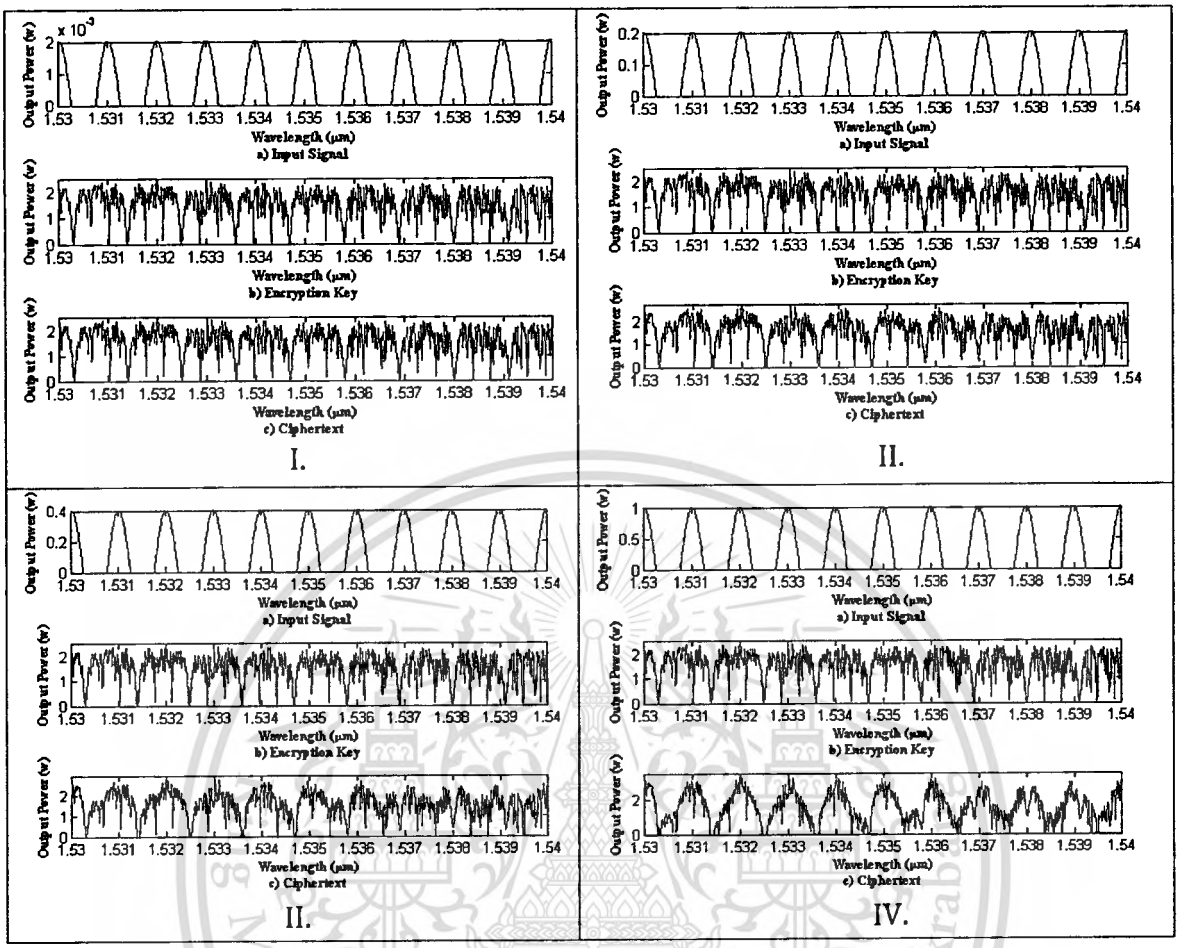

Fig. 6.65 show the simulation results of the additive marking when the signal power of the encryption key is 1000x,10x,5x, and 2x, respectively.

Fig. 6.65I and II have shown that If the signal power of the encryption key is much higher than the signal power of the information signal, 1000x and 10x, respectively, then it can completely hide the information signals which makes the eavesdropper unable to detect the presence of the information signals. Moreover, Fig. 6.65 III and IV have also confirmed that if the signal power of the encryption key is not much higher than the signal power of the information signals, 5x and 2x, respectively, then the presence of the information signal can be easily detected. In conclusion, the signal power of the encryption key must be higher than the signal power of the information signal at least 10x , this is also confirmed by [117]. The signal power of the encryption key of our proposed cryptography system is 1000X higher that the signal power of the input information signal as shown in the Fig. 6.65I.

6.2.3 Cryptography properties

After the new cryptography system has been designed, it should always be evaluated by some basic security analysis. Although, this analysis cannot comprise all possible attacks against the new cipher, this analysis helps to spot and correct defects and flaws before the new scheme is published. First of all, to prevent common attacks, the designed cryptosystem should have the five basic cryptographic properties as shown in the Table 6.19.

Many researchers have noticed that there exists an interesting relationship between the noiselike/chaotic communication and traditional cryptography: many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems.

Table 6.19 Comparison between the chaotic communication and traditional cryptography.

Chaotic property	Cryptographic property	Description
Noiselike Broadband Spread spectrum	Confusion	The output has the same distribution for any input
Sensitivity to initial conditions and variation of parameters	Diffusion with a small change in the system and secret key	A small deviation in the input and system parameters can cause a large change in the whole space
Mixing property	Diffusion and fluctuation	Diffusion and fluctuation in the stream of ciphertext
Deterministic dynamics	Deterministic pseudo-randomness	A deterministic process can cause a random-like (pseudo-random) behavior
Structure complexity	Algorithm (attack) complexity	A simple process has a very high complexity

In this section, we analyze whether our proposed optical cryptography system can form the noiselike communication which has its properties corresponding to the chaotic system and tradition cryptography mentioned above.

6.2.3.1 Noiselike Broadband Spread-spectrum

A fundamental requirement of the pseudo-random noise used in cryptography is that its spectrum should be infinitely broad and flat, and the power density much higher than the signal to be concealed. In other word, the plaintext power spectrum should be effectively buried into the pseudo-random noise power spectrum.

As depicted in Fig. 6.66, when the information signal spreads, and is concealed in the noise. It is not easy to detect the presence of the information signal without prior knowledge of the communication system or the use of sophisticated equipment. Furthermore, even if the presence of the signal is detected, without the appropriate decoding information, a large amount of effort will be required to recover the message.

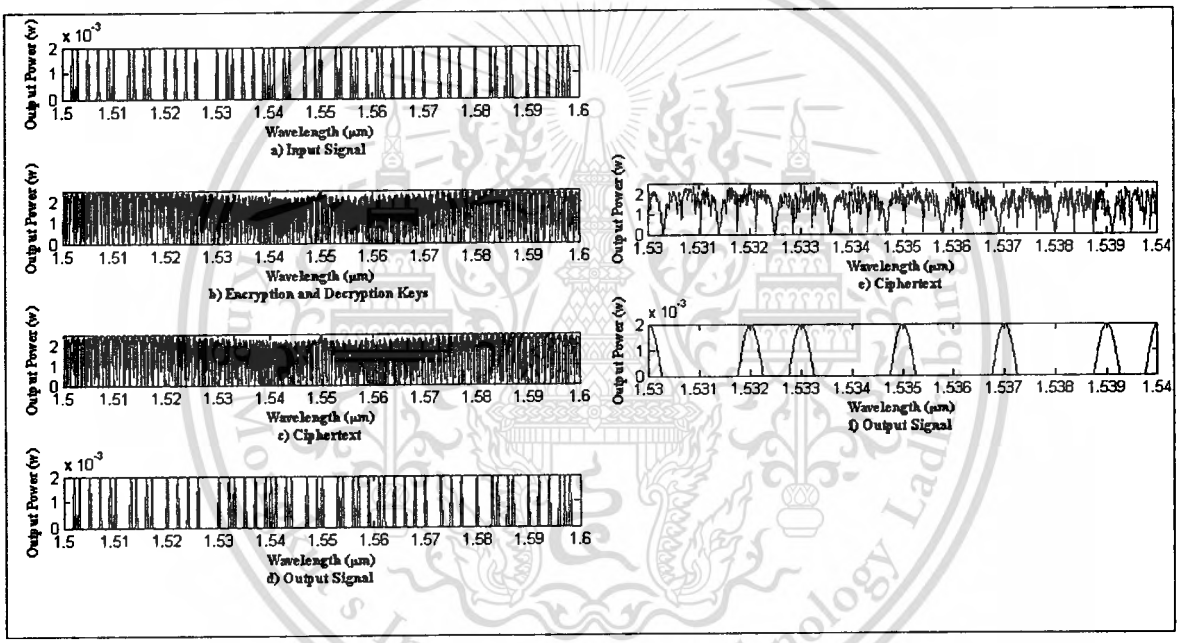

Fig. 6.66 shows the noiselike broadband spread spectrum.

Fig 6.66(c) and (e) show the ciphertext generated from our proposed cryptography system, Fig.6.66(c) shows the ciphertext where the wavelengths in the range of 1.5 μm to 1.5 μm and Fig.6.66(e) shows the ciphertext where the wavelengths in the range of 1.53 μm to 1.54 μm, which confirm its spreading-spectrum across all the wavelengths generally used in the DWDM system. The core principle of our proposed cryptography system is to generate noiselike carrier which its signal power is flat and much higher than that required for simple point-to-point communication. The spreading spectrum is unknown by anyone for whom the signal is unintended, in which case it "encrypts" the signal and reduces the chance of eavesdroppers making sense of it.

Moreover, since the signal power is spread over a large bandwidth (spectrum), so that the eavesdropper cannot determine whether the information signal exists at all. Furthermore, with multiple channels hiding supported, multiple users can transmit the information securely using the same key. The optimum strategy of our proposed cryptography system is for each communicator's signal to look like white noise which is as wideband as possible.

6.2.3.2 Sensitive to initial condition and variation of the parameters

The sensitivity to initial conditions means that each point in such a system is arbitrarily closely approximated by other points with significantly different future trajectories. Thus, an arbitrarily small perturbation of the current trajectory may lead to significantly different future behavior. Minute differences in the initial conditions for such a system result in extremely different outcomes. And the sensitivity to variation of the parameters means that a small deviation in the system parameters can cause a large change at the output.

In the proposed cryptography system, the property of the sensitive to initial conditions and variation of the parameters is used in data encryption. The proposed cryptography system is suitable for data encryption such as messages, images, videos and audio in which the sensitive to initial conditions and variation of the parameters are treated as encryption keys in order to achieve the secure transmission. The encryption key derived from the noiselike signal generated from the PANDA ring resonator is so unpredictable and sensitive; as a result, it obtains much higher security, only a small deviation in the initial condition and system parameters leads to not be able to reproduce the original information signal.

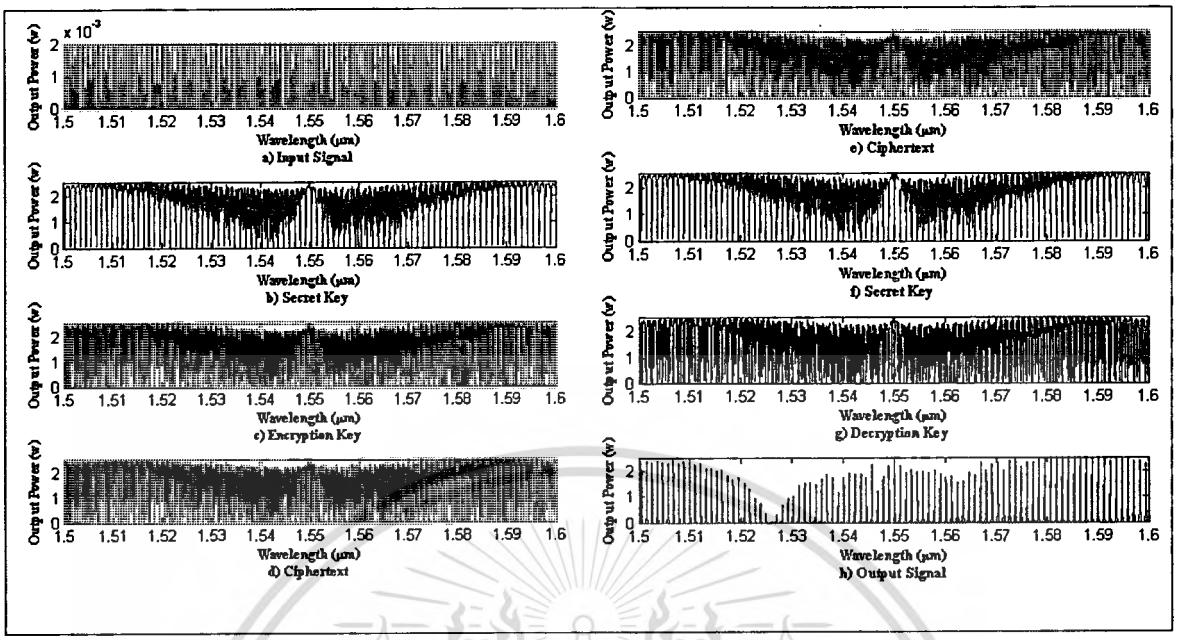

Fig. 6.67 shows the simulation results when the secret key mismatches.

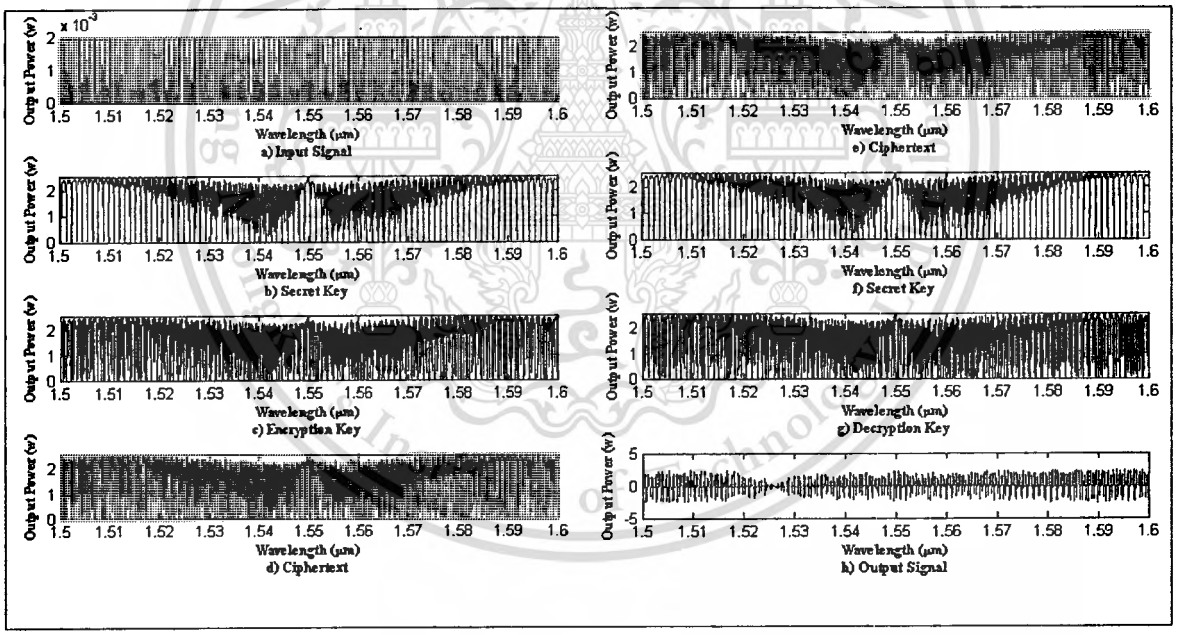

Fig. 6.68 shows the simulation results when the decryption key mismatches.

The noiselike signal generated from the PANDA ring resonator is used to generate the random encryption key stream to encrypt the plaintext element by element. The key streams are the outputs of the encryption-decryption keys generation module. The encryption by a sequence of random (noiselike) signals masks additively a sequence of

plaintext of all the transmission channels, bit by bit, which generates truly random sequence that can hide the information signal from the eavesdropper.

Even the eavesdroppers can trap the transmission signals, however, only a small parameters mismatch such as the radius of the rings , the material type , etc. , the eavesdroppers will not be able to reproduce the original information signal as shown in the experiment 3 and 4, and Fig. 6.67 and 6.68.

The experiment 3 and 4, and Fig. 6.67 and 6.68, show that the proposed cryptography system has the property of the sensitivity to initial conditions and variation of the parameters. In the experiment 2, we have seen that the small difference in the dark-bright soliton pulses to cause the original information signal cannot be recovered, and experiment 3 and 4 have also shown that the small change in the system parameters to cause the original information signal cannot be recovered too.

The main advantage using the proposed cryptography system lies in the observation that the transmitter signal looks like noise for the unauthorized users. Moreover, generating such noiselike signal is often of low cost.

6.2.3.3 Mixing property

The mixing property of the chaos (i.e. topological mixing) means that the system will evolve over time so that any given region or open set of its phase space will eventually be in mixed or fluctuation. The sensitive dependence on initial conditions alone does not give the chaos. For example, consider the simple dynamical system produced by repeatedly doubling an initial value , this system has sensitive dependence on initial conditions everywhere, since any pair of nearby points will eventually become widely separated. However, this example has no the mixing property (fluctuation), and therefore has no chaos. Thus the mixing property is also required by the chaotic system.

The PANDA ring resonator in the proposed cryptography system generates the noiselike signals from the result of the Kerr effect. The Kerr effect is relevant to a change in the refractive index of a material in response to the intensity of the light pulse. This refractive index variation is responsible for the nonlinear optical effects such as self-phase modulation, cross self-phase modulation and etc which leads to the phase fluctuations and mixing, therefore the proposed cryptography system has the characteristic of the mixing property.

6.2.3.4 Deterministic dynamics

The dynamic fluctuations can be generated by a deterministic system. Deterministic dynamic system describes the dynamic in a way that is completely deterministic. If a system is deterministic, this doesn't necessarily imply that later states of the system are predictable from a knowledge of the earlier ones. In this way, it is similar to a random system. For example, the system has been termed "deterministic" since, although it is determined by simple rules, its property of sensitive dependence on initial conditions makes the system, in practice, largely unpredictable. A deterministic process can cause a random-like (pseudo-random) behavior.

The behavior of the proposed system is highly sensitive to initial conditions as mentioned previously. Small differences in initial conditions yield widely diverging outcomes. This happens even though the proposed system is deterministic, meaning that its future behavior is fully determined by their initial conditions, with no random elements involved. In other word, the deterministic nature of the proposed systems does not make it predictable. This behavior is known as deterministic chaos

The proposed cryptography system is dynamic to the generation of random and unpredictable behaviors by a simple system using nonlinear (Kerr) effect.

6.2.3.5 Structure Complexity

One of new trends in the security researches is “the structure complexity” or “simple complexity” i.e. the length of the shortest algorithm producing the cryptographic sequence. The reason is that the demand for the high security system that can be implemented easily is growing because the robustness of the cryptography system also depends on the correctness of its setting. Importantly the system setting must be simple but robust enough against the attacker. The complexity of the system must be enough to protect itself from attacks and system replication. The system parameters must be sensitive to the variation of the parameters.

Our proposed cryptography system is designed using only the simple optical devises which does not require any electrical circuits. Since the noise generation process until the encryption-decryption keys generation process all are done by using only the optical devices so our proposed system is less complex than the Opto-electro system. Moreover, the proposed system was analyzed previously that it is sensitive to the initial condition and variation of the parameters, so it is not easy to duplicate the system in order for reproducing the correct security keys . In addition to the proposed cryptography system presented in this thesis, we are also on the way to propose a higher advance cryptosystem which uses the combination of the encryption-decryption

keys presented in this thesis together with the fix key. The fix key will be defined by the administrator and shared secretly among them. The fix key will be configured during the implementation process (initializing the system), if so, even the attacker can duplicate the system or has the identical system in hand, they will not be able to be authorized to participate in the secure communication without the fix key.

6.2.4 The strength of the additive masking approach

The noiselike communication has many advantages such as broadband, secure and low cost, which is mainly realized by the noiselike signal masking which uses the broadband noiselike signal to hide the information signal, there are two well known types of the noiselike signal masking which are discussed in this section.

6.2.4.1 Additive masking

Additive masking is one of data hiding schemes which also uses the noises as a foundation for data hiding. The goal is to disguise the message as a naturally present.

In formula, the additive masking uses an additive approach to mask the information signal P_i by the noiselike signal, where P_c is the noiselike signal. At the receiver, it synchronizes the noiselike signal with the transmitter, where P'_c is the synchronized noiselike signal, the output information signal P'_i is recovered by minus the received signal P'_s by P'_c.

$$P_s = P_i + P_c \tag{6.1}$$

$$P'_i = P'_s - P'_c \tag{6.2}$$

In Fig. 6.69, the original information signal has been completely buried into the noiselike signal. The signal power of noiselike signal is much higher than the original information signal , so It is not easy to detect the presence of the original information signal.

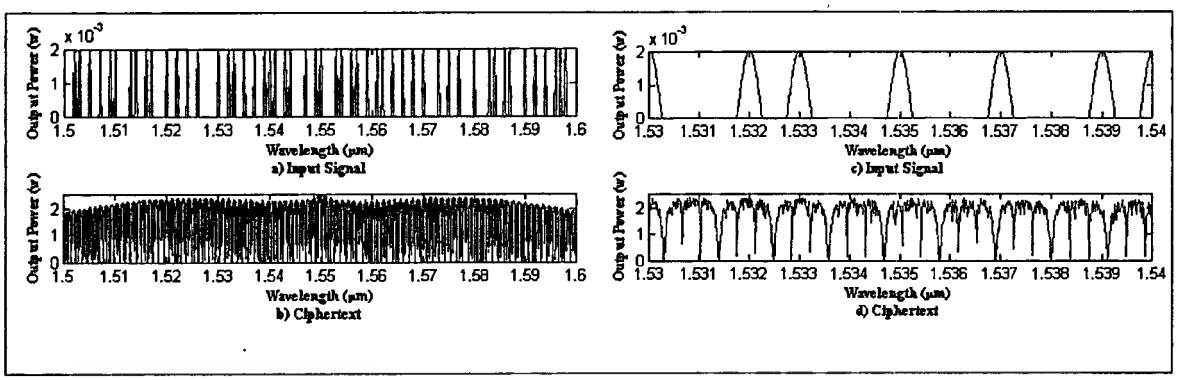

Fig. 6.69 shows the power spectrum of the ciphertext generated from our proposed system.

The simulation results shown in Fig. 6.69 have confirmed that the original information (input) signal is hidden behind the noiselike signal which it is not easily distinguished by the eavesdropper. The power spectrum on the range is relatively broad, covering all the wavelengths generally used by DWDM (1.5-1.6 μm) . The signal power of the ciphertext is much higher than the original information signal, and completely different from the original information signal Therefore, this approach is suitable for our cryptography system which requires the communication in the form of the noiselike broadband spread spectrum.

A band-pass filter such as low-pass filter and high-pass filter is used to eliminate all frequencies above and below the cutoff frequency, sometime it is used by the eavesdropper to filter the noiselike signal from the ciphertext while passing those information signals. Technically It is difficult to filter the noiselike signal generated by our proposed cryptography system from the ciphertxt because our proposed cryptography system adds the power (intensity) of the information signal by the power of the noiselike signal, instead of mixing the information signal frequencies (wavelengths) with the noise frequencies. Therefore, using the frequency filter techniques is not easy to filter the noiselike signal generated by our proposed cryptography system. Moreover, as mentioned above the power spectrum of the noiselike signal is much higher than the power of the information signal, so it is not easy to reproduce the identical noiselike signal in order to recover the information signal by using the subtraction approach. Only one way to decrypt the ciphertext is that the eavesdropper must know all the primers of the system (see all the primers in section 6.2.4), and must be able to reproduce the identical receiver system and trap the noiselike signal. To trap the noiselike signal sent over the optical network is not the easy job, as well as our proposed cryptography has the property of the sensitivity to initial conditions and variation of the parameters, a

small deviation in the system parameters can cause a large change at the output. Thus it is really not easy to recover the information signal by the 3rd party.

6.2.4.2 Multiplicative masking

Multiplicative masking uses a multiplication approach to mask the messages by the noiselike signal, $x_1(t)$ is multiplied by $s(t)$ as the transmission of signals, the receiver performs a reverse process in which the $s(t)$ is divided by the noiselike carrier $x_2(t)$ to reproduce the original information. The encryption and decryption processes can be achieved as follows.

$$s(t) = i(t) \times x_1(t) \tag{6.3}$$

$$i'(t)\,(t) = s(t)/\,x_2(t) \tag{6.4}$$

As shown in the above formula, the multiplication is done in the time domain in which it multiplicatively modulates the information signal with noise signal causing seemly absence of the information signal. The multiplicative masking approach makes the significant changes to the power spectrum, and also makes the power spectrum to be completely different from the original information signal. Then the signal can be transmitted safely without the need to improve the power of noiselike signals in any case. The inescapable weakness of the multiplicative masking approach is that a zero data bit is unmasked by multiplication which means that the data bit is not masked when it equals zero, so the eavesdropper can easily detect the presence of the zero bit causing inherently not to achieve the ideal security. The strengths and weaknesses of the multiplication masking approach will be studied more in the future in order to find the way to continuously develop our cryptography system.

6.2.5 The robustness of the proposed system

How to design robust noiselike secure communication systems is always real challenges for researchers. In this section, we investigate the robustness of our proposed cryptography system in three aspects as below.

6.2.5.1 Tolerant against attacks

When the sender and the receiver are communicating and do not want the third party to see what they are sending, they need to communicate in a way not susceptible to eavesdropping or interception. This is known as communicating in a secure manner or secure communication. The secure communication includes means by which people

can share information with varying degrees of certainty that third parties cannot intercept what was said. With many communications taking place over long distance and mediated by technology, and increasing awareness of the importance of interception issues, technology and its compromise are at the heart of this debate.

The noiselike communication, the security (i.e., privacy) is based on the complex dynamic behaviors provided by the transmission system which creates the random data flow to make the presence of genuine communication harder to detect and traffic analysis less reliable. The properties of chaotic dynamics, such as complex behavior, noiselike dynamics (pseudorandom noise) and spread spectrum, are used to encode data.

We have discussed in the section 6.2.3 that our proposed cryptography system can meet the basic requirements of the chaotic cryptography which it has the following chaotic properties: the noiselike broadband spread spectrum, sensitivity of initial conditions and variation of the parameters, mixing property , deterministic dynamics, and structure complexity.

6.2.5.2 Tolerant against a channel effect

The noiselike communication systems over the Fiber optics disregard the distortions introduced by typical communication channel and optical devices. In general , common distortions in the communication system take the forms of additive noise, attenuation and dispersion.

Additive noise - an interference adds to the signal during its transmission over a communication channel.

Attenuation - in fiber optics, also known as transmission loss, is the reduction in intensity (power) of the light pulse (or signal) with respect to distance travelled through a transmission medium.

Dispersion - the waveform will spread over time, such that a narrow pulse will become an extended pulse, i.e. be dispersed.

Our proposed cryptography system is designed to secure the communication over the fiber optics. The fibers are used instead of metal wires because signals travel along them with less loss and are also immune to electromagnetic interference or additive noise, so we do not have to worry about the additive noise and the attenuation over the long distance. Moreover, we apply the property of the soliton pulse which its

optical field and power spectrum do not change during propagation in the long distance to carry the information signal. We convert the dark and bright soliton pulses into the form of the intensity noise, the intensity noise after the conversion still has the property of the soliton. And then the information signal is masked additively by the encryption key derived from that intensity noise in order to form the random traffic prior to sending it to the receiver. With the communication using the soliton as carrier, we do not have to be concerned about the dispersion and again attenuation of the communicating pulses in the long distance.

However, the fiber-optic communications can be distortion e.g. caused by scattering, absorption and etc but it is considered very small. Fig. 6.70, 6.71 and 6.72 show that our proposed cryptosystem can be tolerant against small loss, we induce the loss to the proposed cryptography system by increasing the attenuation coefficient of the AD4 from 0 to 0.1, 0.5, and 1, the simulation results are shown in Fig. 6.70(b) and (d), Fig. 6.71 (b) and (d), and Fig. 6.72 (b) and (d), respectively.

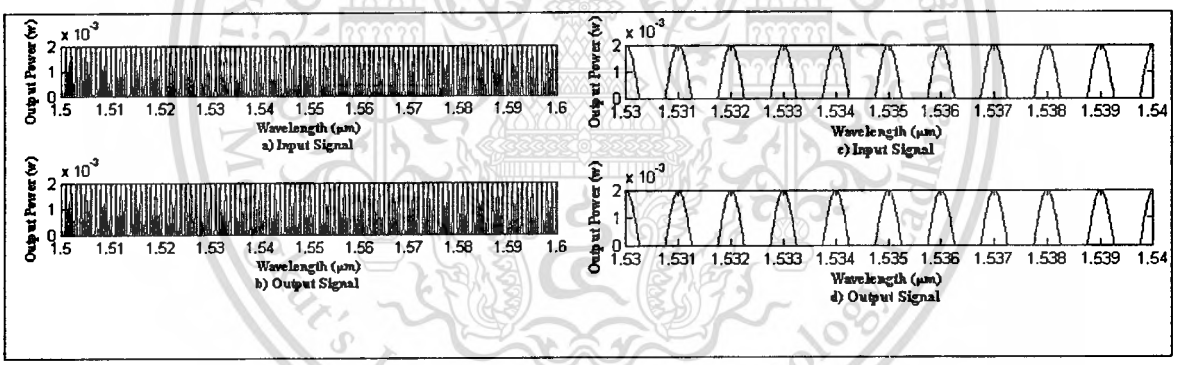

Fig. 6.70 shows the simulation results when change the attenuation coefficient of the AD4 from 0 to 0.1.

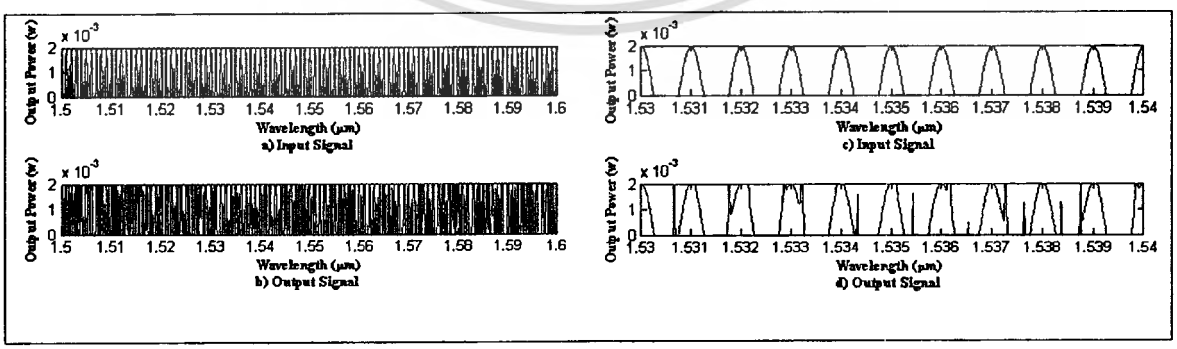

Fig. 6.71 shows the simulation results when change the attenuation coefficient of the AD4 to 0.5.

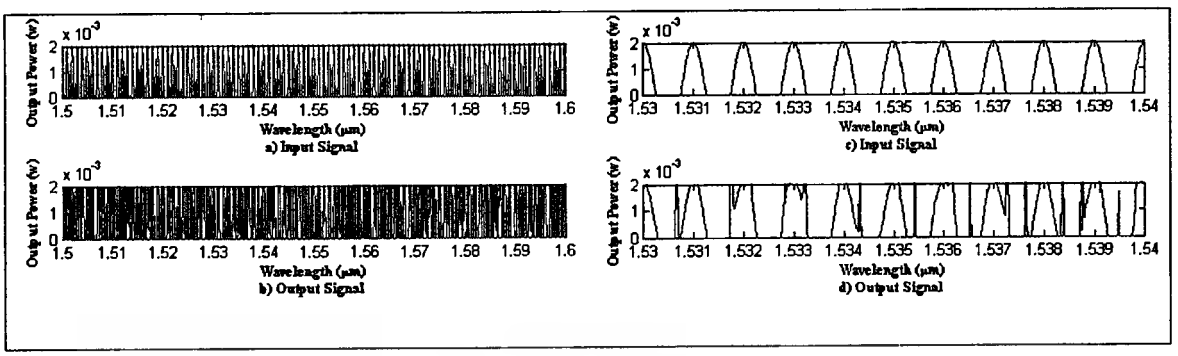

Fig. 6.72 shows the simulation results when change the attenuation coefficient of the AD4 to 1.

6.2.5.3 Tolerant against the synchronization delay.

The quality of the noiselike communication depends crucially on the accuracy and robustness of the synchronization at the receiver. Because of the simple design of the proposed cryptography system, which consists of a few optical devices cascaded making the reduction of the synchronization error to very minimum. The same noiselike signal propagates via two optical paths in which both paths have same distance, same number of the optical devices as well as same type of the optical devices until reaching out the other end, so the synchronization delay can consider being negligible. However, in this section we would like to demonstrate that what happens if the synchronization delay is induced and whether our proposed system can be tolerant against that small synchronization delay.

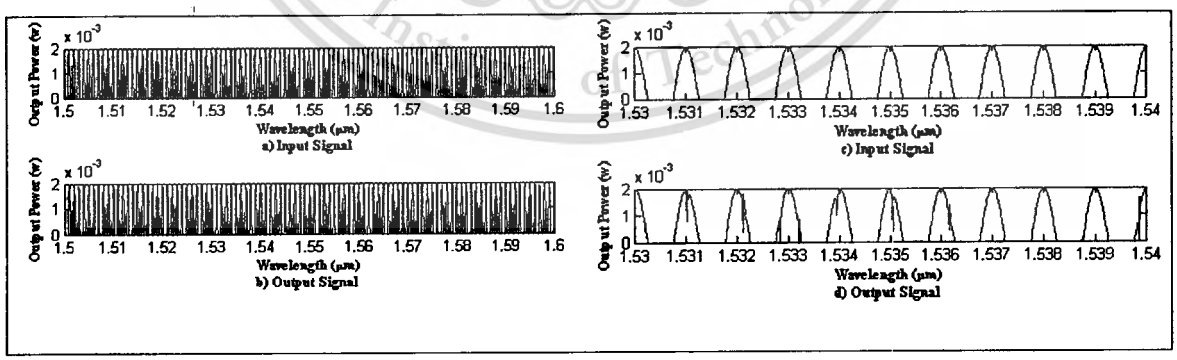

Fig. 6.73 shows the simulation results when change the refractive index of the AD4 from 3.4 to 3.40000001.

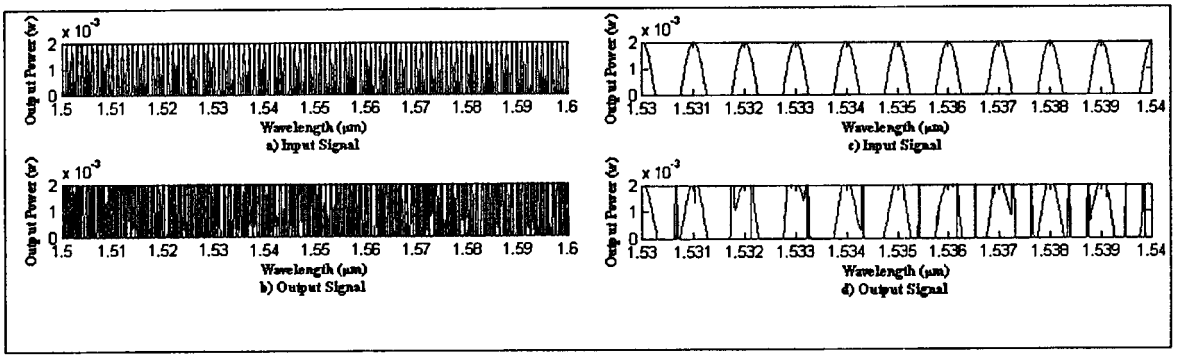

Fig. 6.74 shows the simulation results when change the refractive index of the AD4 to 3.4000001.

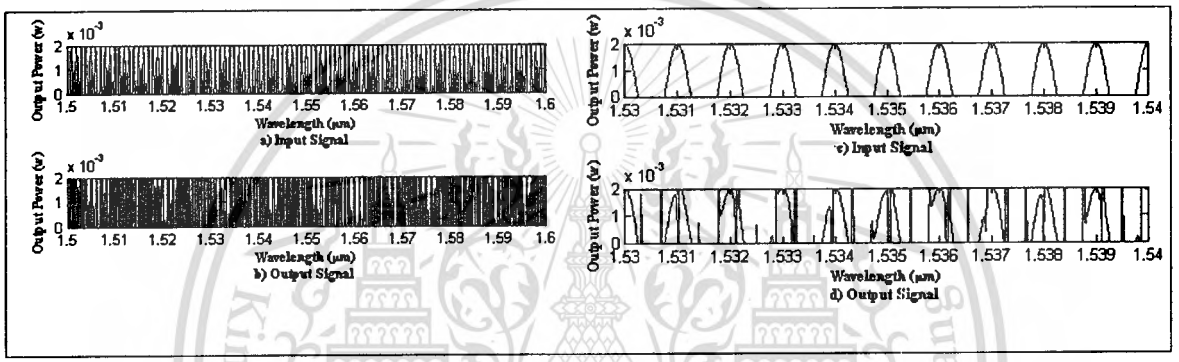

Fig. 6.75 shows the simulation results when change the refractive index of the AD4 to 3.400001.

The simulation results confirm the effectiveness of the design, Fig. 6.73(b) and (d), 6.74(b) and (d), and 6.75(b) and (d) depict that even the outputs are affected from the synchronization delays, they still can be interpreted. The small delays are caused from the change of the refractive index at the AD4. We change its refractive index from 3.4 to 3.40000001, 3.4000001 and 3.400001, the simulation results illustrate in the Fig. 6.73, 6.74 and 6.75, respectively.

6.2.6 The security primers of the proposed system

The radius of the rings, the coupling coefficient (κ) , the effective core area (A_{eff}), and the material type of the PANDA ring resonator as well as the characteristic of the input dark-bright soliton pulses are the primers of the noiselike signal generation module. If the eavesdropper would like to reproduce the noiselike signal by himself, he needs to know exactly all the primers mentioned above. Moreover, after he has the nosielike signal either create by himself or trap from the optical network, he still has to

know all the primers of the Add/drop filters used at the receiver (AD3 and AD4) including the radius of the rings, coupling coefficient (κ) , and the material type in order to create the correct secret and decryption keys, respectively.

Table 6.20 shows all primers of the proposed optical cryptography system.

Optical Device	Primers
PANDA ring resonator used in the noiselike signal generation module	The radius of the rings (R_{ad}, R_r, R_l), the coupling coefficient (κ_0,κ_1,κ_2, κ_3) , the effective core area (A_{eff}) and the material type as well as the characteristic of the dark-bright soliton pulses used for the noiselike signal generation.
Add/drop filters at the receiver : AD3 and AD4	Radius of the ring (R), Coupling coefficient (κ_5,κ_6) , and material type.

It is really not easy to guess all primers as shown in the Table 6.20, and due to the sensitivity to initial conditions and variation of the parameters of the proposed system, the small change of particular parameter leads to unable to recover the original information signal. In the worse case, even the eavesdropper has all the identical devices, the rekeying mechanism of the proposed cryptography system still can protect the system from eavesdropping the entire communication.

6.2.7 Contribution of the Thesis

Uomwech, Sarapat, and Yupapin proposed the literature named "the Dynamic modulated Gaussian pulse propagation within the double PANDA ring resonator system" in 2009. As the review in the section 2.3, they found the interesting results of Gaussian pulse propagation within a double PANDA ring resonator system. The authors simulated and analyzed the dynamic waveforms of propagating light pulse within the desired system. By using the input Gaussian pulse with center wavelength at 1550 nm and the practical parameters, results obtained have shown that the multi wavelengths light sources can be generated and achieved, and the dynamic behaviors of light pulses propagating within the system in the form of the noiselike can be seen. In that literature, the authors only proposed the approach which can be used to form the noiselike signal, the optical cryptography system that is used to apply that approach is not initially

proposed yet.

Later in 2010, Pakorn et al. [70] proposed his literature named "Public key suppression and recovery using a PANDA ring resonator for high security communication", it was also reviewed in the section 2.4. He proposed an interesting security technique that applies the dynamics state of the dark-bright soliton propagation and collision within the PANDA ring resonator. The obtained outputs can be controlled and used to form the digital public key.

Pakorn has proposed the novel security technique which is very useful for many researchers. Our work also adopted his initiative in order to develop the complete all-optical cryptography system. The key enhancements of our proposed cryptography system to compare with Pakorn's system are shown as follows.

Table 6.21 compares the proposed optical cryptography system with the Pakorn's system.

Features	The proposed optical cryptography system	Pakorn's system
Security level	Noiselike communication	Only digital public key generation method
Key management	Transmitter and Receiver use the different key pairs	Shared key
Encryption and Decryption Methods	Additive Masking	Not specify
Rekeying	Yes	Not specify
Channel spacing	1 nm	Not specify
Bit rate – Encryption throughput	40 Gbps per channel, totally 4 Tbps.	Not specify
Number of devices used at the transmitter	3 devices (one PANDA ring resonator, and two Add/drop filters)	2 devices (one PANDA ring resonator, and one microring resonator)
Number of devices used at the receiver	2 devices – two Add/drop filters	1 device – Microring resonator
Number of devices used for noiselike signal generation	1 device – the PANDA ring resonator	1 device – the PANDA ring resonator

Table 6.21 (cont.) compares the proposed optical cryptography system with the Pakorn's system.

Features	The proposed optical cryptography system	Pakorn's system
Number of devices used for Secret/shared key generation at the transmitter	1 device – the Add/drop filter	1 device – the Microring resonator
Number of devices used for Secret/shared key generation at the receiver	1 device – the Add/drop filter	1 device – the Microring resonator
Number of devices used for Encryption-Decryption keys generation at the transmitter	1 device – the Add/drop filter	Not available, proposed only 1 level of key generation (the secret key generation module)
Number of devices used for Encryption-Decryption keys generation at the receiver	1 device – the Add/drop filter	Not available, proposed only 1 level of key generation (the secret key generation module)
Total delay time of the transmitter part	42.70400000 ps	20.97520000 ps
Total delay time of the receiver part	28.46933333 ps	6.99173333 ps
Delay time for noiselike signal generation	14.23466667 ps	13.98346667 ps
Delay time for Secret/shared key generation at the transmitter	7.11733333 ps	6.99173333 ps
Delay time for Secret/shared key generation at the receiver	7.11733333 ps	6.99173333 ps
Delay time of Encryption-Decryption key generation module at the transmitter	21.35200000 ps	Not available, proposed only 1 level of key generation (the secret key generation module)

Table 6.21 (cont.) compares the proposed optical cryptography system with the Pakorn's system.

Features	The proposed optical cryptography system	Pakorn's system
Delay time of Encryption-Decryption key generation module at the receiver	21.35200000 ps	Not available, proposed only 1 level of key generation (the secret key generation module)
Advantage	Only optical devices used for the entire communication	Require more electrical circuits for encryption and decryption processes

1. We proposed the optical cryptography system that forms the noiselike secure communication. The proposed cryptography system presented in the previous chapter including the noiselike signal generation, the secret key Generation, and the encryption-decryption keys generation modules. The simulation results of each module have been shown previously that the noiselike secure communication could be realized by our cryptography system. Pakorn just proposed the system that can only generate the digital public key. He showed the schematic diagram of the overall system but he did not demonstrate the methodology which uses that digital public key for the secure communication.

2. At the encryption-decryption keys generation module, we used the Add/drop filter to generate the encryption and decryption keys. As the add/drop filter has two output ports (Through port and Drop port) , we used the output at the through port as the encryption key for the transmitter and on the other side we used the output at the drop port as the encryption key for the receiver. Pakorn used the microring resonator (MR) to extract the key signal from the noiselike signal prior to transforming it to be the digital public key. The microring resonator has only one output so the transmitter and receiver have to use the same key (shared key) for the encryption. If the eavesdropper can reproduce the encryption key then he can break the communication in both directions.

3. We used the additive masking approach to bury the information signal into the noiselike signal. The ciphertexts generated from our cryptography system have the property of the noiselike broadband spread spectrum and sensitivity to initial conditions and variation of parameters which are required for the noiselike cryptography. Pakorn did not propose the encryption technique that is suitable for his digital public key.

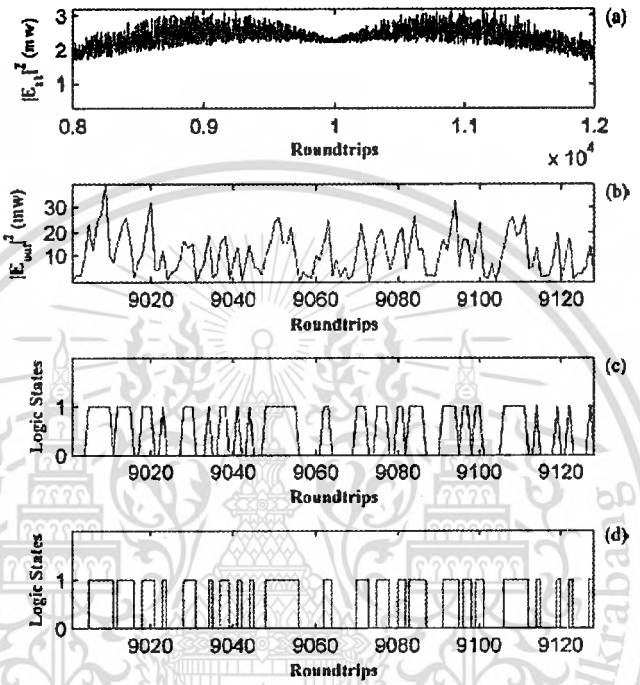

Fig. 6.76 show the simulation results how to generate the digital public key.

Fig. 6.76 shows the simulation results of all the processes used to produce the digital public key in Pakorn's system. Fig. 6.76(a) shows the noiselike signal generated from the PANDA ring resonator, and then the noiselike signal is input to the microring resonator. Fig. 6.76(b) shows the output power of the microring resonator at the roundtrips in the range of 9001 to 9128. The output powers of the microring resonator are later clipped using Eq.(6.5) below, its output is shown in Fig 6.76(c).

$$u(v) = \begin{cases} 0, & v < 10.0\,\text{mW} \\ 1, & v \geq 10.0\,\text{mW} \end{cases} \tag{6.5}$$

Where $u(v)$ represents the logic state, and v is the signal power.

The clipped signals are then performed by the least-squares method in which finally the digital public key is obtained as shown in the Fig 6.67(d). The output digital

public key is"00001111110111100111001000011100010011001001000111111110000001 10000001110011100110111100001111011011000001111110010000100100010".

4. The ability to rekey was also demonstrated in this thesis which it was missing from the Pakorn's system

5. Our proposed cryptography system provides extremely high encryption throughput. The channel spacing used by our proposed cryptography system is 1nm which currently can support up to 40 Gbps per channel [118]. Moreover, our proposed system can accommodate 100 channels at the wavelengths in the range of 1.53 μm to 1.54 μm, so it supports totally 4 Tbps encryption throughput at the moment. Pakorn did not specify how to use his digital public key, so the throughput of his system is unknown. However, as the digital public key must later be processed by the electrical circuit, so the throughput of his system is limited dramatically by the electrical circuit.

6. Our proposed system consists of three devices at the transmitter part (one PANDA ring resonator, and two Add/drop filters), and two devices at the receiver part (two Add/drop filters). Pakorn's system consists of two devices at the transmitter part (one PANDA ring resonator and one microring resonator), and one device at the receiver part. The total delay time at the transmitter part, total delay time at the receiver part, and the delay time at every module of our proposed system are very close to those taken by the Pakorn's system, the difference of the total delay times are first caused from the difference in the number of the devices being used in our proposed system and Pakorn's system. We use one more device (Add/drop filter) for the encryption-decryption keys generation module which its radius is 300 μm (longer ring radius causes higher delay time because of longer distance to propagate) and its refractive index is 3.4, which adds the delay time approximately 21.352 ps to both the transmitter and receiver parts. Second, the refractive index of the devices used in our proposed system is a little bit higher than Pakorn's system as shown in the Table 6.27 so our devices must cause a little bit higher delay time because the higher the refractive index, the slower the speed of light through the medium. The Table 6.27 and 6.28 compare the used parameters of both systems, and Fig. 6.77-6.71 compare the delay time of both systems.

7. As mentioned earlier, the output obtained from Pakorn's system is the digital public key which requires the Optical to Electrical (O/E) and Electrical to Optical (E/O)

conversion in the encryption and decryption processes. On the other hand, our proposed system uses only the optical devices for the entire secure communication which is much simpler and faster than the Pakorn's system.

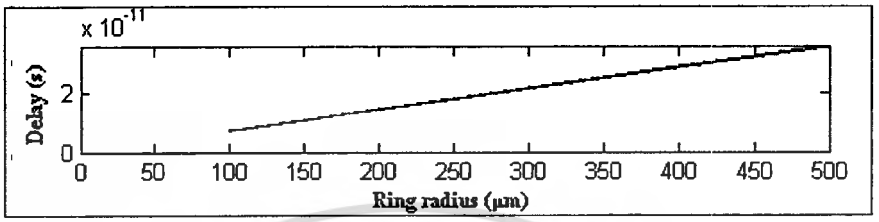

Fig. 6.77 compares the delay times of the noiselike signal generation parts, when the ring radius of the both PANDA ring resonators is changed.

Table 6.22 compares the delay times of the noiselike signal generation parts, when the ring radius of the both PANDA ring resonators is changed.

Ring Radius	Our proposed system	Pakorn's system
100	7.11733333 ps	6.99173333 ps
200	14.23466667 ps	13.98346667 ps
300	21.35200000 ps	20.97520000 ps
400	28.46933333 ps	27.96693333 ps
500	35.58666667 ps	34.95866667 ps

Fig. 6.77 and Table 6.22 compare the delay times of the noiselike signal generation part of our proposed system (shown in red) with the one used in Pakorn's system (shown in blue) when the ring radius of both PANDA ring resonators is changed in the range of 100 μm to 500 μm. In this case, it shows that the delay times taken by the noiselike signal generation part of both systems are almost the same.

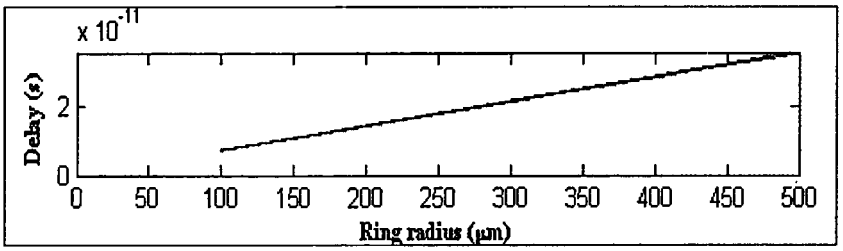

Fig. 6.78 compares the delay times of the secret and shared key generation parts, when the ring radius of the AD1 (red) and MR (blue) is changed.

Table 6.23 compares the delay times of the secret and shared key generation parts, when the ring radius of the AD1 (red) and MR (blue) is changed.

Ring Radius	Our proposed system	Pakorn's system
100	7.11733333 ps	6.99173333 ps
200	14.23466667 ps	13.98346667 ps
300	21.35200000 ps	20.97520000 ps
400	28.46933333 ps	27.96693333 ps
500	35.58666667 ps	34.95866667 ps

Fig. 6.78 and Table 6.23 compare the delay times of the secret key generation part of our proposed system (shown in red) with the delay times of the shared key generation part of Pakorn's system (shown in blue) when the ring radius of the optical devices, AD1 and MR, used in the secret key generation part of our proposed system and shared key generation part of Pakorn's system, respectively, is changed in the range of 100 μm to 500 μm. In this case, it shows that the delay times taken by the secret key generation part of our proposed system and shared key generation part of Pakorn's system are almost the same. Previously the Fig. 3.4 in the chapter 3 shows that if the ring radius decreases, then the attenuation coefficient (α) increases (where the coupling coefficient , κ ,is fixed), which means that the smaller ring radius has the higher blending loss. The higher blending loss causes the lower output power circulated back to the

coupling region, if so, the interference at the coupling region has less fluctuation (output signal power rises and falls in a small amount).

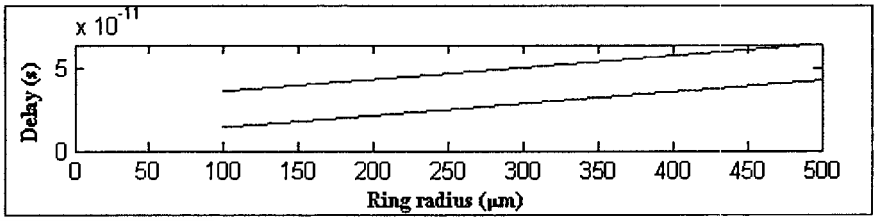

Fig. 6.79 compares the total delay times of the transmitter part of the both systems when the ring radius of the PANDA ring resonators is changed.

Table 6.24 compares the total delay times of the transmitter part of the both systems when the ring radius of the PANDA ring resonators is changed.

Ring Radius	Our proposed system	Pakorn's system
100	35.58666667 ps	13.98346667 ps
200	42.70400000 ps	20.97520000 ps
300	49.82133333 ps	27.96693333 ps
400	56.93866667 ps	34.95866667 ps
500	64.05600000 ps	41.95040000 ps

Fig. 6.79 and Table 6.24 compare the total delay times of the transmitter part of our proposed system (shown in red) with the total delay times of the transmitter part used in Pakorn's system (shown in blue) when the ring radius of both PANDA ring resonators is changed in the range of 100 μm to 500 μm. In this case, it shows that the total delay times taken by the transmitter part of our proposed system are a little bit higher than the transmitter part of Pakorn's system in all radii but it is considered very small different (~21.6 ps).

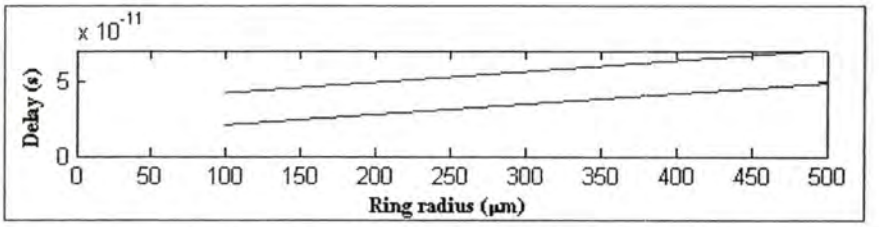

Fig. 6.80 compares the total delay times of the transmitter part of both systems when the ring radius of the AD1 (red) and MR (blue) is changed.

Table 6.25 compares the total delay times of the transmitter part of both systems when the ring radius of the AD1 (red) and MR (blue) is changed.

Ring Radius	Our proposed system	Pakorn's system
100	42.70400000 ps	20.97520000 ps
200	49.82133333 ps	27.96693333 ps
300	56.93866667 ps	34.95866667 ps
400	64.05600000 ps	41.95040000 ps
500	71.17333333 ps	48.94213333 ps

Fig. 6.80 and Table 6.25 compare the total delay times of the transmitter part of our proposed system (shown in red) with the total deal times of the transmitter part used in Pakorn's system (shown in blue) when the ring radius of the optical devices, AD1 and MR, used in the secret key generation part of our proposed system and shared key generation part of Pakorn's system, respectively, is changed in the range of 100 μm to 500 μm. In this case, it shows that the total delay times taken by the transmitter part of our proposed system are a little bit higher than the transmitter part of Pakorn's system in all radii but it is considered very small different (~21.73 ps).

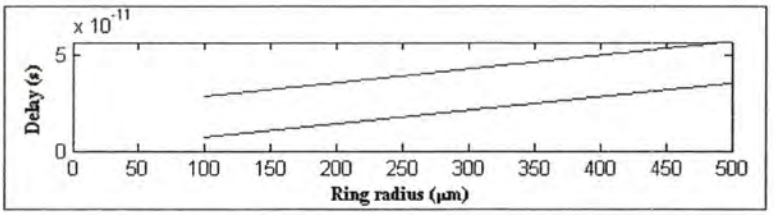

Fig. 6.81 compares the total delay times of the receiver part when the ring radius of the AD3 and MR is changed.

Table 6.26 compares the total delay times of the receiver part when the ring radius of the AD3 and MR is changed.

Ring Radius	Our proposed system	Pakorn's system
100	28.46933333 ps	06.99173333 ps
200	35.58666667 ps	13.98346667 ps
300	42.70400000 ps	20.97520000 ps
400	49.82133333 ps	27.96693333 ps
500	56.93866667 ps	34.95866667 ps

Fig. 6.81 and Table 6.26 compare the total delay times of the receiver part of our proposed system (shown in red) with the total deal times of the receiver part used in Pakorn's system (shown in blue) when the ring radius of the optical devices, AD3 and MR, used in the secret key generation part of our proposed system and shared key generation part of Pakorn's system, respectively, is changed in the range of 100 μm to 500 μm. In this case, it shows that the total delay times taken by the receiver part of our proposed system are a little bit higher than the receiver part of Pakorn's system in all radii but it is considered very small different (~21.47 ps).

Table 6.27 compares the used parameters of the noiselike signal generation part of both systems.

Parameters of the noiselike signal generation part	The proposed system	Pakorn's system
Optical device type	PANDA ring resonator	PANDA ring resonator
Linear refractive index : n_0	3.4	3.34
Nonlinear refractive index : n_2	2×10^{-15}	1.3×10^{-13}
Ring radius of the center ring : R_{ad}	200 µm	200 µm
Ring radius of the right ring : R_r	100 µm	15 µm
Ring radius of the left ring : R_l	100 µm	15 µm
Coupling coefficient : κ_0, κ_1, κ_2, and κ_3	0.2	0.1,0.2,0.2,0.1, respectively
Coupling loss : γ_0, γ_1, γ_2, and γ_3	0.15	0.01
Attenuation coefficient of the center ring : α of R_{ad}	50	0
Attenuation coefficient of the right ring : α of R_r	100	0.1
Attenuation coefficient of the left ring : α of R_l	100	0.1
Effective core area (A_{eff}) of the center ring	0.25×10^{-12}	0.50×10^{-12}
Effective core area (A_{eff}) of the right ring	0.25×10^{-12}	0.25×10^{-12}
Effective core area (A_{eff}) of the left ring	0.25×10^{-12}	0.25×10^{-12}

The PANDA ring resonator applies the Kerr effect to generate the noiselike signal. The Kerr effect is a change in the refractive index (n) of a material in response to an applied electric field ($n = n_0 + n_2 I$) when propagates in the nonlinear media (high non linear refractive index n_2) The Kerr effect causes in self-phase modulation, a self-induced

phase- and frequency-shift of a pulse of light as it travels through a medium (phase fluctuation). The higher nonlinear refractive index causes the higher fluctuation (the fluctuation here means the signal power sharply raises and falls) which it looks like having more noise. As in the Table 6.27, the nonlinear refractive index of the PANDA ring resonator used in the Pakorn's system is a little bit higher than our proposed system, so at this point the noiselike signal generated from the PANDA ring resonator of the Pakorn's system has a little bit more fluctuation than the noiselike signal generated from our PANDA ring resonator. However, the noiselike signal generated from the PANDA ring resonator of our cryptography system will be later filtered by two Add/drop filters prior to hiding the information signal, the noiselike signal generated from Pakorn's system will be filtered by only one microring resonator. Thus finally the noiselike signal at the output of the second Add/drop filter in our proposed system (the encryption key) is harder to reproduce by the eavesdropper than the output of the microring resonator in Pakorn's system. In order to reproduce the correct decryption key for decrypting successfully the ciphertext sent over our proposed system, the eavesdropper also has to know the used parameters of both add/drop filters. In addition, Pakorn did not use the noiselike signal for the information hiding, he used the noiselike signal for the digital public key generation.

Table 6.28 compares the used parameters of the secret and shared key generation parts.

Parameters of the secret/shared key generation part	The proposed system	Pakorn's system
Optical Device type	Add/Drop filter (AD)	Microring Resonator (MR)
Refractive Index : n	3.4	$3.34 + 1.3 \times 10^{-13}$
Ring radius : R	100 μm	100 μm
Coupling Coefficient (	$\kappa_4 = \kappa_5 = 0.2$	$\kappa = 0.5$
Attenuation Coefficient : α	100	0

CHAPTER 7

CONCLUSION

We began by first introducing the motivation of this research, describing the goal and the scope of work, and defining the expected results.

History of the chaos theory was reviewed in the chapter 2, and then the Chaotic Cryptography proposed by Gilles Millérioux et al. was investigated , three chaos masking methods presented by them including Additive masking, Message embedding and Hybrid message embedding were very useful for this research. Later, the dynamic modulated Gaussian pulse propagation within the double PANDA ring resonator system proposed by Yupapin et al. was investigated which it was applied later for the chaotic/noiselike signal generation. Then Pakorn et al. also found that the dynamic behavior of the dark-bright soliton propagation and collision within the PANDA ring resonator can be used to form the noiselike signal. The literature reviews were very important in the development of our optical cryptography system and they were the key success for this thesis.

In the chapter 3, necessary mathematical background materials on dark and bright solitons and the optical devices used in the system design were introduced. The mathematical backgrounds presented in this chapter were essential for the system design and modeling.

We investigated the theories of the cryptography and chaos-based communication in chapter 4, many aspects of the chaos-based communication have been described elaborately in this chapter including Spread Spectrum, Chaotic Synchronization, Chaos masking and Chaos modulation.

The optical cryptography system was proposed in chapter 5. The transmitter part consists of one PANDA ring resonator, two optical add/drop filters and one Optical Power Modulator, and the receiver part consists of two optical add/drop filters and one Optical Power Demodulator. The authors use the combination of the noiselike signal, secret key and encryption-decryption keys for the secure communication. First the noiselike signal is obtained from the dynamic states of dark-bright soliton propagation and collision within the PANDA ring resonator. The noiselike signal is sent to the receiver via the separate channel for the synchronization. Second the noiselike signal is input to the first add/drop filter causing the secret key is created, the same secret key is created on each side and not distributed over the optical network, only the transmitter and receiver know the secret key. Third the secret key is later input to the second add/drop

filter in order to create the encryption-decryption keys, similarly both transmitter and receiver create the encryption-decryption keys by their own which both keys are not seen in the optical network. Finally the encryption key is used by Optical Power Modulator for masking the information signals and the decryption key is used by Optical Power Demodulator for unmasking the received signals (ciphertext). The eavesdroppers without the correct decryption key cannot recover the original information signals.

The following mathematical simulations were conducted and their result have presented in the chapter 6:

1. Changing the channel spacing.
2. Generating the new noiselike signal.
3. Secret key mismatches.
4. Decryption key mismatches.
5. Changing the power (intensity) of the input pulses.
6. Changing the input pulses.
7. Rekeying at every time T.
8. Decrypting the ciphertext by the old decryption key after rekeying.

The simulation results obtained have shown that the proposed optical cryptography system worked well as expected in all experiments. The high security communication over optical networks can indeed be achieved by the proposed system; the transmitted information signal is converted to the noiselike signal before travelling over the optical network without any electronic device or electronic control circuit is required. In the second part of the chapter 6 we discussed technically about the proposed optical cryptography system including the limitation, the security measurements, the cryptography properties, the strength of the additive masking approach, the robustness of the proposed system, the security primers of the proposed system, and the contribution of the thesis.

In the conclusion, the proposed optical cryptography system first is able to provide the high security communication over the optical network by applying the noiselike signal generated from the PANDA ring resonator, second the secret key and encryption-decryption keys are generated separately on each side and not distributed over the optical network so they are safe from the eavesdroppers, finally due to only the optical devices used in the design, it relieves the optical network from undesirable latencies caused by processing related to O/E and E/O conversions required by general encryption and decryption processes. The key contribution of this thesis is to provide the cryptography for ultra-high speed communication over the optical network.

Future work

The authors are being on the way to develop the other noiselike optical cryptography system. Instead of using only the encryption and decryption keys presented in this thesis, the possibility of using the combined key has been investigating. The combined key mentioned here is originated from the random and fixed keys, in which the random key is generated in the same way as presented in this thesis and the fixed key is assigned by the administrator. Partial simulation results obtained have shown that a higher level of the security can be achieved by using the combined key, the ciphertext encrypted using the combined key is more randomness. However, more evaluations are still required in order to confirm the correctness of the system.

REFERENCES

[1] M. Hasler, "Synchronization of chaotic systems and transmission of information," **Int. J. Bifurc. Chaos,** vol. 8, no. 4, Apr. 1998.

[2] G. Millérioux, A. Hernandez, and J. M. Amigó, "Conventional cryptography and message embedding," **in Proc. 2005 Int. Symp. Nonlinear Theory Appl. (NOLTA 2005), Bruges, Belgium,** Oct. 2005.

[3] M. J. Ogorzalek, "Taming chaos—Part I: Synchronization," IEEE **Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 40, no. 10, Oct. 1993. pp. 693–699

[4] T. Yang, "A survey of chaotic secure communication systems," **Int. J. Comput. Cogn.**, 2004.

[5] P. Hua, B. J. Luff, G. R. Quigley, J. S. Wilkinson, and K. Kawaguchi "Integrated optical dual Mach–Zehnder interferometer sensor," **Sens. Actuators,**2002. pp. 250–257.

[6] T. Carmon, T. J. Kippenberg, L. Yang, H. Rokhsari, S. Spillane, and K. J. Vahala "Feedback control of ultra-high-Qmicrocavities: Application to micro-Raman lasers and microparametric oscillators," **Opt. Express**, 2005. pp. 3558–3566.

[7] P. D. Townsend "Quantum cryptography on optical fiber networks," **Opti. Fiber Technol.**, 1998. pp. 345–370.

[8] W. Sririth, S.Mitatha, O. Pingern, and P. P. Yupapin "A novel temporal dark-bright solitons conversion system via an add/drop filter for signal security use," **Optik,** 2010. pp. 1955–1958.

[9] B. Knobnob, S. Mitatha, K. Dejhan, S. Chaiyasoonthorn, and P. P. Yupapin "Dark–bright optical solitons conversion via an optical add/drop filter for signals and networks security applications," **Optik**, 2010. pp. 1743–1747.

[10] P. P. Yupapin "Generalized quantum key distribution via micro ring resonator for mobile telephone networks," **Optik**,2010. pp. 422–425.

[11] P. Gallion, F. Mendieta, and S. Jiang "Signal and quantum noise in optical communications and cryptography," **Prog. Opt.**, 2009. pp. 149–259.

[12] Y. Dumeige, C. Arnaud, and P. F´eron "Combining FDTD with coupled mode theories for bistability in micro-ring resonator," **Opt. Commun.**, 2005. pp. 376–383.

[13] P. Rabiei "Calculation of losses in micro-ring resonators with arbitrary refractive index or shape profile and its applications," **J. Lightwave Technol.**, 2005, pp. 1295–1301.

[14] Y. Kokubun, Y. Hatakeyama, M. Ogata, S. Suzuki and N. Zaizen, "Fabrication technologies for vertically coupled microring resonator with multilevel crossing

busline and ultracompact-ring radius," **IEEE J. Sel. Top. Quantum Electron.**, 2005. pp. 4-10.

[15] N. Suwanpayak,M.A. Jalil,C. Teeka, J.Ali, and P. P. Yupapin, "Optical vortices generated by a PANDA ring resonator for drug trapping and delivery applications," **Biomed. Opt. Express**, 2011. pp. 159-- 168.

[16] B. Jukgoljun, N. Suwanpayak, C. Teeka, and P. P. Yupapin, "Hybrid transceiver and repeater using a PANDA ring resonator for nano communication," **Opt. Eng.**, 2010.

[17] T. Phatharaworamet, C. Teeka, R. Jomtarak, S. Mitatha, and P. P. Yupapin, "Random binary code generation using dark-bright soliton conversion control within a PANDA ring resonator", **Lightw. Technol.**, 2010. pp. 2804–2809.

[18] Huaguang Z., Derong L. and Zhiliang W. **Controlling Chaos.** London:Springer-Verlog, 2009.

[19] Robinson RC. **An Introduction to Dynamical Systems: Continuous and Discrete.** New York:Prentice Hall, 2004.

[20] Diacu F., Holmes P. **Celestial Encounters: The Origins of Chaos and Stability.** New JERSEY:Princeton University Press. Princeton,1996.

[21] Van der Pol, B. and J. Van der Mark. "Frequency demultiplication." **Nature**, Vol. 120, 1927. pp. 363-364 (1927)

[22] Birkhoff GD. **Dynamical Systems (revised edition).** Rhode Island:American Mathematical Society, 1966.

[23] Birkhoff, G. D. "Proof of the ergodic theorem." **Proc. Natl. Acad. Sci. USA.**, Vol. 17, 1931. pp. 656-660.

[24] Smale S. "Differentiable dynamical systems." **Bull Mmer Math Society**, 1967. pp. 73:747-817

[25] Ruelle D, Takens F. "On the nature of turbulence." **Commun Math Phys**, 1971. pp. 20:167-192

[26] Li TY, Yorke JA "Period three implies chaos." **Am Math Mon**, 1975. pp. 82:985-992

[27] Sharkovskii AN "Coexistence of cycles of a continuous map of a line into itself." J **Ukr Math**, 1964. pp. 16:61-71

[28] May RM "Simple mathematical model with very complicated dynamics." **Nature**, 1976. pp. 261:459-467

[29] Enns R, McGuire G. **Nonlinear Physics with Maple for Scientists and Engineers.** Boston:Birkhäuser, 1997.

[30] Tucker W. "A rigorous ODE solver and Smale's 14th problem." **Found Comput Math**, 2002. pp. 2:53-117

[31] Mandelbrot B. **The Fractal Geometry of Nature.** Paris:Freeman, 1983.

[32] Ott, E., C. Grebogi and J. A. Yorke. "Controlling chaos." **Phys. Rev. Lett.**, Vol. 64, 1990, pp. 1196-1199.

[33] Gilles Millérioux, José Maria Amigó, and Jamal Daafouz "A Connection Between Chaotic and Conventional Cryptography" **IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS**, VOL. 55, NO. 6, JULY 2008, pp. 1695-1703

[34] Adrian Jacobo, Miguel C. Soriano, Claudio R. Mirasso, and Pere Colet "Chaos-Based Optical Communications: Encryption Versus Nonlinear Filtering" **IEEE JOURNAL OF QUANTUM ELECTRONICS**, VOL. 46, NO. 4, APRIL 2010. pp.499-505.

[35] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," **IEEE Trans. Circuits. Syst. II, Analog. Digit. Signal Process.**, vol. 40,no. 10, Oct. 1993, pp. 626–633.

[36] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communications systems," **Int. J. Bifurc. Chaos**, vol. 3, no. 6, 1993. pp. 1619–1627.

[37] G. Kolumban, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos—Part II: Chaotic modulation and chaotic synchronization," **IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 45, no. 11, Nov. 1998. pp. 1129–1140.

[38] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," **IEEE Trans. Circuits. Syst. II, Analog. Digit. Signal Process.**, vol. 40, no. 7, Jul. 1993. pp. 634–642.

[39] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," **Int. J. Bifurc. Chaos**, vol. 3, no. 2, 1993. pp. 973–977.

[40] F. Anstett, G. Millérioux, and G. Bloch, "Global adaptive synchronization based upon polytopic observers," **in Proc. IEEE Int. Symp. Circuits Syst. , Vancouver, Canada**, May 2004, pp. 728–731.

[41] H. J. C. Huijberts, H. Nijmeijer, and R.Willems, "System identification in communication with chaotic systems," **IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 47, no. 6, Jun 2000. pp. 800–808.

[42] A. L. Fradkov and A. Y. Markov, "Adaptive synchronization of chaotic systems based on speed-gradient method and passification," **IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 44, no. 10, Oct. 1997. pp. 905–912.

[43] H. Dedieu and M. Ogorzalek, "Identification of chaotic systems based on adaptive synchronization," **in Proc. ECCTD'97, Budapest, Hungary**, Sep. 1997, pp. 290–295.

[44] G. Millérioux and C. Mira, "Coding scheme based on chaos synchronization from noninvertible maps," **Int. J. Bifurc. Chaos**, vol. 8, no. 10, 1998. pp. 2019–2029.

[45] Z. P. Jiang, "A note on chaotic secure communication systems," **IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 49, no. 1, Jan. 2002. pp. 92–96.

[46] K. Y. Lian and P. Liu, "Synchronization with message embedded for generalized lorenz chaotic circuits and its error analysis," **IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 47, no. 9, Sep. 2000. pp. 1418–1424.

[47] G. Millérioux and J. Daafouz, "Unknown input observers for message- embedded chaos synchronization of discrete-time systems," **Int. J. Bifurc. Chaos**, vol. 14, no. 4, Apr. 2004. pp. 1357–1368.

[48] T. Yang, "A survey of chaotic secure communication systems," **Int. J. Comput. Cogn.**, 2004.

[49] M. Hasler, "Synchronization of chaotic systems and transmission of information," **Int. J. Bifurc. Chaos**, vol. 8, no. 4, Apr. 1998.

[50] T. Yang, C. W. Wu, and L. O. Chua, "Cryptography based on chaotic systems," **IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 44, no. 5, May 1997. pp. 469–472.

[51] A. T. Parker and K. M. Short, "Reconstructing the keystream from a chaotic encryption scheme," **IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 48, no. 5, May 2001. pp. 624–630.

[52] G. Grassi and S. Mascolo, "Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal," **IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 44, no. 10, Oct. 1997. pp. 1011–1014,

[53] H. Nijmeijer and I. M. Y. Mareels, "An observer looks at synchronization," **IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 44, no. 10, Oct. 1997. pp. 882–890.

[54] M. Itoh, C. W. Wu, and L. O. Chua, "Communications systems via chaotic signals from a reconstruction viewpoint," **Int. J. Bifurc. Chaos**, vol. 7, no. 2, 1997. pp. 275–286.

[55] G. Millérioux, "Chaotic synchronization conditions based on control theory for systems described by discrete piecewise-linear maps," **Int. J. Bifurc. Chaos**, vol. 7, no. 7, 1997. pp. 1635–1649.

[56] A. Isidori. **Nonlinear Control Systems, ser.** Communications and Control Engineering Series. New York: Springer, 1995.

[57] U. Feldmann, M. Hasler, and W. Schwarz, "Communication by chaotic signals: The inverse system approach," **Int. J. Circuit Theory Appl.**, vol. 24, 1996. pp. 551–579.

[58] L. Boutat-Baddas, J. P. Barbot, D. Boutat, and R. Tauleigne, "Sliding mode observers and observability singularity in chaotic synchronization," **Math. Prob. Eng.**, vol. 1, May 2004. pp. 11–31.

[59] M. Boutayeb, M. Darouach, and H. Rafaralahy, "Generalized statespace observers for chaotic synchronization and secure communications," **IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 49, no. 3, Mar. 2002. pp. 345–349.

[60] E. Inoue and T. Ushio, "Chaos communication using unknown input observers," **Electron. Commun. Jpn. III**, vol. 84, no. 12, 2001. pp. 21–27.

[61] G. Millérioux and J. Daafouz, "An observer-based approach for input independent global chaos synchronization of discrete-time switched systems," **IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl.**, vol. 50, no. 10, Oct. 2003. pp. 1270–1279.

[62] G. Millérioux and J. Daafouz, "Unknown input observers for message-embedded chaos synchronization of discrete-time systems," **Int. J. Bifurc. Chaos**, vol. 14, no. 4, Apr. 2004. pp. 1357–1368.

[63] G. Millérioux and J. Daafouz. **Chaos in Automatic Control, Chapter Polytopic Observers for Synchronization of Chaotic Maps.** ser. Control Engineering Series. Boca Raton, FL: CRC , 2006. pp. 323–344.

[64] A. Klimov and A. Shamir. **New Cryptographic Primitives Based on Multiword T-Functions.** Berlin, Germany: Springer, 2004. vol. 3017, ch. 1, pp. 1–15.

[65] K. Uomwech, K. Sarapat, and P. P. Yupapin "DYNAMIC MODULATED GAUSSIAN PULSE PROPAGATION WITHIN THE DOUBLE PANDA RING RESONATOR SYSTEM" **MICROWAVE AND OPTICAL TECHNOLOGY LETTERS**, Vol. 52, No. 8, August 2010.

[66] D. Deng and Q. Guo, "Ince-Gaussian solitons in strongly nonlocal nonlinear media", **Opt Lett**, 2007. pp. 3206–3208.

[67] P.P. Yupapin and W. Suwancharoen, "Chaotic signal generation and cancellation using a microring resonator incorporating an optical add/drop multiplexer," **Opt Commun**, 2007. pp. 343–350.

[68] Q. Xu and M. Lipson. **All-optical logic based on silicon micro-ring resonators.** 2007. pp. 924–929.

[69] Y. Kokubun, Y. Hatakeyama, M. Ogata, S. Suzuki, and N. Zaizen "Fabrication technologies for vertically coupled micro ring resonator with multilevel crossing

busline and ultracompact-ring radius," **IEEE J Sel Top Quantum Electron,** 2005.pp.

[70] P. Juleang, P. Phongsanam, S. Mitatha and P. P. Yupapin "Public key suppression and recovery using a PANDA ring resonator for high security communication," **Opt. Eng.,** 2011, pp. 035002-2 - 035002-6.

[71] Keerayoot S. **"A Design of Nano-Scale Sensor Base On An Optical Add/Drop Filter."** Doctor of Philosophy in Applied Physics, Faculty of Science, King Mongkut's Institute of Technology Ladkrabang, 2011.

[72] E. A. J. Marcatili. "Bends in Optical Dielectric Guides" **Bell System Technical Journal,** vol. 48, no. 7, 1969. pp. 2103-2132.

[73] E. A. J. Marcatili. "Dielectric rectangular waveguide and directional coupler for integrated optics" **Bell System Technical Journal,** vol. 48, no. 7, 1969. pp. 2071-2102.

[74] C. K. Madsen, and J. H. Zhao. "A general planar waveguide autoregressive optical filter" **Lightwave Technology, Journal of,** vol. 14, no. 3, 1996. pp. 437-447.

[75] S. C. Hagness, D. Rafizadeh, S. T. Ho, and A. Taflove. "FDTD microcavity simulations: design and experimental realization of waveguide-coupled single-mode ring and whispering-gallery-mode disk resonators" **Lightwave Technology, Journal of,** vol. 15, no. 11, 1997. pp. 2154-2165.

[76] D. Rafizadeh, J. P. Zhang, S. C. Hagness, A. Taflove, K. A. Stair, S. T. Ho, and R. C. Tiberio. "Waveguide-coupled AlGaAs / GaAs microcavity ring and disk resonators with high f inesse and 21.6-nm f ree spectral range" **Optics Letters,** vol. 22, no. 16, 1997. pp. 1244-1246.

[77] B. E. Little, J. S. Foresi, G. Steinmeyer, E. R. Thoen, S. T. Chu, H. A. Haus, E. P. Ippen, L. C. Kimerling, and W. Greene. "Ultra-compact Si-SiO_2 microring resonator optical channel dropping filters" **Photonics Technology Letters, IEEE,** vol. 10, no. 4, 1998. pp. 549-551.

[78] D. J. W. Klunder, E. Krioukov, F. S. Tan, T. van der Veen, H. F. Bulthuis, G. Sengo, C. Otto, H. J. W. M. Hoekstra, and A. Driessen. "Vertically and laterally waveguide-coupled cylindrical microresonators in Si3N4 on SiO2 technology" **Applied Physics B: Lasers and Optics,** vol. 73, no. 5, 2001. pp. 603-608.

[79] B. Vanderhaegen, D. Van Thourhout, J. De Merlier, G. Sarlet, L. Vanwassenhove, I. Moerman, P. Van Daele, and R. Baets. "High Q GaInAsP ring resonator filters" **Proceedings of the 9th European Conference on Integrated Optics and Technical Exhibition (ECIO 99),** Torino, Italy, Apr. 1999. pp. 381-384.

[80] M. K. Chin, C. Youtsey, W. Zhao, T. Pierson, Z. Ren, S. L. Wu, L. Wang, Y. G. Zhao, and S. T. Ho. "GaAs microcavity channel-dropping filter based on a race-track resonator" **Photonics Technology Letters, IEEE**, vol. 11, no. 12, 1999. pp. 1620-1622.

[81] D. G. Rabus. **Integrated Ring Resonators.** Berlin:Springer-Verlag, 2007.

[82] Dominik G. Rabus. **"Realization of Optical Filters using Ring Resonators with integrated Semiconductor Optical Amplifiers in GaInAsP/InP."** PhD. Thesis of Technischen Universität Berlin. 2002.

[83] Chaiwat S. **"Enhancement of Free Spectral Range Frequency Using Ring Resonators."** Master of Engineering in Computer Engineering, Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, 2011.

[84] Rivest, Ronald L. **Cryptology.** In J. Van Leeuwen. Handbook of Theoretical Computer Science. Elsevier, 1990.

[85] AJ Menezes, PC van Oorschot, and SA Vanstone. **Handbook of Applied Cryptography.** ISBN 0-8493-8523-7.

[86] Jonathan K. and Yehda L. **Introduction to Modern Cryptography.** Boca Raton,FL: Chapman & Hall/CRC, 2007.

[87] R. Paschotta **Encyclopedia of Laser Physics and Technology.** Germany:Wiley-VCH, 2007.

[88] D. Gonze. **"Stochastic simulations and their application to molecular networks."** [Online]. Available : http://www.inrialpes.fr/schoolleshouches07/program.html. 2007.

[89] Jiu C. F., and Chi K. T. **Reconstruction of Chaotic Signals with Applications to Chaos-Based Communications.** Sigapore: World Scientific, 2008.

[90] Williams G.P. **Chaos Theory Tamed.** London:Taylor and Francis, 1997.

[91] Kohda T. and A. Tsuneda. "Statistics of chaotic binary sequences." **IEEE Trans. Information Theory.,** Vol. 43,1997. pp. 104-112.

[92] Dixon R. C. **Spread Spectrum Systems: with Commercial Applications (3rd ed.).** New Yrok:John Wiley and Sons. 1994.

[93] Yamada T. and H. Fujisaka "Stability theory of synchronized motion in coupled-oscillator systems I." **Prog. Theor. Phys.,** Vol. 69, 1983. pp. 32-47.

[94] Yamada t. and H. Fujisaka "Stability theory of synchronized motion in coupled-oscillator systems II." **Prog. Theor. Phys.,** Vol. 70, 1983. pp. 1240-1248.

[95] Afraimovich V. S., N. N. Verichev and M. I.Rabinovich "Stochastic synchronization of oscillations in dissipative systems." **Inv. VUZ. Rasiofiz. RPQAEC.,** Vol. 29,1986, pp. 795-803.

[96] Pecora L. M. and T. L. Carroll "Synchronization in chaotic systems." **Phys. Rev. Lett.,** Vol. 64, 1990. pp. 821-824.

[97] Carroll T. L. and L. M. Pecora "Synchronizing chaotic circuits." **IEEE Trans. Circ. Syst.,** Vol. 38, 1991. pp. 453-356.

[98] Pecora L. M. and T. L. Carroll "Driving systems with chaotic signals." **Phys. Rev. A.,** Vol. 44, 1991. pp. 2374-2383.

[99] Carroll T. L. and L. M. Pecora "Cascading synchronized chaotic systems." **Phisical D.,** Vol. 67, 1993. pp. 126-140.

[100] Pecora L. M., T. L. Carroll, G. A. Johnson and D. J. Mar "Fundamentals of synchronization in chaotic systems, concept, and applicatons." Chaos., Vol. 7, 1997. pp. 520-543

[101] Lorenz E. N. "Deterministic nonperiodic flow" **J. Atmospheric Sciences.** Vol. 20, No.2, 1963. pp. 130-141.

[102] Cuomo K. M., and A. V. Oppenheim "Circuit implementation of synchronized chaos with applications to communications." **Phys. Rev. Lett.,** 1993. Vol. 71, pp. 65-68.

[103] Chen G. and Z. Dong "Controlling Chua's circuit." **J. Circ. Syst. Computers.** Vol. 3, 1993. pp. 139-149.

[104] Halle K. S., C. W. Wu, M. Itoh and L. O. Chua. "Spread spectrum communication through modulation of chaos." **Int. J. Bifurcation Chaos.,** Vol. 3, 1993. pp. 469-477.

[105] John J. K. and R. E. Amritkar "Synchronization of unstable orbits using adaptive control." **Phys. Rev. E.,** Vol. 49,1994. pp. 4843-4848.

[106] Peter S. **Chaos Application in Telecommunications.** Boca Raton,FL: CRC Press, 2006.

[107] Pecora, L.M. and Caroll, T.L., "Synchronization in chaotic systems," **Phys. Rev. Lett.,** 1990. pp. 821-824.

[108] Shannon, C.E., Communication theory of secrecy systems. Bell Sys. Tech. J., 1949. pp. 657-715.

[109] K. Sarapat, N. Sangwara, K. Srinuanjan, P. P. Yupapin, and N. Pornsuwancharoen "Novel dark-bright optical solitons conversion system and power amplification," **Opt. Eng.,** 2009.

[110] T. Phatharaworamet, C. Teeka, R. Jomtarak, S. Mitatha, and P. P. Yupapin "Random binary code generation using dark-bright soliton conversion control within a PANDA ring resonator," **J. Lightwave Technol.**, 2010.

[111] D. G. Rabus, M. Hamacher, U. Troppenz, and H. Heidrich "Optical filters based on ring resonators with integrated semiconductor optical amplifiers In GaInAsP–InP," **IEEE J. Sel. Top. Quantum Electron**, 2002. pp. 1405–1411.

[112] G. L. Li, and P. K. L. Yu. "Optical Intensity Modulators for Digital and Analog Applications," **Journal of Lightwave.,** vol. 21, no. 9, 2003.

[113] Y. Kokubun, Y. Hatakeyama, M. Ogata, S. Suzuki, and N. Zaizen "Fabrication technologies for vertically coupled microring resonator with multilevel crossing busline and ultracompact-ring radius," **IEEE J. Sel. Top. Quantum Electron.**, 2005, pp. 4–10.

[114] FIBER-OPTIC.INFO. "**Dense Wavelength-division Multiplexing**" [Online]. Available : http://www.fiber-optics.info/articles/dense_wavelength-division_multiplexing, 2012.

[115] Olson Technology. "**DWDM ITU Wavelengths.**" [Online]. Available : www.olson-technology.com/AppNotes/ITU-Grid.pdf. 2012.

[116] Eudyna. "**1,550nm DWDM Direct Modulation DFB Laser.**" [Online]. Available : http://www.datasheet4u.net/datasheet/F/L/D/FLD5F15CX-A_EudynaDevices.pdf.html. 2012.

[117] G. Zhang, and L. He "Power Spectrum Mask in Chaotic Secure Communication," **International Conference on Computer Application and System Modeling (ICCASM 2010).**, 2010, pp. V6-418 – V6-421.

[118] T. Schmidt "40G DWDM: A case study in market fragmentation," **Communications and Photonics Conference and Exhibition (ACP).**, 2019, pp. 1-7.

APPENDIX

LIST OF PUBLICATIONS

1. R. Putthacharoen, P. Juleang, S. Mitatha, and P. P. Yupapin. 2011 "Novel optical cryptography using PANDA ring resonator for highly secured communication" **Journal of Spie – The International Society for Optical Engineering** (Impact Factor:2011:0.822).
2. S. Mitatha, R. Putthacharoen, and P. P. Yupapin. 2011 "THz frequency bands generation for Radio-over-Fiber systems" **Optik - International Journal for Light and Electron Optics** (Impact Factor:2010:0.454).
3. R. Putthacharoen, and Pratheep B. 2011 "Protecting Cookies from Cross Site Script Attacks Using Dynamic Cookies Rewriting Technique" **International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Republic of Korea** (Impact Factor:NA)..
4. R. Putthacharoen, and S. Miththa. 2011 "Estimated Transfer Time of Web Contents for Size Based scheduling" **International Conference on Embedded Systems and Intelligent Technology (ICESIT), Phuket, Thailand** (Impact Factor:NA).

Optical Engineering

SPIEDigitalLibrary.org/oe

Novel optical cryptography using PANDA ring resonator for highly secured communication

Rattipong Putthacharoen
Pakorn Juleang
Somsak Mitatha
Preecha P. Yupapin

Novel optical cryptography using PANDA ring resonator for highly secured communication

Rattipong Putthacharoen
Pakorn Juleang
Somsak Mitatha
King Mongkut's Institute of Technology Ladkrabang
Hybrid Computing Research Laboratory
Faculty of Engineering
Bangkok, 10520, Thailand

Preecha P. Yupapin
King Mongkut's Institute of Technology Ladkrabang
Nanoscale Science and Engineering Research Alliance (N'SERA)
Faculty of Science
Bangkok, 10520, Thailand
E-mail: kypreech@kmitl.ac.th

Abstract. We propose a novel method of an optical cryptography using the dark-bright soliton conversion control in a modified add/drop optical filter. By using the control arrangement, the obtained outputs of the dynamic states of dark-bright soliton can be used to form the key suppression for communication security application, in which the key recovery can be obtained by controlling the add/drop filter outputs. The optical cryptography consists of an add/drop filter which is used to generate the encryption and decryption keys from the optical keys (LIP signals). A Mach–Zehnder interferometer is used for multiplexing and de-multiplexing operations. Simulation results obtained shows, that the proposed system can be used to form a high security communication system. © *2011 Society of Photo-Optical Instrumentation Engineers (SPIE).* [DOI: 10.1117/1.3595425]

Subject terms: optical cryptography; communication security; key suppression; Key recovery.

Paper 110096R received Jan. 28, 2011; revised manuscript received May 6, 2011; accepted for publication May 9, 2011; published online Jul. 6, 2011.

1 Introduction

A PANDA ring resonator type has been successfully used to investigate the dynamic behavior of dark-bright soliton collision within the modified add/drop filter.[1–4] All optical devices are increasingly becoming important as integrated components for advanced optical technology applications and is widely used as optical sensor, signal processing, and optical communication. The communication security segment has been recognized as a promising tool for information that necessitates the security and privacy requirements due to the large demand of the world networks. Today, the security schemes, such as quantum and optical techniques, have been widely used in many applications such as sensors,[5] computing,[6] communication,[7] signal processing,[8] and especially optical device in security communications.[9–11] Recently, an optical device, known as a microring resonator in the form of an optical add/drop filter, has been found in many applications.[12–14] The authors have shown that the transmitted signals can be suppressed with the chaotic signals. The required signals could be retrieved by the add/drop filter and the encryption–decryption method by using the proposed optical design system. However, the search for new devices and techniques still remains. In this paper, the authors have proposed the use of key suppression and recovery for optical cryptography using a PANDA ring resonator for high security communication. The required key can be suppressed (buried) by the noisy signals, and the required signals can be secured and recovered (retrieved) by the specific designed optical device. The required data can be encrypted and decrypted by the optical encryption decryption keys, respectively, in which both keys can be generated by using the suppressed optical keys (LIP signals). In an application, such a proposed method can be used to form the secure communication either as digital or analog communications.

2 Proposed Modeling

The proposed system consists of three optical devices, namely a PANDA ring resonator, an add–drop filter, and Mach–Zehnder interferometer, as shown in Figs. 1, 2, and 3. The transmitter part of the optical cryptography system consists of a PANDA ring resonator, two add–drop filters, and one Mach–Zehnder interferometer. The receiver consists of two add–drop filters, and one Mach–Zehnder interferometer.

An add/drop filter and the double microring resonator known as a PANDA ring resonator, is shown in Fig. 1. To perform the dark-bright soliton conversion, the dark and bright solitons are first input into the add/drop optical filter system. The input optical field (E_{in}) and the control port optical field (E_{con}) of the bright and dark soliton pulses are given by[15]

$$E_{in}(t) = A \operatorname{sech}\left[\frac{T}{T_0}\right] \exp\left[\left(\frac{z}{2L_D}\right) - i\omega_0 t\right], \quad (1)$$

$$E_{con}(t) = A \tanh\left[\frac{T}{T_0}\right] \exp\left[\left(\frac{z}{2L_D}\right) - i\omega_0 t\right]. \quad (2)$$

Here A and z are the optical field amplitude and propagation distance, respectively. T is a soliton pulse propagation time in a frame moving at the group velocity, $T = t - \beta_1 z$, where β_1 and β_2 are the coefficients of the linear and second-order terms of Taylor expansion of the propagation constant. $L_D = T_0^2/|\beta_2|$ is the dispersion length of the soliton pulse. T_0 is a soliton pulse propagation time at initial input (or soliton pulse width), where t is the soliton phase shift time, and the frequency shift of the soliton is ω_0. This solution describes a pulse that keeps its temporal width invariance as it propagates, and thus is called a temporal soliton. When the soliton peak intensity ($|\beta_2/\Gamma T_0^2|$) is given, then T_0 is known. For the soliton pulse in the microring device, a balance should be achieved between the dispersion length (L_D) and the nonlinear length ($L_{NL} = 1/\Gamma\phi_{NL}$), where $\Gamma = n_2 k_0$, is the length scale over which dispe-rsive or nonlinear effects makes the beam become wider or narrower. For a soliton pulse, there is

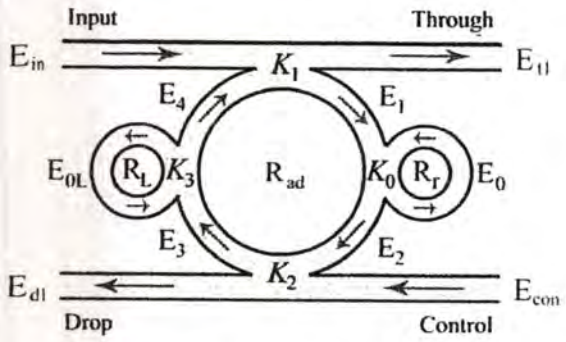

Fig. 1 Schematic diagram of PANDA ring resonator.

a balance between dispersion and nonlinear lengths, hence $L_D = L_{NL}$.

In Fig. 1, the PANDA ring resonator is used for the binary coded suppression. When the input light pulse passes through the first optical coupler of the add/drop optical multiplexing system, the transmitted and circulated optical fields can be written as[16]

$$E_{t1} = \sqrt{1-\gamma_1}\left[\sqrt{1-\kappa_1}E_{in} + j\sqrt{\kappa_1}E_4\right], \tag{3}$$

$$E_1 = \sqrt{1-\gamma_1}\left[\sqrt{1-\kappa_1}E_4 + j\sqrt{\kappa_1}E_{in}\right], \tag{4}$$

$$E_2 = E_0 E_1 e^{-\alpha/2L/2 - jk_n L/2}. \tag{5}$$

Here κ_1 is the intensity coupling coefficient, γ_1 is the fractional coupler intensity loss, α is the attenuation coefficient, $k_n = 2\pi/\lambda$ is the wave propagation number, λ is the input wavelength light field, and $L = 2\pi R_{ad}$, R_{ad} is the radius of add/drop device.

The optical fields at the second coupler of the add/drop optical multiplexing system are given by

$$E_{d1} = \sqrt{1-\gamma_2}\left[\sqrt{1-\kappa_2}E_{con} + j\sqrt{\kappa_2}E_2\right], \tag{6}$$

$$E_3 = \sqrt{1-\gamma_2}\left[\sqrt{1-\kappa_2}E_2 + j\sqrt{\kappa_2}E_{con}\right], \tag{7}$$

$$E_4 = E_{0L} E_3 e^{-\alpha/2L/2 - jk_n L/2}. \tag{8}$$

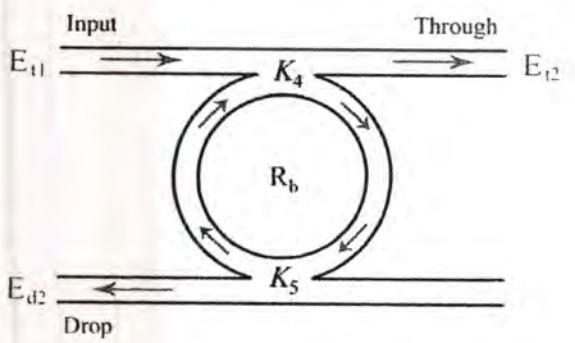

Fig. 2 Schematic diagram of the add/drop filter.

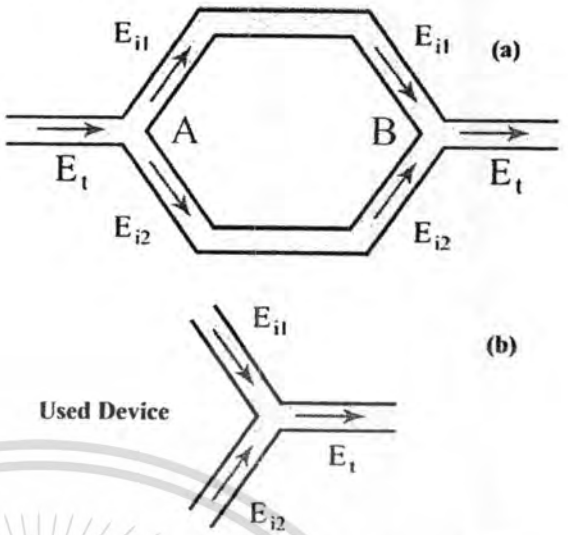

Fig. 3 Schematic diagram of the Mach–Zehnder interferometer.

Here κ_2 is the intensity coupling coefficient, and γ_2 is the fractional coupler intensity loss. The circulated light fields, E_0 and E_{0L}, are the light field circulated components of the microring radii, R_r and R_L which couples on to the right-hand side (RHS) and left-hand side (LHS) of the add/drop optical multiplexing system, respectively. The light field transmitted and circulated components on the RHS microring, R_r, are given by

$$E_2 = \sqrt{1-\gamma}\left[\sqrt{1-\kappa_0}E_1 + j\sqrt{\kappa_0}E_{r2}\right], \tag{9}$$

$$E_{r1} = \sqrt{1-\gamma}\left[\sqrt{1-\kappa_0}E_{r2} + j\sqrt{\kappa_0}E_1\right], \tag{10}$$

$$E_{r2} = E_{r1} e^{-\alpha/2L_1 - jk_n L_1}. \tag{11}$$

Here κ_0 is the intensity coupling coefficient, γ is the fractional coupler intensity loss, α is the attenuation coefficient, $k_n = 2\pi/\lambda$ is the wave propagation number, λ is the input wavelength light field, and $L_1 = 2\pi R_r$, R_r is the radius of right microring.

From Eqs. (9)–(11), the circulated roundtrip light fields of the RHS microring radii, R_r, are given in Eqs. (12) and (13), respectively,

$$E_{r1} = \frac{j\sqrt{1-\gamma}\sqrt{\kappa_0}E_1}{1-\sqrt{1-\gamma}\sqrt{1-\kappa_0}e^{-\alpha/2L_1 - jk_n L_1}}, \tag{12}$$

$$E_{r2} = \frac{j\sqrt{1-\gamma}\sqrt{\kappa_0}E_1 e^{-\alpha/2L_1 - jk_n L_1}}{1-\sqrt{1-\gamma}\sqrt{1-\kappa_0}e^{-\alpha/2L_1 - jk_n L_1}}. \tag{13}$$

Thus, the output circulated light field, E_0, for the right microring is given by

$$E_0 = E_1\left\{\frac{\sqrt{(1-\gamma)(1-\kappa_0)} - (1-\gamma)e^{-\alpha/2L_1 - jk_n L_1}}{1-\sqrt{(1-\gamma)(1-\kappa_0)}e^{-\alpha/2L_1 - jk_n L_1}}\right\}. \tag{14}$$

Similarly, the output circulated light field, E_{0L}, for the LHS microring at the left side of the add/drop optical multiplexing system is given by:

$$E_{0L} = E_3 \left\{ \frac{\sqrt{(1-\gamma_3)(1-\kappa_3)} - (1-\gamma_3)e^{-\alpha/2L_2 - jk_nL_2}}{1 - \sqrt{(1-\gamma_3)(1-\kappa_3)}e^{-\alpha/2L_2 - jk_nL_2}} \right\}, \tag{15}$$

where κ_3 is the intensity coupling coefficient, γ_3 is the fractional coupler intensity loss, α is the attenuation coefficient, $k_n = 2\pi/\lambda$ is the wave propagation number, λ is the input wavelength light field, and $L_2 = 2\pi R_L$, R_L is the radius of the LHS microring.

From Eqs. (3)–(15), the circulated light fields, E_1, E_3, and E_4 are defined by $x_1 = (1-\gamma_1)^{1/2}$, $x_2 = (1-\gamma_2)^{1/2}$, $y_1 = (1-\kappa_1)^{1/2}$, and $y_2 = (1-\kappa_2)^{1/2}$. Thus,

$$E_1 = \frac{jx_1\sqrt{\kappa_1}E_{in} + jx_1x_2y_1\sqrt{\kappa_2}E_{0L}E_{con}e^{-\alpha/2L/2 - jk_nL/2}}{1 - x_1x_2y_1y_2E_0E_{0L}e^{-\alpha/2L - jk_nL}}, \tag{16}$$

$$E_3 = x_2y_2E_0E_1e^{-\alpha/2L/2 - jk_nL/2} + jx_2\sqrt{\kappa_2}E_{con}, \tag{17}$$

$$E_4 = x_2y_2E_0E_{0L}E_1e^{-\alpha/2L - jk_nL} + jx_2\sqrt{\kappa_2}E_{0L}E_{con}e^{-\alpha/2L/2 - jk_nL/2}. \tag{18}$$

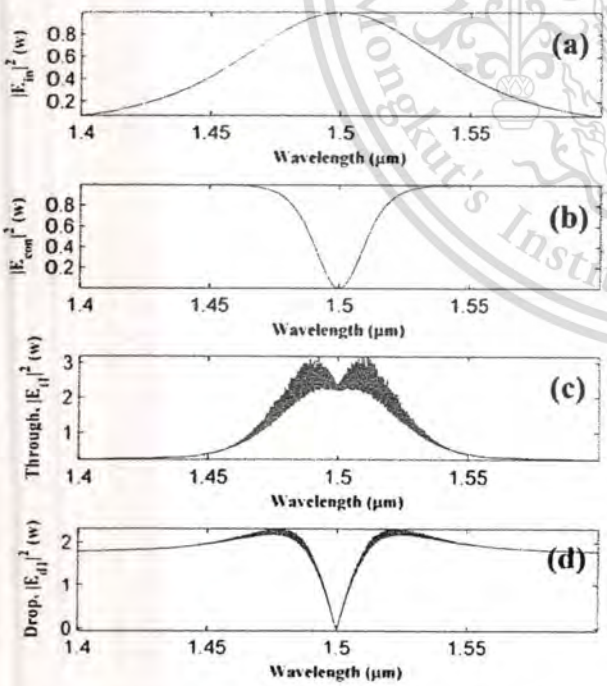

Fig. 4 Simulation result for optical key suppression, where (a) $|E_{in}|^2$, (b) $|E_{con}|^2$, (c) $|E_{t1}|^2$, and (d) $|E_{d1}|^2$, where $R_r = 15$ μm, $R_L = 15$ μm, $R_{sd} = 200$ μm, and $\alpha = 5 \times 10^{-5}$ dB mm^{-1}.

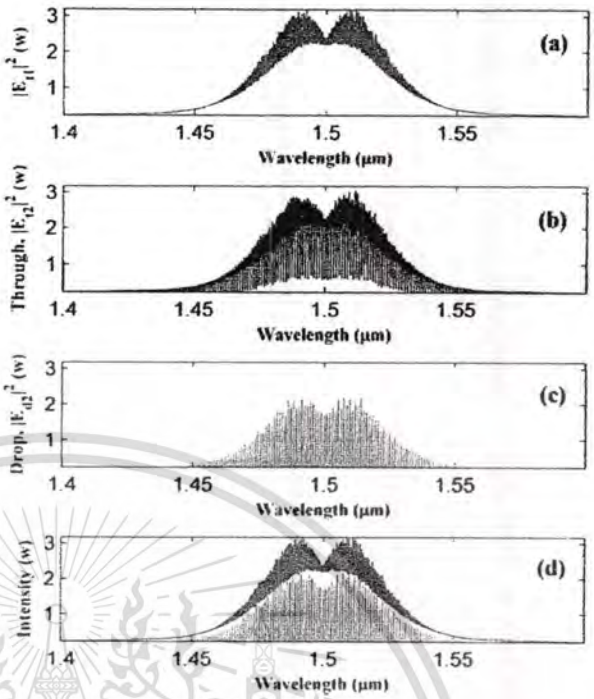

Fig. 5 Simulation result for optical key recovery, where (a) $|E_{t1}|^2$, (b) $|E_{t2}|^2$, (c) $|E_{d2}|^2$, and (d) comparison of key suppression and key recovery, where $R_b = 100$ μm and $\alpha = 5 \times 10^{-5}$ dB mm^{-1}.

From Eqs. (3), (5), and (16)–(18), the output optical field of the through port (E_{t1}) can be expressed as:

$$E_{t1} = x_1y_1E_{in} + \begin{pmatrix} jx_1x_2y_2\sqrt{\kappa_1}E_0E_{0L}E_1 \\ -x_1x_2\sqrt{\kappa_1\kappa_2}E_{0L}E_{i2} \end{pmatrix} e^{-\alpha/2L/2 - jk_nL/2}. \tag{19}$$

The power output of the through port (P_{t1}) is written by

$$P_{t1} = (E_{t1}) \cdot (E_{t1})^* = |E_{t1}|^2. \tag{20}$$

Similarly, from Eqs. (5), (6), and (16)–(18), the output optical field of the drop port (E_{d1}) is given by

$$E_{d1} = x_2y_2E_{con} + jx_2\sqrt{\kappa_2}E_0E_1e^{-\alpha/2L/2 - jk_nL/2}. \tag{21}$$

The power output of the drop port (P_{d1}) is expressed by

$$P_{d1} = (E_{d1}) \cdot (E_{d1})^* = |E_{d1}|^2. \tag{22}$$

An add/drop optical filter device with the appropriate parameters is shown in Fig. 2. The electric field detected by photodetector is given by[17]

$$E_{t2} = E_{t1}\frac{-\sqrt{1-\kappa_4}e^{-\alpha/2L_b - jk_nL_b} + \sqrt{1-\kappa_4}}{1 - \sqrt{1-\kappa_4}\sqrt{1-\kappa_5}e^{-\alpha/2L_b - jk_nL_b}}. \tag{23}$$

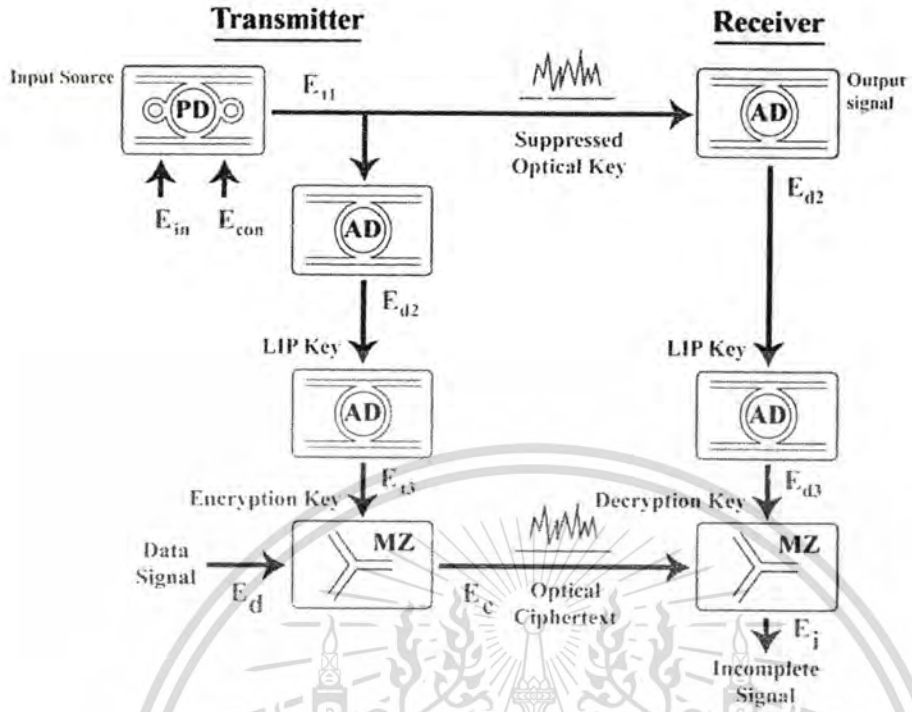

Fig. 6 Schematic diagram of optical cryptography system, where PA: PANDA ring resonator device, AD: add/drop filter device, and MZ: Mach–Zehnder interferometer device.

Here $L_b = 2\pi R_b$, R_b is the radius of the add/drop optical filter decoded as shown in Fig. 2. The power output of the drop port (P_{t2}) is expressed by

$$P_{t2} = (E_{t2}) \cdot (E_{t2})^* = |E_{t2}|^2 . \tag{24}$$

The electric field detected by photodetector is given by

$$E_{d2} = E_{t1} \frac{-\sqrt{\kappa_4 \kappa_5} e^{-\alpha/2 L_b/2 - j k_n L_b/2}}{1 - \sqrt{1-\kappa}\sqrt{1-\kappa_5} e^{-\alpha/2 L_b - j k_n L_b}} . \tag{25}$$

The power output of the drop port (P_{d2}) is expressed by

$$p_{d2} = (E_{d2}) \cdot (E_{d2})^* = |E_{d2}|^2 . \tag{26}$$

The proposed system uses the Mach–Zehnder interferometer as shown in Fig. 3. The required optical cryptography is performed by incorporating the Mach–Zehnder interferometer. Considering the output (E_t) at point B which is equal to input 1 (E_{i1}) plus input 2 (E_{i2}), the electric field detected by a photodetector is given by[18]

$$E_t = E_{i1} + E_{i2}. \tag{27}$$

The power output of the drop port (P_{d2}) is expressed by

$$P_t = (E_t) \cdot (E_t)^* = |E_t|^2 . \tag{28}$$

3 Key Suppression and Recovery

In simulation for optical key suppression, the used parameters of a PANDA ring resonator are fixed to be $\kappa_0 = 0.1$, $\kappa_1 = 0.2$, $\kappa_2 = 0.2$, and $\kappa_3 = 0.1$, respectively. The ring radii are $R_{ad} = 200\ \mu$m, $R_r = 15\ \mu$m, and $R_L = 15\ \mu$m. A_{eff} are 0.50, 0.25, and 0.25 μm^2 (Ref. 19) for the PANDA ring resonator, right and left microring resonators, respectively. For optical key recovery, the parameters of the add/drop filter are fixed to be $\kappa_4 = 0.5$, $\kappa_5 = 0.2$, $R = 100\ \mu$m, and $A_{eff} = 0.25\ \mu$m^2, respectively. Moreover, our optical key suppression and recovery system should be possible to be fabricated, which can be confirmed by using the practical device parameters. Simulation results of the opticale key signal with center wavelengths are at $\lambda_0 = 1.50\ \mu$m.

Figure 4 shows the simulation result for optical key suppression, where (a) $|E_{in}|^2$, (b) $|E_{con}|^2$, (c) $|E_{t1}|^2$, and (d) $|E_{d1}|^2$, where $R_r = 15\ \mu$m, $R_L = 15\ \mu$m, $R_{ad} = 200\ \mu$m, and $\alpha = 5 \times 10^{-5}$ dB mm^{-1}. Here Fig. 1(a) is the input port for optical key suppression. The bright soliton pulse with 1 W peak power is input into the input port. Figure 4(b) is the control port output that uses the dark soliton pulse with 1 W peak power. The power output of the drop port is shown in Figure 4(d). Figure 4(c) shows the power outputs of the through port, which is the optical key suppression signal that is transmitted to the receiver for secure optical communication, and that can be formed as the reference signal in communication. Moreover, the peak power outputs of the through port and drop port are 2.3 and 3.2 W, respectively. They are larger than the input light pulse due to the optical nonlinear effects.

Figure 5 shows the simulation result for optical key recovery, where (a) $|E_{t1}|^2$, (b) $|E_{t2}|^2$, (c) $|E_{d2}|^2$, and (d) comparison of suppression and recovery keys, where $R_b = 30\ \mu$m and $\alpha = 5 \times 10^{-5}$ dB mm^{-1}. Here Fig. 5(a) is the input port for optical recovery key. The suppression key signal, which looks like a noisy signal, input into this port is actually the highly secure optical communication. Figures 5(b) and 5(c)

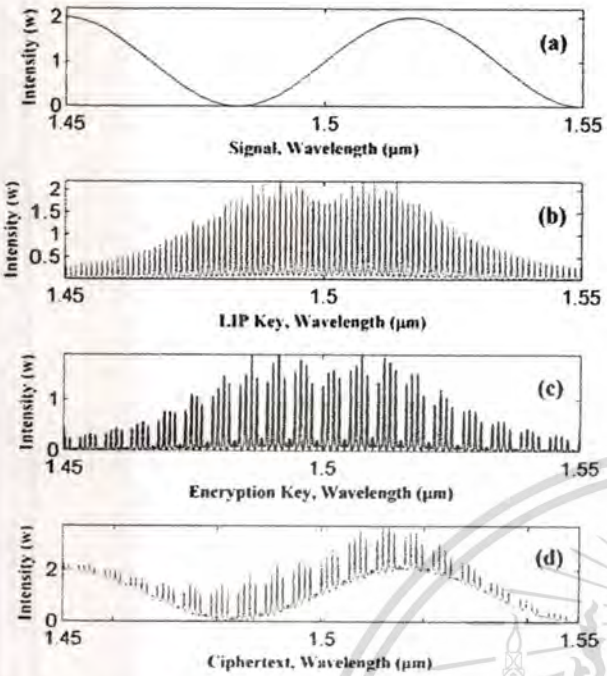

Fig. 7 Simulation result of optical cryptography at sender side, where (a) data signal, (b) LIP signal(key), (c) encryption key, and (d) ciphertext.

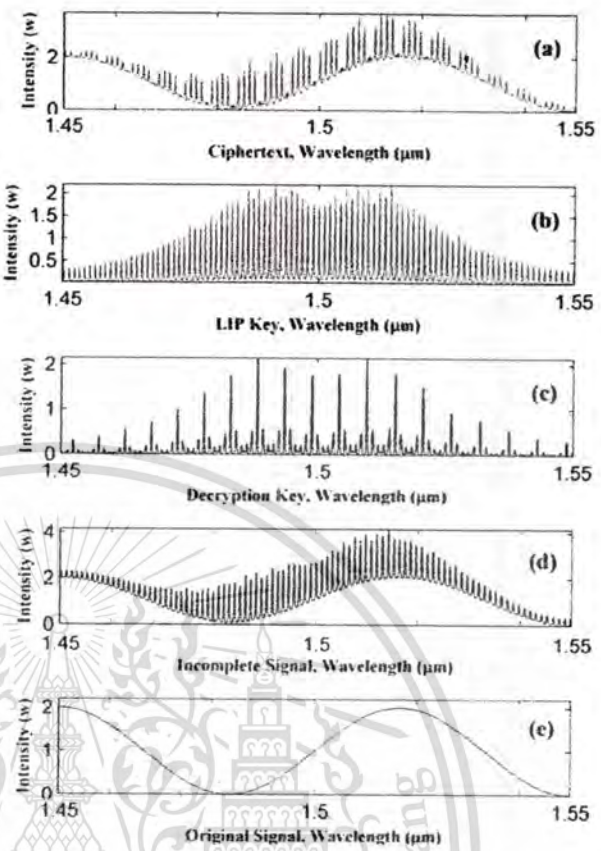

Fig. 8 Simulation result of optical cryptography at receiver side, where (a) ciphertext, (b) LIP signal (key), (c) decryption key, (d) incomplete data signal, and (e) original data signal.

shows the power output of the through and drop ports for signal recovery, respectively. The power output from the drop port is the analog signal which is sent by a sender and is used as an optical key in the cryptography system referred to as the LIP signal (key). Figure 5(d) shows the comparison of the suppressed optical key and recovered optical key, in which the secret signals are hidden by noisy signals.

4 Optical Cryptography System

Figure 6 shows the schematic diagram of an optical cryptography system, where PA refers to the PANDA ring resonator device, AD is an add/drop filter device, and MZ is the Mach–Zehnder interferometer device. The transmitter consists of 1 PA, 2 AD, and 1 MZ. Bright soliton pulse (E_{in}) and dark soliton pulse (E_{con}) is input into the input and control ports of the system (key suppression part) for key suppression. The output signal obtained is E_{t1}. It is the optical suppressed key which is sent to the receiver as a security signal as shown in Fig. 4(c). First, AD performs the optical key or LIP key which is generated at the transmitter side (E_{d2}) from the suppressed signal as shown in Fig. 5(c). Second, the AD function is generated by the LIP key to form the encrypted and decrypted keys. But the transmitter uses the encryption key from the encryption data by MZ. This means that the data which is encrypted is sent to the specific receiver, in which the LIP key from the recovery key becomes the ciphertext.

The receiver part consists of 2 AD and 1 MZ. The signal (E_{t1}) is sent into the input port by the transmitter as shown in Fig. 5(a). The output signal (E_{d2}) that departs from the drop port is the LIP key as shown in Fig. 5(c), is sent by the transmitter. The LIP key is used for encrypting and decrypting key generations. But the receiver part uses the decryption key from the data encryption by MZ. The decryption key is used for the ciphertext decryption, which is also sent by the transmitter. Thus, our proposed system can be claimed as a new and novel security technique using an optical cryptography design, in which the secret data can be in the form of analog or digital data signals. Moreover, this triple security function can be realized when the security can be formed by using the suppressed optical key, the optical key changing in every data frame, and a new optical cryptography technique.

Figure 7 shows the simulation result of optical cryptography at the sender side, where (a) data signal, (b) LIP key, (c) encryption key, and (d) ciphertext. Here, Fig. 7(a) is an example of the data signal (E_d). Figure 7(b) shows the LIP key which is generated by the key recovery par. Figure 7(c) shows the encryption key which is generated by the LIP key using the add/drop filter device. Figure 7(d) shows the optical ciphertext which originates from the encrypted key to encrypt the data signal. Figure 8 shows the simulation result of optical cryptography at the receiver side, where (a) ciphertext, (b) LIP key, (c) decryption key, (d) incomplete data signal and (e) original data signal. Figuer 8(a) shows the optical ciphertext which is sent by the transmitter. Figure 8(b) shows the LIP key which is generated by the key recovery part. Figure 8(c) shows the decryption key which is generated by the LIP key (E_{t2}) using the add/drop filter device. Figure 8(d) shows the incomplete data (E_i) signal which originates the decryption key to decrypt the ciphertext signal. Finally, the receiver can obtain the original signal (secret signal) as shown in

Figure 8(e) by using the original data (E_d) = incomplete data (E_i) – LIP key (E_{i2}).

5 Conclusion

A new novel design for optical communication security by using the key suppression and recovery methods, referred to as optical cryptography, has been demonstrated by using the dark-bright soliton pair within a PANDA ring resonator. The proposed system can be fabricated using practical PANDA ring resonator parameters. The key suppression is designed based on a PANDA ring resonator in which the key recovery is obtained by using the add/drop filter. The optical cryptography is designed using the add/drop filter and the Mach–Zehnder interferometer concept. The add/drop filter is used to generate the encryption, decryption keys from the LIP key, and the Mach–Zehnder interferometer is used for signal combination. The secured communication functions of the proposed optical cryptography system can be realized by using the suppressed key, which can be changed (rearranged) in every data frame. In conclusion, the simulation results obtained have shown that the proposed system can indeed be achieved via the key suppression and recovery for the optical cryptography system.

References

1. N. Suwanpayak, M. A. Jalil, C. Teeka, J. Ali, and P. P. Yupapin, "Optical vortices generated by a PANDA ring resonator for drug trapping and delivery applications," *Biomed. Opt. Express* **2**(1), 159–168 (2011).
2. P. P. Yupapin, N. Suwanpayak, B. Jukgoljun, and C. Teeka, "Hybrid transceiver using a PANDA ring resonator for nanocommunication," *Phys. Express* **1**(1), 1–8 (2011).
3. M. Tasakorn, C. Teeka, R. Jomtarak, and P. P. Yupapin, "Multitweezers generation control within a nanoring resonator system," *Opt. Eng.* **49**(7) 075002 (2010).
4. B. Jukgoljun, N. Suwanpayak, C. Teeka, and P. P. Yupapin, "Hybrid transceiver and repeater using a PANDA ring resonator for nano communication," *Opt. Eng.* **49**(12), 125003 (2010).
5. P. Hua, B. J. Luff, G. R. Quigley, J. S. Wilkinson, and K. Kawaguchi, "Integrated optical dual Mach–Zehnder interferometer sensor," *Sens. Actuators* **B 87**, 250–257 (2002).
6. C. Kostrzewa, R. Moosburger, G. Fischbeck, B. Schuppert, and K. Petermann, "Tunable polymer optical add/drop filter for multi-wavelength networks," *IEEE Photonics Technol. Lett.* **9**(11), 1487–1489 (1997).
7. P. D. Townsend, "Quantum cryptography on optical fiber networks," *Opti. Fiber Technol.* **4**(4), 345–370 (1998).
8. T. Carmon, T. J. Kippenberg, L. Yang, H. Rokhsari, S. Spillane, and K. J. Vahala, "Feedback control of ultra-high-Q microcavities: Application to micro-Raman lasers and microparametric oscillators," *Opt. Express* **13**(9), 3558–3566 (2005).
9. W. Siririth, S. Mitatha, O. Pingern, and P. P. Yupapin, "A novel temporal dark-bright solitons conversion system via an add/drop filter for signal security use," *Optik (Jena)* **121**(21), 1955–1958 (2010).
10. B. Knobnob, S. Mitatha, K. Dejhan, S. Chaiyasoonthorn, and P. P. Yupapin, "Dark–bright optical solitons conversion via an optical add/drop filter for signals and networks security applications," *Optik (Jena)* **121**(19), 1743–1747 (2010).
11. P. P. Yupapin, "Generalized quantum key distribution via micro ring resonator for mobile telephone networks," *Optik (Jena)* **121**(5), 422–425 (2010).
12. P. Gallion, F. Mendieta, and S. Jiang, "Signal and quantum noise in optical communications and cryptography," *Prog. Opt.* **52**, 149–259 (2009).
13. Y. Dumeige, C. Arnaud, and P. Féron, "Combining FDTD with coupled mode theories for bistability in micro-ring resonator," *Opt. Commun.* **250**(4–6), 376–383 (2005).
14. P. Rabiei, "Calculation of losses in micro-ring resonators with arbitrary refractive index or shape profile and its applications," *J. Lightwave Technol.* **23**(3), 1295–1301 (2005).
15. K. Sarapat, N. Sangwara, K. Srinuanjan, P. P. Yupapin, and N. Pornsuwancharoen, "Novel dark-bright optical solitons conversion system and power amplification," *Opt. Eng.* **48**, 045004 (2009).
16. T. Phatharaworamet, C. Teeka, R. Jomtarak, S. Mitatha, and P. P. Yupapin, "Random binary code generation using dark-bright soliton conversion control within a PANDA ring resonator," *J. Lightwave Technol.* **28**(19), 2804–2809 (2010).
17. D. G. Rabus, M. Hamacher, U. Troppenz, and H. Heidrich, "Optical filters based on ring resonators with integrated semiconductor optical amplifiers In GaInAsP–InP," *IEEE J. Sel. Top. Quantum Electron* **8**(6), 1405–1411 (2002).
18. A. Srivastava and S. Medhekar, "Switching of one beam by another in a Kerr type nonlinear Mach-Zehnder interferometer," *Opt. Laser Technol* **43**(1), 29–35 (2006).
19. Y. Kokubun, Y. Hatakeyama, M. Ogata, S. Suzuki, and N. Zaizen, "Fabrication technologies for vertically coupled microring resonator with multilevel crossing busline and ultracompact-ring radius," *IEEE J. Sel. Top. Quantum Electron.* **11**, 4–10 (2005).

Rattipong Putthacharoen received BEng and MEng degrees in computer engineering from King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand in 2000 and 2005, respectively. He is currently working toward a DEng degree in School of Computer Engineering, Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang. He is currently on the research staff in Hybrid Computing Research laboratory, Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang. His research interests are optical computing system, optical router and network, and network security.

Pakorn Juleang is a doctoral student in computer engineering at King Mongkut's Institute of Technology Ladkrabang (KMITL), Bangkok, Thailand. He is a lecturer in computer engineering at the KMITL and member of Hybrid Computing Research Laboratory (HCRL). His research interests are in the field of microprocessor and microcomputer design and verification, embedded system design and development, nonlinear optical communication, and hybrid computing system.

Somsak Mitatha received his BInd. degree in technology television, his MEng degree in electrical engineering, and a DEng degree in electrical engineer from King Mongkut's Institute of Technology Ladkrabang (KMITL), Bangkok, Thailand, in 1987, 1995, and 2008, respectively. He has been a member of the Department of Computer Engineering, where he is currently an associate professor in computer engineering. He has authored/co-authored 100 technical journal papers and 5 chapters and books. His research interests are in computer hardware design, pattern recognition, embedded systems, nonlinear optical communication, and computer network and security.

Preecha P. Yupapin received his PhD in electrical engineering from City University of London, United Kingdom in 1993. He is a professor of Applied Physics at the Department of Applied Physics, Faculty of Science, King Mongkut's Institute of Technology Ladkrabang (KMITL), Bangkok, Thailand. He has authored/co-authored more than 300 ISI journal papers and 20 chapters and books. He has supervised 60 PhD students and candidates in both local and international universities. He has also been appointed as an editorial board member and editor in chief of 6 international journals. His research interests are in optical sensors, nanophotonics, linear and nonlinear optical communication, nanomedicine, nano engineering, security camera, quantum information and network, hybrid communication networks, and innovative communication. He is a member of Thai Institute Physics (TIP), SPIE, and was a president of the OSA-Thailand Chapter from 2002 to 2004.

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

THz frequency bands generation for Radio-over-Fiber systems

S. Mitatha[a], R. Putthacharoen[a], P.P. Yupapin[b,*]

[a] Hybrid Computing Research Laboratory, Department of Computer Engineering, Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand
[b] Nanoscale Science and Engineering Research Alliance, Advanced Research Center for Photonics, Physics Division, Faculty of Science, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand

ARTICLE INFO

Article history:
Received 26 October 2010
Accepted 7 July 2011
Available online xxx

Keywords:
Radio-over-Fiber
DWDM
THz technology
Terabit wireless

ABSTRACT

We propose a new design THz frequency for Radio-over-Fiber (RoF) systems that use the dense wavelength division multiplexing wavelength enhancement, whereas the increasing in channel capacity and signal security can be provided. The increasing in number of channel can be obtained by the increasing in wavelength density, while the security is introduced by the specific wavelength filter, which is operated by the central operator. The optical communication wavelength enhancement is reviewed. The advantage is that the proposed system can be implemented and used incorporating with the existed communication link in both wire and terabit wireless communication system.

1. Introduction

The THz communication technology has become a part of all communication systems such as fiber optic communication, wireless communication, and RoF. The THz communication is effective data rate 1 Tbit/s [1] or communication with a THz carrier wave. The Gab of THz communication is using rang of frequency from 200 GHz to 10 THz. The THz can be generated by quantum transitions of light, which can generate very high intensity both the transition between the electric [2] and photonic [3] sources. The THz are becoming the high speed communication, one of them, the RoF is the fiber-wireless (WiFi) [4] network incorporate with optical communication and radio frequency with WDM and millimeter-wave (mm-wave) frequency [4]. The architecture of a mm-wave fiber-wireless architecture are central office (CO) which is connected to a large number of antenna or THz antenna [5] base station (BSs) via an optical fiber network over some the optical link method such as RF-over-fiber, IF-over-fiber, and Baseband-over-fiber [6]. These techniques transmitter deploys a Mach–Zehnder intensity (MZI) modulator to generate the required optical carrier frequency to provide point-to-point and point-to-multipoint links. The RoF, such as Hybrid Fiber Radio (HFR) [7] transmitted signals and then propagate over fiber links toward remote base stations (BSs) by using wavelength division multiplexing (WDM). The architecture is an attractive solution for broad-band access since they allow quick and cost-effective network deployment. Basically, the RoF systems are composing of central office (CO), base station (BSs) transmits optical carriers modulated at radio-frequency (RF). Optical fiber is an excellent medium for RF signal transmission due to the very high bandwidth (BW), low loss, light weight, small cross section, and low cost. In this ROF system, a head-end (HE), which consists of an optical-to-electrical (O/E) and electrical-to-optical (E/O) modules, is connected to the BS. A remote antenna unit (RAU) will be used in each picocell which connected to the HE by optical fibers. The RoF systems are applying for many wireless applications such as fiber-to-the-home (FTTH), Universal Mobile Telecommunications System (UMTS), Vehicular Ad-Hoc Network (VANET) [8] and microcellular system [9,10]. The microcellular system proposed the RoF for cellular systems by shares one optical source at the BS among all microcells, where frequency reuse is realized by external modulation of the optical carrier to improve the channel capacity. Intend to apply RoF for VANET, which proposed by the Intelligent Transport System (ITS) to serve numerous applications in area of vehicular system such as traffic monitoring, traffic conditions, traffic alert, and roadside service. These applications occur from difference technologies, for instance local area network (WLAN) or Wireless Fidelity (WiFi), and WiMAX or cellular network, which these models link both wire and wireless media. The RoF THz frequency can offer these technologies to improve the capacity and security, however, the bandwidth for usable are the important problem for this network. The THz communication is one alternative technology for the performance improvement. In these articles, we propose new platform to generate THz frequency for RoF system by using the dense wavelength division multiplexing (DWDM). The rest of this paper is structure as follows. Section 2 revises the operating principle. Section 3 proposed the DWDM

* Corresponding author.
E-mail address: kypreech@kmitl.ac.th (P.P. Yupapin).

0030-4026/$ – see front matter © 2011 Elsevier GmbH. All rights reserved.
doi:10.1016/j.ijleo.2011.07.013

generation for wireless link in RoF and shows the simulation results. In Section 4 is the conclusion of this work.

2. Operating principle

The basic of ring resonators operation, light from a monochromatic light source is launched into a ring resonator with constant light field amplitude (E_0) and random phase modulation as shown in Fig. 1, compose of terms in attenuation (α) and phase (ω_0) constants, which results in temporal coherence degradation. Hence, the time dependent input light field (E_{in}), without pumping term, can be expressed as [11]

$$E_{in}(t) = E_0 e^{-\alpha L + j\phi_0(t)} \tag{1}$$

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

$$n = n_0 + n_2 I = n_0 + \left(\frac{n_2}{A_{eff}}\right) P, \tag{2}$$

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 [12].

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 [14]

$$\left|\frac{E_{out}(t)}{E_{in}(t)}\right|^2 = (1-\gamma) \times \left[1 - \frac{(1-(1-\gamma)x^2)\kappa}{(1-x\sqrt{1-\gamma}\sqrt{1-\kappa})^2 + 4x\sqrt{1-\gamma}\sqrt{1-\kappa}\,\sin^2\left(\frac{\phi}{2}\right)}\right] \tag{3}$$

Eq. (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, $(1-\kappa)$, and a fully reflecting mirror. κ is the coupling coefficient, and $x = \exp(-\alpha L/2)$ represents a roundtrip loss coefficient, $\phi_0 = kLn_0$ and $\phi_{NL} = kL(n_2/A_{eff})P$ are the linear and nonlinear phase shifts, $k = 2\pi/\lambda$ is the wave propagation number in a vacuum. Where L and a are a waveguide length and linear absorption coefficient, respectively. In this work, the iterative method is introduced to obtain the results as shown in Eq. (3), similarly, when the output field is connected and input into the other ring resonators.

The input optical field as shown in Eq. (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 Eq. (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 Eqs. (4) and (5) [13,14].

$$\left|\frac{E_t}{E_{in}}\right|^2 = \frac{(1-\kappa_1) - 2\sqrt{1-\kappa_1}\cdot\sqrt{1-\kappa_2}e^{-(\alpha/2)L}\cos(k_n L) + (1-\kappa_2)e^{-\alpha L}}{1+(1-\kappa_1)(1-\kappa_2)e^{-\alpha L} - 2\sqrt{1-\kappa_1}\cdot\sqrt{1-\kappa_2}e^{-(\alpha/2)L}\cos(k_n L)} \tag{4}$$

and

$$\left|\frac{E_d}{E_{in}}\right|^2 = \frac{\kappa_1\kappa_2 e^{-(\alpha/2)L}}{1+(1-\kappa_1)(1-\kappa_2)e^{-\alpha L} - 2\sqrt{1-\kappa_1}\cdot\sqrt{1-\kappa_2}e^{-(\alpha/2)L}\cos(k_n L)} \tag{5}$$

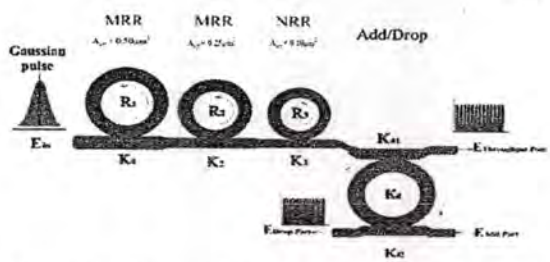

Fig. 1. A schematic of a Gaussian soliton generation system, where R_s: ring radii, κ_s: coupling coefficients, R_d: an add/drop ring radius, A_{eff}: effective areas, MRR: microring resonator, NRR: nanoring resonator, K_{42} and K_{42} are add/drop coupling coefficients.

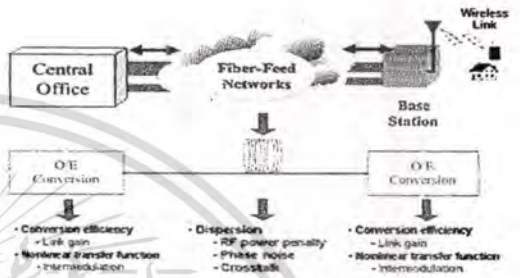

Fig. 2. Overview of optical impairments in mm-wave fiber-wireless links [6].

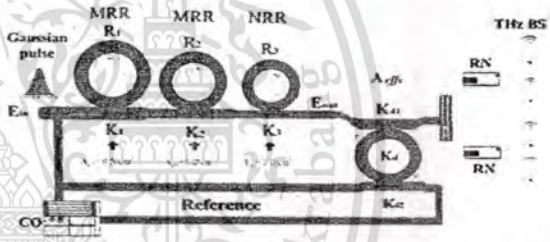

Fig. 3. The THz RoF System, where R_s: ring radii, κ_s: coupling coefficients, R_d: an add/drop ring radius, A_{eff}: Effective areas, MRR: Microring resonator, NRR: Nanoring resonator, K_{42} and K_{42} are add/drop coupling coefficients.

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 [15]. 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. κ_1 and κ_2 are coupling coefficient of add/drop filters, $k_n = 2\pi/\lambda$ is the wave propagation number for in a vacuum, and the waveguide (ring resonator) loss is ($=0.5$ dB mm^{-1}. The fractional coupler intensity loss is $\gamma = 0.1$. In the case of add/drop device, the nonlinear refractive index is neglected.

Please cite this article in press as: S. Mitatha, et al., THz frequency bands generation for Radio-over-Fiber systems. Optik - Int. J. Light Electron Opt. (2011), doi:10.1016/j.ijleo.2011.07.013

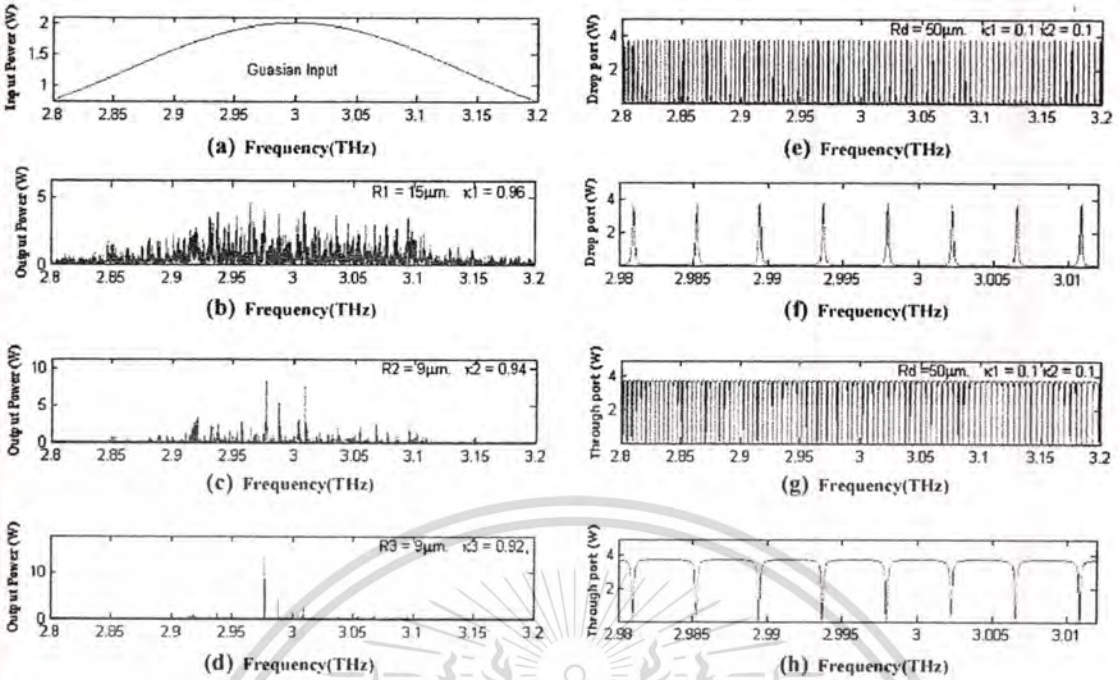

Fig. 4. Results of the THz frequency band with the center frequency at 3 THz, where (a) the input Gaussian pulse, (b) the large bandwidth signal, (c) the filtering and amplifying signals, (d) output frequency band, (e) and (f) are the drop port signals, (g) and (h) are the through port signals.

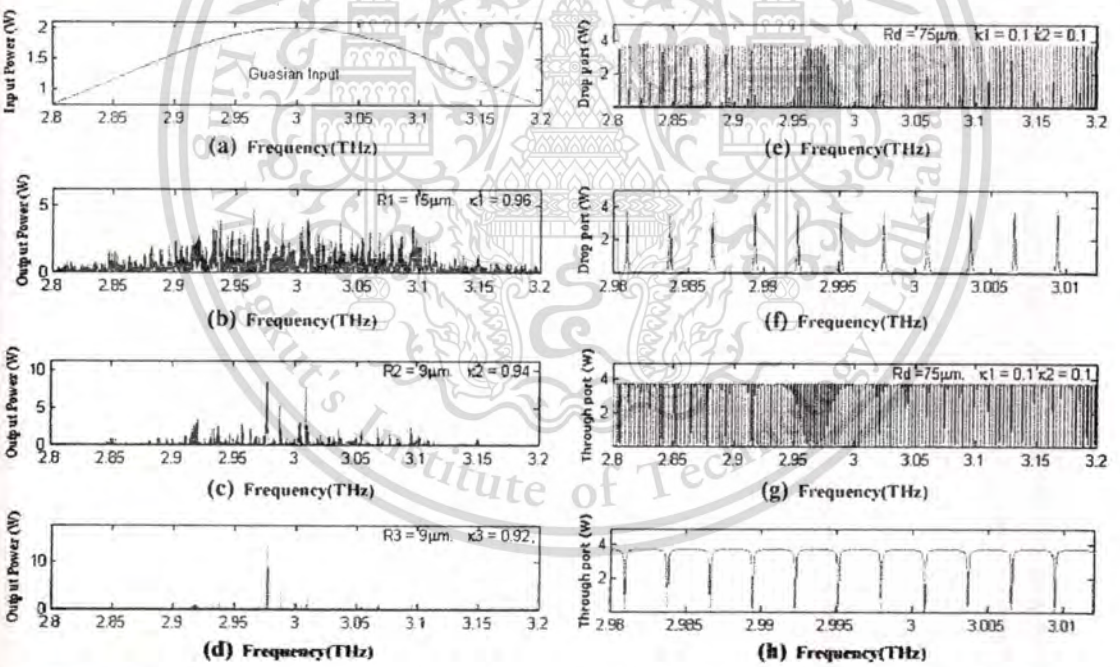

Fig. 5. Results of the THz frequency band with the center frequency at 3 THz, where (a) the input Gaussian pulse, (b) the large bandwidth signal, (c) the filtering and amplifying signals, (d) output frequency band, (e) and (f) are the drop port signals, (g) and (h) are the through port signals.

3. The THz generation

The basic RoF is show in Fig. 2, which the DWDM optical signals are generation from central office, then communicate via fiber-feed to remote note (RN) or base stations and the last, the base station convert the optical signal to THz wireless. In currently, the optical wavelengths for the use are 1.3 μm and 1.55 μm. In this article, we replace these wavelength by propose the terahertz wavelength is 3 THz by generate from the micro ring resonators.

From Figs. 1 and 3, 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 device (second 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 (frequency) is input into the system. In practice, the maximum frequency that can be confined within the optical waveguide has been increased by using the composite of materials

Please cite this article in press as: S. Mitatha, et al., THz frequency bands generation for Radio-over-Fiber systems. Optik - Int. J. Light Electron Opt. (2011), doi:10.1016/j.ijleo.2011.07.013

known as meta-materials [16], which is shown that the wavelength close to few mm (THz region) can be confined within the waveguide. In operation, 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 device (second ring) as shown in Fig. 1. Finally, the required signals can be obtained via a drop port of the add/drop filter. An optical field in the form of Gaussian pulse from a laser source at the specified center frequency is input into the system.

From Fig. 4, the Gaussian pulse with center frequency (f_0) at 3.0 THz, 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. 4(a). The large bandwidth signals can be seen within the first microring device, and shown in Fig. 4(b). The suitable ring parameters are used, for instance, ring radii $R_1 = 15.0\ \mu m$, $R_2 = R_3 = 9.0\ \mu m$, and $R_d = 50.0\ \mu m$. In order to make the system associate with the practical device [17,18], the selected parameters of the system are fixed to $n_0 = 3.34$ (**InGaAsP/InP**), $A_{eff} = 0.50\ \mu m^2$ and $0.25\ \mu m^2$ for a microring and add/drop ring resonator, respectively, $\alpha = 0.5\ dB\ mm^{-1}$, $\gamma = 0.1$. In this investigation, the coupling coefficient (kappa, κ) of the microring resonator is ranged from 0.10 to 0.96. The nonlinear refractive index of the microring used is $n_2 = 2.2 \times 10^{-17}\ m^2/W$. In this case, the attenuation of light propagates within the system (i.e. wave guided) used is $0.5\ dB\ mm^{-1}$. 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 [13], which is shown in Fig. 4(b). The large bandwidth signal is generated within the first ring device. In applications, the specific input or output frequencies can be used and generated, where the suitable parameters are used and shown in the figures. The similar manner is as shown in Fig. 5, where the different parameters are the R_d radii and coupling coefficients, where the small FSR is obtained. In Fig. 5, results of the THz frequency band with the center frequency at 3 THz, where (a) the input Gaussian pulse, (b) the large bandwidth signal, (c) the filtering and amplifying signals, (d) output frequency band, (e) and (f) are the drop port signals, (g) and (h) are the through port signals.

In application, the use of the generated frequency band for RoF communication which corporate wire and both up-down links for wireless link is employed via THz antenna. Furthermore, there are several frequency bands available as shown in Figs. 4 and 5, which can be brought the high capacity channels and multi switching system in the RoF system, which is discussed in the previous. By using the propose design as shown in Fig. 3, the extended light source frequency bands can be used for multi frequency switching, which can be used employed via the wireless or simultaneous up link and down link system [19], the higher channel capacity can also be obtained by using FSR modification and more available frequency bands, for instance, the use of system different parameters can provide more frequency bands as shown in Fig. 5. The generated carrier signals can be used as the modulated carrier that can be used to form the simultaneous up and down link and multi switching, which is controlled by a computer server. This can also be used with the existed public network installation or Ad Hoc network applications. Furthermore, the pumping part is not required in such a system. The new available frequency bands can be use to form the new multi-frequency layer protocol, where more communication capacity can be performed.

4. Conclusion

We have shown that the multi frequency bands can be generated by using a Gaussian pulse propagating within the micro ring resonator system, which can be simultaneous link within a single device and available for the extended multi switching application with the frequency center at the THz band. This can be used with the existed public networks, mobile network, and hybrid network. In this work, generate the high bandwidth THz enhancements DWDM communication for RoF systems to link both wire and wireless network. The THz DWDM bands can be generating by using a 3 THz center wavelength of Gaussian pulse propagating within micro-ring and nano-ring resonator. The system is capable of simultaneous link within a single device and is available for extended multi switching application with the frequency centered at the THz band. The DWDM in this article occurred form nonlinear effect and resonance of pulse in micro-ring and nano-ring resonator. This work the can be generating great number of bandwidth are the pulse 22 channels and FSR ≈ 0.00125 THz which from bandwidth ranges from 2.98 to 3.01 THz.

References

[1] K.C. Huang, Z. Wang, Terahertz terabit wireless communication, IEEE Microwave Maga. (2011) 108–116.
[2] W.R. Deal, X.B. Mei, V. Radisic, K. Leong, S. Sarkozy, B. Gorospe, J. Lee, P.H. Liu, W. Yoshida, J. Zhou, M. Lange, J. Uyeda, R. Lai, Demonstration of a 0.48 THz amplifier module using InP HEMT transistors, IEEE Microw. Wirel. Compon. Lette. 20 (5) (2010) 289–291.
[3] F. Blanchard, G. Sharma, L. Razzari, X. Ropagnol, H. Bandulet, F. Vidal, R. Morandotti, J. Kieffer, T. Ozaki, H. Tiedje, H. Haugen, M. Reid, F. Hegmann, Generation of intense terahertz radiation via optical methods, IEEE J. Sele. Quan. Elect. 17 (1) (2011) 5–16.
[4] N. Ghazisaidi, M. Maier, C. Assi, Fiber-wireless (FiWi) access networks: a survey, IEEE J. Commun. 47 (2) (2009) 160–167.
[5] E. Vourch, B. Della, D.L. Berre, D. Herve, Millimeter-wave power-fading compensation for WDM fiber-radio transmission using a wavelength-self-tunable single-sideband filter, IEEE Trans. Microwave 50 (12) (2002) 3009–3015.
[6] A. Sharma, G. Singh, Rectangular microstirp patch antenna design at THz frequency for short distance wireless communication systems, Springer Link J. Infra. Milli THz Wave 30 (1) (2009) 1–7.
[7] C. Lim, A. Nirmalathas, M. Bakaul, P. Gamage, K.L. Lee, Y. Yang, D. Novak, R. Waterhouse, Fiber-wireless networks and subsystem technologies, IEEE J. Lightwave Technol. 28 (4) (2010) 390–405.
[8] C.T. Lin, J. Chen, P.C. Peng, C.F. Peng, W.R. Peng, B.S. Chiou, S. Chi, Hybrid optical access network integrating fiber-to-the-home and radio-over-fiber systems, IEEE Photo. Tech. Lett. 19 (8) (2007) 610–612.
[9] H.B. Kim, M. Emmelmann, B. Rathke, A. Wolisz, A radio over fiber network architecture for road vehicle communication systems, IEEE Vehi. Tech. Conference (VTC-2005) (5) (2005) 2920–2924.
[10] J.S. Wu, J. Wu, H.W. Tsao, A radio-over-fiber network for microcellular system application, IEEE Trans. Vehicular Tech. 47 (1) (1998) 84–94.
[11] N. Pleros, K. Vyrsokinos, K. Tsagkaris, N.D. Tselikas, A 60 GHz radio-over-fiber network architecture for seamless communication with high mobility, IEEE J. Lightwave. Technol. 27 (12) (2009) 1957–1967.
[12] D. Deng, Q. Guo, Ince-Gaussian solitons in strongly nonlocal nonlinear media, Opt. Lett. 32 (2007) 3206–3208.
[13] Q. Xu, M. Lipson, All-optical logic based on silicon micro-ring resonators, Opt. Exp. 15 (3) (2007) 924–929.
[14] P.P. Yupapin, W. Suwancharoen, Chaotic signal generation and cancellation using a microring resonator incorporating an optical add/drop multiplexer, Opt. Commun. 280 (2) (2007) 343–350.
[15] P.P. Yupapin, P. Saeung, C. Li, Characteristics of complementary ring-resonator add/drop filters modeling by using graphical approach, Opt. Commun. 272 (2007) 81–86.
[16] M. Fujii, J. Leuthold, W. Freude, Dispersion relation and loss of subwavelength confined mode of metal-dielectri-gap optical waveguides, IEEE Photon. Technol. Lett. 21 (6) (2009) 362–364.
[17] Y. Kokubun, Y. Hatakeyama, M. Ogata, S. Suzuki, N. Zaizen, Fabrication technologies for vertically coupled micro ring resonator with multilevel crossing busline and ultracompact-ring radius, IEEE J. Sel. Top. Quantum Electron. 11 (2005) 4–10.
[18] Y. Su, F. Liu, Q. Li, System performance of slow-light buffering, and storage in silicon nano-waveguide, Proc. SPIE 6783 (2007) 7832P.
[19] S. Mithata, N. Pornsuwancharoen, P.P. Yupapin, A simultaneous short wave and millimeter wave generation using a soliton pulse within a nano-waveguide, IEEE Photon. Technol. Lett. 21 (13) (2009) 932–934.

Please cite this article in press as: S. Mitatha, et al., THz frequency bands generation for Radio-over-Fiber systems. Optik - Int. J. Light Electron Opt. (2011), doi:10.1016/j.ijleo.2011.07.013

Protecting Cookies from Cross Site Script Attac Using Dynamic Cookies Rewriting Technique

Rattipong Putthacharoen*, Pratheep Bunyatnoparat *

*Department of Computer Engineering, Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand

s8060056@kmitl.ac.th,kbprathe@kmitl.ac.th

***Abstract*— Web applications often use cookies for maintaining an authentication state between users and web applications, these cookies are typically sent to the users by the web applications after the users have been successfully authenticated. Every subsequent request that contains the valid cookies will be automatically allowed by the web applications without any further authentication. The cookies are used to both identify and authenticate the users; therefore they are an interesting target for potential attackers. Cross Site Scripting attack (XSS for short) is one of popular attacks which is often used to steal the cookies from a browser's database. In this paper, we introduce a new technique called "Dynamic Cookies Rewriting", this technique aims to render the cookies useless for XSS attacks. Our technique is implemented in a web proxy where it will automatically rewrite the cookies that are sent back and forth between the users and the web applications. With our technique in place, the cookies at the browser's database now are not valid for the web applications; therefore the XSS attack will not be able to impersonate the users using stolen cookies.**

***Keywords*— Cookies, Cross Site Script Attacks, Web Proxy, HTTP and HTTPs.**

I. INTRODUCTION

In World Wide Web, web browsers and web applications communicate to each other through HTTP. The HTTP is a stateless protocol [1] which the web browsers send requests for resources and the web applications supply those resources, no session states are retained. The web applications generally use cookies to provide a mechanism for creating stateful HTTP sessions. The cookies are supported by nearly all modern browsers and therefore allow for a great flexibility in how user sessions are managed by the web applications. For web applications that require authentication, they often use the cookies to store session IDs [2], and then pass the cookies to users after they have been authenticated. The cookies are stored in the user's web browser. The web browser returns the cookies every time it needs to reconnect as a part of an active session and then the web application associates the cookies with the user. As the cookies can both identify and authenticate the users [3], this makes the cookies a very interesting target for attackers. In many cases, the attacker who can obtain valid cookies of the user session can use them to directly enter that session. Cross Site Script (XSS) attack is one of popular attacks which is often used to steal the cookies using a malicious script. The malicious script on executing steals the cookies of the user from a browser's database and sends them to the attacker who can then use them for malicious purposes. With the cookies of the user in hand, the attacker can impersonate the user and then acts instead of that user, and interacts with the web application.

The remainder of this paper is organized as follows. Section II discusses topics which are related to a proposed approach: XSS attack types, cookie mechanism, a concept of a web proxy, and basic protections of the cookies. Section III presents the proposed approach. We then evaluate the proposed approach in section IV, and discuss about challenges in section V. Finally, we conclude and also brief the future work in Section VI.

II. BACKGROUND

A. XSS Attack Types

There is no standardized classification of the XSS attacks, obviously there are two well known types of the XSS attacks [4][5]: Non-persistent, and Persistent.

1) Non-persistent (or reflected) XSS: means that malicious code is not persistently stored in a vulnerable server, but it is immediately echoed by the vulnerable server back to a victim.

To consider Figure 1, if the victim is accessing www.bank.com in order to do an online transaction, in the same time the victim may also be accessing www.attacksite.com, and be persuaded into clicking on a below link:

```
<a href = "http://www.bank.com/
<SCRIPT>
  document.location ='http://www.attacksite.com/
  stealcookie.php?'+document.cookie;
</SCRIPT>">
Click here to win a million dollars.
</a>
```

Figure 1. Example of Non-persistent XSS attack

When the victim clicks on the link, the malicious script will be sent to the web server (www.bank.com) as a requested page. Once the web server cannot find the requested page, it

will usually return an error page. The web server may also decide to include a name of the requested page in the error page which is actually the malicious script. When the malicious script is executed on the victim's browser, the cookies of the www.bank.com will then be sent to the www.attacksite.com. An owner of the www.attacksite.com can use those cookies to impersonate the victim with respect to the www.bank.com. The malicious script can read the cookies of the www.bank.com without being denied by the same origin policy [13] because it was echoed by the www.bank.com, so it has the same origin as the cookies.

2) Persistent (or stored) XSS: means that the malicious code is persistently stored in a server's storage, and may later be embedded in an HTML page sent to the victim.

To consider a script shown in Figure 2 which it is posted on an online message board of the www.bank.com.

```
Click here to see a new promotion.
<SCRIPT>
  document.images[0].src=http://www.attacksite.com/
  images.jpg?stealcookie+ document.cookie;
</SCRIPT>
```

Figure 2. Example of Persistent XSS attack

The victim who reads a message will receive the malicious script as a part of the message. The victim's browser will then execute the malicious script which will later send the cookies of the www.bank.com to the www.attacksite.com. Again the malicious script can read the cookies of the www.bank.com because it was loaded from the www.bank.com which has the same origin as the cookies.

Some authors have also presented the other advance XSS attacks such as DOM-based XSS [5]-[7] attack, Induced XSS [7] and so on but they are out of scope of this paper.

B. COOKIES

The cookies are a mechanism to provide stateful communications over the HTTP. As mentioned earlier, the cookies are broadly used to store the session IDs or personal sensitive information in today's web applications. The cookies are sent by the web application as a part of a response message using Set-Cookie or Set-Cookie2 header. The browser stores the cookies in its database, and includes the cookies with every subsequent request to the web application. The browser uses Cookie header to return the cookies, as shown in Figure 3.

In general the cookies can be classified into two types: session cookies and persistent cookies [1].

- Session cookies are temporarily used; they are discarded when the browser is closed.
- Persistent cookies can be kept longer until they expire, they are stored on a disk and survive across a computer restarts.

There are two different version of cookie specifications in use [1]: Version 0 cookie (NetScape cookie), and Version 1 cookie (RFC 2965). The version 0 cookie is the most widely used version, it defines the Set-Cookie header, and header as follows.

Set-Cookie: name=vale [;expires=date] [;path=patn] [;domain=domain] [;secure]

Cookie: name = value

For example:

Set-Cookie:SID= 123abc;domain=.kmitl.ac.th

Cookie: SID=123abc

In version 0, the cookies are identified by the combination of the following attributes: name, domain, and path. The web server can use an arbitrary string as the value of the name attribute. The domain and path attributes inform the browser that the cookie must be sent back to the server when requesting URL of a given domain and path. If the domain and path attributes are not specified, then they default to the domain and path of the requested object. The expires and secure attributes are possibly not used.

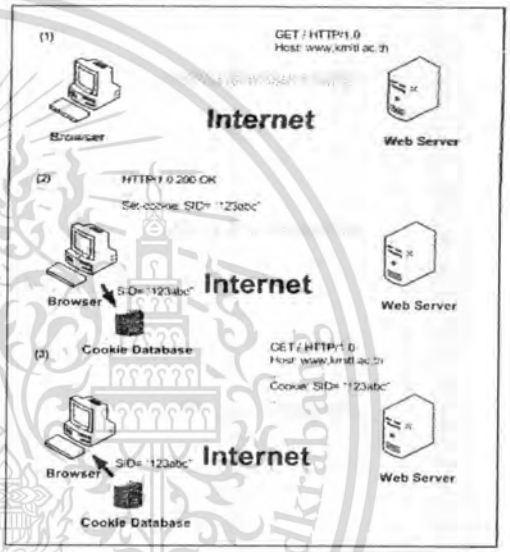

Figure 3. The web server and client exchange the cookies

The version 1 cookie is an extended version of Netscape cookie. In addition to indentifying the cookies by name, domain and path attributes as in the version 0, the version 1 adds an ability to identify the cookie by the port attribute as well. The web server must set the cookie using the Set-Cookie2 header instead of the Set-Cookie header. The browser still returns the cookie using the Cookie header as the version 0 but uses a different format [1]. The web server must always specify the value of the name attribute and the cookie version in the cookie, and the browser must return the same values. Almost all modern browsers (latest versions at the time of this writing) do not support the version 1 cookie except Opera browser [14][15], so the version 1 cookie is not widely used by web developers. The following example shows the Set-Cookie2 header and the Cookie header that are used in the version 1 cookie:

Set-Cookie2: SID= "123abc"; versions= "1"

Cookie: $version= "1";
SID= "123abc"

The domain and path attributes default to the domain and path of the requested object as in the version 0. The port attribute can be as follows:

- The web server explicitly specifies the port attribute along with its portlist in the cookie, e.g. Set-Cookie2: SID= "123abc"; versions= "1"; port= "80,8000".
- If the web server includes the port attribute but without specifying the portlist, e.g. Set-Cookie2: SID= "123abc"; versions= "1";port, then the port attribute defaults to the port that the object was requested.
- If the web server does not include the port attribute in the cookie, then it allows "Any" port

In version 1, the web server is possible to include the following attributes in the version 1 cookie as well [1]: comment, commentURL, discard, max-age, and secure.

The browser discards the cookies, if those cookies are under any of the following conditions:

- The browser is closed, if the cookie is not persistent.
- An expiration date has been passed or changed to a date in the past.
- The user forces to delete the cookies.

C. *Web Proxy*

The web proxy is an intermediary or a middleman [1] that fulfills transactions on behalf of clients, many organizations allow the users only to access the internet via the web proxy. It is an important control point for web surfing which is commonly built in with various security capabilities. The web proxy can be a separate device or a part of a firewall. It must sit between the clients and the web servers, and acts as both the client to the web server and the web server to the client. All web connections from the clients are intercepted at the web proxy, and then the web proxy will initiate new web connections to the web servers on behalf of the clients, see Figure 4.

Today web proxy can intercept both HTTP and HTTPs connections [8]-[10] so it can have a full control on both protocols. A main difference between the HTTP and the HTTPs is that the HTTPs sends HTTP requests and responses over SSL connections that encrypt all data. In order to see web contents inside the SSL connections, the web proxy must be able to terminate and also initiate the SSL connections [1].

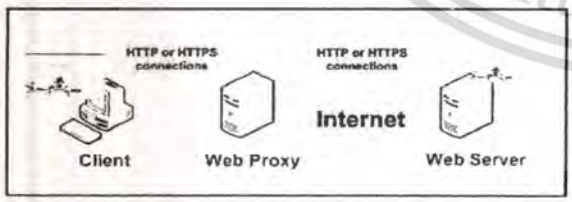

Figure 4. Web Proxy intercepts both HTTP and HTTPs

D. *Protection of Cookies*

It is possible to totally disable using the cookies, but it may cause the web servers denying to work without the cookies. So instead of disabling the cookies, in this session we will discuss about common solutions to protect from the attacks [2].

1) IP Mapping: The web server maps IP addresses of the users with the cookies and denies any access that comes from invalid IP addresses. This helps to mitigate the problem but it does not work where the users access the Internet through the web proxy.

2) HttpOnly Attribute: HttpOnly attribute is a Microsoft extension, it can also be included in the cookies before being sent to the browser. With the HttpOnly attribute, the browser will deny scripting languages to access those cookies. The HttpOnly attribute is originally not a part of the HTTP; the browsers that are not aware of this attribute will ignore it and will consequently remain vulnerable.

3) Secure Cookies: Secure cookies mean that the clients and the web servers only send the cookies via the SSL connections. When using the SSL, all requests and responses are encrypted including the cookies. This can protect the cookies from sniffing whenever they are sent across the network; however this cannot protect the cookies on the browser itself.

No solutions mentioned above can guarantee that the cookies will be safe from the XSS attacks. We propose a new approach in the next section which aims not to protect the cookies but instead renders the cookies not reusable for the attackers.

III. Our Approach

In this section, we present the new approach that significantly protects the cookies from the XSS attacks. Our approach can be implemented simply in the web proxy without any change required on both web browser and web server. We propose a new technique called "Dynamic Cookie Rewriting" which is then implemented as a part of our web proxy. With this technique in place, the web proxy will automatically rewrite the value of the name attribute in the cookie with the randomized value before sending the cookie to the browser, so the browser will keep the randomized value in its database instead of the original value sent by the web server. The returned cookie from the browser will also be rewritten back to the original value at the web proxy before being forwarded to the web server. As the browser's database does not store the original values of the cookies, so even the XSS attacks can steal the cookies from the browser's database, the cookies cannot be used later to impersonate the users

Our approach supports both version 0 and version 1 cookies. We design a table for storing the cookies of both versions as follows.

TABLE I. Table for Storing the Attribute Values

Name	Domain	Path	Port	Original Value	Randomized Value
SID	kmitl.ac.th	/	Any	123abc	&^@#$5

We use four attributes to identify the cookies: name, domain, path and port. The port attribute will only be used with the version 1 cookie. After the web proxy reads the cookies from the response message sent by the web server, it will store all required attribute values into the table as shown in the Table I, and rewrites the values of the name attributes with the randomized values before sending to the browser. The randomized values will also be kept on the same table. The web proxy will only change the name attribute of the cookie, the other attributes will remain the same.

The domain, path or port attributes may not be included in the cookies sent by the web server, if this happens, the following rules will be applied:

- The domain attribute defaults to the same as the requested object, so the web proxy will store the domain of the requested object into the table.
- The path attribute also defaults to the same as the requested object, the web proxy will store the path of the requested object into the table too.
- If the web server includes the port attribute but without specifying the portlist, then the port attribute defaults to the port that the object was requested. Therefore the port that the object was requested will be stored into the table.
- If the web server does not include the port attribute in the cookie, then the web proxy will store "Any" port into the table.
- If it is the version 0 cookie, then the web proxy will store "Any" port into the table.

The web proxy will use the information in the table to rewrite back the values of the name attributes in the cookies (sent by the browsers) back to the original values, as shown in Figure 5.

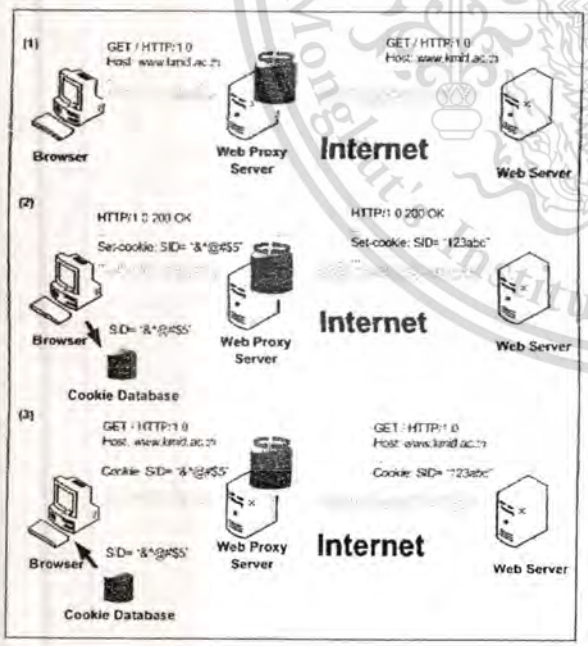

Figure 5. How the Dynamic Rewriting Cookies technique work

If the web proxy receives the request message the cookies, and also the domain, path and port requesting URL of that request message match an entry in the table, then that entry will be deleted from the table prior to the web proxy forwards that request message to the web server.

And finally if the value of the name attribute in the cookie sent by the web server is changed from that exists in the table, then the web proxy will update the table accordingly.

IV. Evaluation

We wrote a simple web proxy and implemented our proposed approach using JAVA programming language. We ran our web proxy on the Windows 2008. The current version of our code does not support the HTTPs.

We conducted experiments to evaluate a compatibility of our approach on five popular web browsers: Google Chrome v6, Firefox v3, IE v8, Opera v10 and Safari v4. We wrote the server's code using Perl and ran it on Apache 2. We then used three scenarios to evaluate our approach as shown below.

Scenario 1 – evaluated our approach with the version 0 cookies using all five browsers on the following test cases.

- Set-Cookie: SID= abcdefg1
- Set-Cookie: SID= abcdefg2 ;domain= .test0.com
- Set-Cookie: SID=abcdefg3;domain=.test0.com;path= /lab1
- Set-Cookie: SID=abcdefg4;domain=.test0.com; path= /lab2
- Set-Cookie: SID=abcdefg5;domain= .test0.com; path=/ lab1

Scenario 2 – evaluated our approach with the version 1 cookies using the Opera browser on the following test cases.

- Set-Cookie2: SID="abcdefg6";version= "1";
- Set-Cookie2: SID= "abcdefg7";version= "1"; domain= ".test1.com"
- Set-Cookie2: SID= "abcdefg8"; version= "1"; domain= ".test1.com";path= "/lab1"
- Set-Cookie2: SID="abcdefg9"; version= "1"; domain= ".test1.com";path= "/lab2"
- Set-Cookie2: SID= "abcdefg10"; version= "1"; domain= ".test1.com";path= "/lab1";port
- Set-Cookie2: SID= "abcdefg11"; version="1"; domain= ".test1.com";path="/lab2";port= "80,8000"
- Set-Cookie2: SID= "abcdefg12";version= "1"; domain= ".test1.com";path= "/lab1"

Scenario 3 – evaluated our approach with real websites on the internet. Currently we have experimented with 120 websites.

The results showed that our approach worked well with all three scenarios. We saw in the experiments that the browsers stored and returned the randomized values properly and the web server accepted the cookies sent from our web proxy.

V. Discussion

To implement our proposed approach in the web proxy and deploy it in the live environment, we have to consider at least the following three challenges:

- Compatibility - our approach changes the values of the cookies in HTTP header, so we have to make sure that this will not break the HTTP and be able to work well and transparently with all websites on the internet. Although almost all websites on the internet use only the version 0 cookies but our approach follows both version 0 and version 1 cookie specifications in order to be sure that it is able to manage properly all cookies sent by all websites. We conducted the experiments as shown in the scenario 1 and scenario 2 of the previous section to prove that our approach is able to handle both the version 0 and version 1 cookies, and also verify in the scenario 3 that it does not have any side effects on the HTTP protocol and be able to work well and transparently with the real websites on the internet.
- Performance - deploying the web proxy into the network definitely adds more latency and increases the response time. However, the web proxy is usually built in with a caching capability which is able to cache web contents and serve the cached contents locally to the users [11]. So with the web proxy in place, instead of degrading the system performance, it helps to leverage overall performance, improve user experience and also reduce internet bandwidth usage [11]. Hardware platforms have been developing dramatically over the past few years [12]. With the advanced hardware platform itself, the latency on the web proxy will be reduced accordingly.
- Single point of failure - as our web proxy must rewrite the cookies, and keep the original values of the cookies in its database. So when it fails, those original (and valid) values will be gone. Fortunately, there are several technologies in place which are able to detect and bypass the web proxy once it fails such as PAC file, WCCP Protocol, Policy Based Routing (PBR) and so on. With one of those technologies, even the web proxy fails, the clients are still able to reach the web servers. While invalid cookies in hand, the users must be re-authenticated by the web servers. After successful authentication, the authenticated users will be able to access web services as usual without the web proxy involved.

Although deploying the web proxy has some challenges as mentioned above, the web proxy still has huge advantages [8]-[10] such as Web Content Caching, Network Address Translation (NAT), Authentication and authorization, Content filtering, URL filtering, Malware prevention, Data leak protection , Logging /Reporting and so on which organizations can gain benefits from those advantages along approach.

VI. Conclusions

This paper has presented the Dynamic Rewriting Cookie technique which aims to disarm the attackers from impersonating the users. This technique was implemented as a part of our web proxy and then was evaluated with three scenarios. The results showed that our new technique worked well with both versions 0 and version 1 cookies, and has showed no errors with any real world websites.

Currently we are doing more researches on how to program our web proxy to intercept the HTTPs. Nearly all e-commerce web sites today send the cookies over the SSL connections. Based on our current study and current evaluation, we believe that our technique will also work well with the HTTPs. In order to prove that, our web proxy must be able to intercept the SSL connections which this is a big part of our future work.

Acknowledgment

The authors would like to thank Rene Spallek for providing a review and valuable comments.

References

[1] D. Gourley, B. Totty, M. Sayer,S. Reddy, and A. Aggarwal, *HTTP The Definitive Guide*, 1st ed., O'Reilly Media, US, 2002.

[2] D. Kristol, "HTTP State Management Mechanism,", in *Internet Society*,2000. Available: http://www.ietf.org/rfc/rfc2965.txt

[3] "Cross Site Scripting Techniques and mitigation,", GovCertUK, revision 1.0,October 2009. Available: www.govcertuk.gov.uk

[4] J. Garcia-Alfaro and G. Navarro-Arribas, "Prevention of Cross-Site Scripting Attacks on Current Web Applications,". Available: http://hacks-galore.org/guille/pubs/is-otm-07.pdf

[5] S. Saha, "Consideration Points: Detecting Cross-Site Scripting," *(IJCSIS) International Journal of Computer Science and Information Security*,Vol. 4, No. 1 & 2, 2009.

[6] A. Klein, "DOM Based Cross Site Scripting or XSS of the Third Kind,",July2005.Available:http://www.webappsec.org/projects/articles/071105.shtml

[7] A. Wiegenstein, M. Schumacher, X. Jia, and F. Weidemann "Whitepaper: The Cross Site Scripting Threat,", 2007. Available: http://www.virtualforge.de

[8] "White paper: How to Gain Visibility and Control of Encrypted SSL Web Sessions,". Available: http://www.bluecoat.com

[9] "Technology Overview: Cisco IronPort Web Usage Controls,". Available: http://www.ironport.com

[10] "Solution Brief: McAfee Web Gateway,". Available: http://www.mcafee.com

[11] S. Patarin and M. Makpangou, "On-line Measurement of Web Proxy Cache Efficiency,". Available : http://hal.inria.fr/inria-00071804/PDF/RR-4782.pdf

[12] "White paper: Platform 2015:Intel® Processor and Platform Evolution for the Next Decade,". Available : http://epic.hpi.uni-potsdam.de/pub/Home/TrendsAndConceptsII2010/HW_Trends_borkar_2015.pdf

[13] S. Shah, *WEB 2.0 SECURITY: Defending Ajax, RIA, and SOA*, Charles River Media – Thomson, US, 2008.

[14] UW Staff Web server [Online]. Available: http://staff.washington.edu/fmf/2009/06/19/setting-cookies/

[15] Wikipedia website [Online]. Available: http://en.wikipedia.org/wiki/Talk%3AHTTP_cookie

Estimated Transfer Time of Web Contents for Based Scheduling

Rattipong Putthacharoen
Somsak Mitatha
Pratheep Bunyatnoparat
Department of Computer Engineering, Faculty of Engineering,
King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand
s8060056@kmitl.ac.th, kmsomsak@kmitl.ac.th, kbprathe@kmitl.ac.th

Abstract - **The size-based scheduling policies such as the shortest-remaining-processing-time (SRPT) and the preemptive-shortest-job-first (PSJF) are long known that they reduce the mean response time for serving static web contents (e.g. images and files) to clients and improve a quality of web services but they are not widely used in practice. The reason is that job sizes are not known in advance so the size-based scheduling policies cannot be applied. In this paper we propose an algorithm to estimate the transfer time of the static web content which we then let the estimated transfer time be the job size for the size-based scheduling polices. With our algorithm in place, the size-based scheduling polices can be then applied in practice.**

I. Introduction

Improving a quality of web services on the Internet has been a big challenge to researchers because web users access to web servers from anywhere in the world which there are different link sizes, different latencies and different congestion. A number of mechanisms were proposed to improve the mean response time of the web servers in order to leverage the quality of the web services. One of the most important mechanisms to improve the mean response time is a scheduling. The scheduling determines the order in which packets from different flows are sent [1].

The packet scheduling in network devices (e.g. router, switch and Web proxy) has been an active area for the researchers over the past decade [2]. It has been long known [1] that the size-based scheduling policies such as the shortest-remaining-processing-time (SRPT) and the preemptive-shortest-job-first (PSJF) [2] are the optimal scheduling with respect to minimizing the mean response time but they are not widely used in practice. The reason why they are not widely used is that job sizes are not known in advance so the size-based scheduling policies cannot be applied. However, for web applications this may not be the case, in this paper we propose a simple algorithm to estimate the total time of transferring a given static web content between a client and the web server which we call it then the estimated transfer time. We later use the estimated transfer time as the job size for the size-based scheduling policies. The goal of this paper is to propose the simple and effective algorithm, so then the size-based scheduling policies can be widely used in practice.

The remainder of this paper is organized as follows. Section II discusses topics which are related to a proposed algorithm: Size-based Scheduling and Sliding Window Protocol. Section III presents the proposed algorithm. We then show evaluation results in section IV, and discuss about the results in section V. Finally, we conclude and also introduce future works in Section VI.

II. Background

A. *Size-based Scheduling*

The size-based scheduling policies [4] use the job sizes to determine which job to serve next. These policies generally favor short jobs rather than large jobs.

- Shortest-Remaining-Processing-Time (SRPT). This is a preemptive scheduling policy which always serves the job that has the currently smallest remaining time. If the new job has shorter processing time than the job in service, then it preempts the job in service. SRPT is known to minimize the mean response time.
- Preemptive-Shortest-Job-First (PSJF). This is very similar to SRPT. It is the preemptive scheduling policy which favors the smallest original size rather than the smallest remaining time. It can be useful when the remaining time is not known.
- Shortest-Job-First (SJF). This is a non-preemptive version of PSJF. It always chooses the shortest job (shortest original size) to serve first but if the new job has the shorter original size; it cannot preempt the job in service.

B. *Sliding Window Protocol*

TCP uses window-based [5][8] to control the number of packets sent between the client and the server. This means that the client only accepts a certain amount of packets sent by the server, the server must not send more than the full window without receiving acknowledgements.

The client and the server each have a window size w_c and w_s respectively, $w_c \geq w_s$. They each also have a current sequence number n_c and n_s. The n_s is the next packet to be sent, n_c is the first packet not yet received. All packets below n_c have been received, when the client receives packets, it sends the acknowledgment with the new n_c. The server keeps track of the highest acknowledgment it has received n_a. All packets up to, but not including n_a have been received.

If the server has data to send, it may send up to w_s packets ahead of the latest acknowledgment n_a. It may send the packet number n_s as long as $n_s < n_a+w_s$.

If the client receives the packet numbered x, the client checks to see if it falls in the receive window, $n_c \leq x < n_s+w_c$. If it falls within the window, the client accepts it, otherwise the client discards and does not modify n_c.

III. ALGORITHM

As mentioned earlier, we let the estimated transfer time of the static web content be the job size for the size-based scheduling policies. Therefore, instead of estimating the job size, we propose the algorithm to estimate the transfer time of the static web content as follows.

$$\text{ECTT} = \frac{\text{CL}}{w_c} \times \text{FWTT} \qquad (1)$$

Where ECTT is the estimated transfer time of the static web content, CL is a content-length, w_c is an original window size of the client which it comes with a GET request (our algorithm uses a fixed window size), FWTT is the time from the GET request arrives until $n_a \geq n_{fa}+w_c$. The n_{fa} is the acknowledgement number that it also comes together with the GET request which we call it "first acknowledgement", see Fig 1.

E.g. ECTT = (200,000 byte / 65,535 byte)*7.70 sec = 23.50 sec.

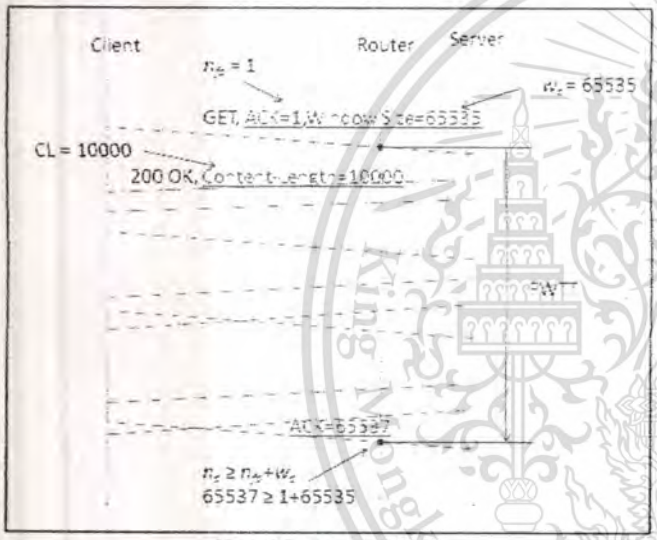

Fig 1. CL, w_c, and FWTT

The content-length (CL) field [3][5] in the response HTTP message indicates the size of the web content in bytes that response to the GET method of the request HTTP message.

If the web content is small, CL ≤ 65,535, then we use the following algorithm to estimate the transfer time of the small web content. The value "65,535" refers to the maximum window size [7], the TCP window size is limited to between 2 and 65,535 bytes.

$$\text{ECTT} = \frac{\text{CL}}{sw_c} \times \text{SWTT} \qquad (2)$$

Where SWTT is the time from the GET request arrives until receiving a second acknowledgement n_{sa}, $n_{sa} > n_{fa}$, see Fig 2. The sw_c is a sub-window size ($n_{sa} - n_{fa}$) which it is the number of bytes sent during SWTT.

E.g. ECTT = (10,000 byte /2,920 byte)*0.6 sec = 2.054 sec.

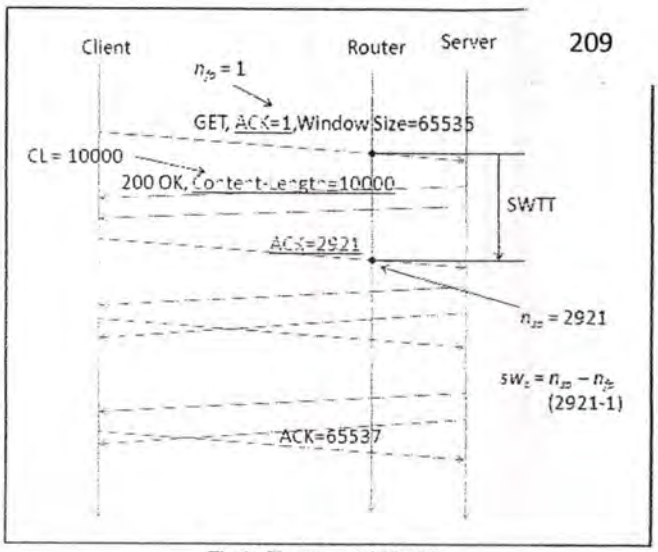

Fig 2. CL, sw_c, and SWTT

If we combine (1) and (2) then:

$$\text{ECTT} = \begin{cases} \frac{\text{CL}}{sw_c} \times \text{SWTT}, & \text{CL} \leq 65{,}535 \\ \frac{\text{CL}}{w_c} \times \text{FWTT}, & \text{CL} > 65{,}535 \end{cases} \qquad (3)$$

IV. EVALUATION RESULTS

The evaluation aims to prove that an actual transfer time (ATT) of the static web content is close to our ECTT. We did a live simulation to evaluate our proposed algorithm as shown in Fig 3. We stored several files into the web server, they each had different sizes ranged from 10Kbyte to 10 Mbyte. The web server was Apache2.2, the Apache2.2 was running on Windows XP SP2, CPU T2600@2.16 GHz 994 MHz, 2 GB of RAM. The client was Window XP SP3, CPU m52@2.40 GHz 1.17 GHz, 3 GB of RAM. We wrote a bat file continuously to generate the GET requests from the client to the web server using Wget command. We used Ethereal software to sniff all packets that were sent back and forth between the client and the web server. The round trip time (RTT) of WAN simulator was set to 200 msec in the first experiment and 600 msec in the second experiment respectively. A link size was 2Mbps.

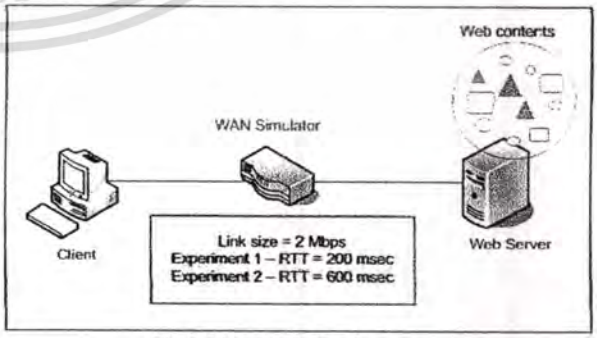

Fig 3. Live simulation diagram

After both experiments, we compare the ECTT and ATT as shown in Fig. 4-9. We have seen that if the content-lengths fall in between 100Kbyte and 10Mbyte (100KB ≤ CL ≤ 10MB) as shown in Fig 4-7 and between 10Kbyte and 30 Kbyte (10KB ≤ CL ≤ 30KB) as shown in Fig 8-9, then ECTT is close to the ATT. Both ECTT and ATT are going in the same direction.

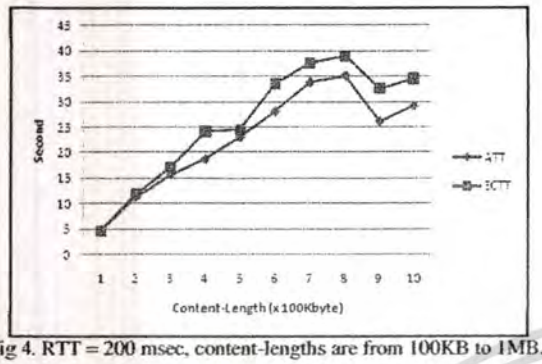

Fig 4. RTT = 200 msec, content-lengths are from 100KB to 1MB.

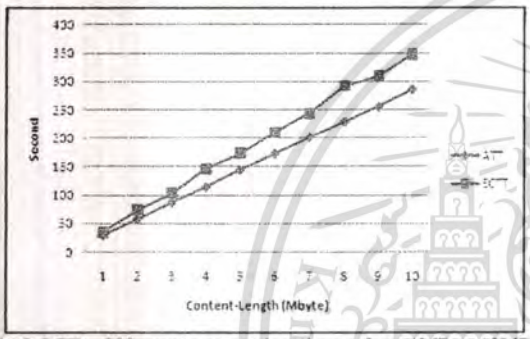

Fig 5. RTT = 200 msec, content-lengths are from 1MB to 10MB.

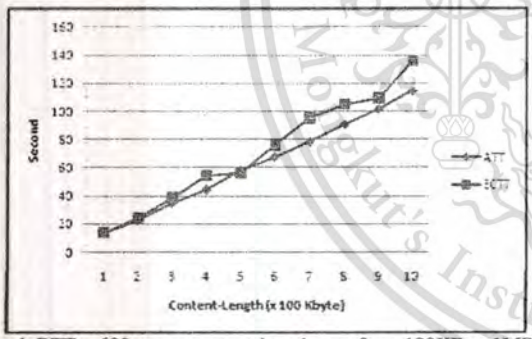

Fig 6. RTT = 600 msec, content-lengths are from 100KB to 1MB.

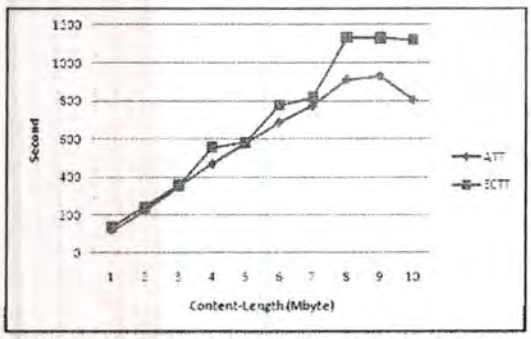

Fig 7. RTT = 600 msec , content-lengths are from 1MB to 10MB.

Even though the ECTT and the ATT are quite the content-lengths are in between 40Kbyte a (40KB ≤ CL ≤ 60KB) as shown in Fig 8-9 (A gap between the ECTT and ATT are longer), but both ECTT and ATT are going in the same direction, so the algorithm is still applicable.

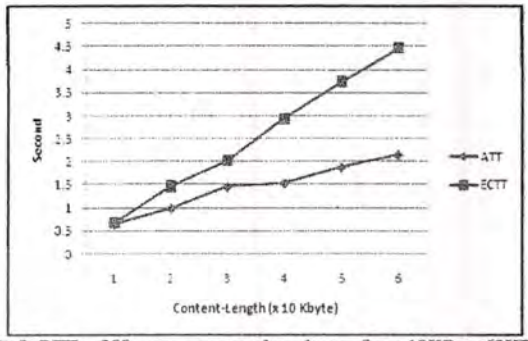

Fig 8. RTT = 200 msec , content-lengths are from 10KB to 60KB.

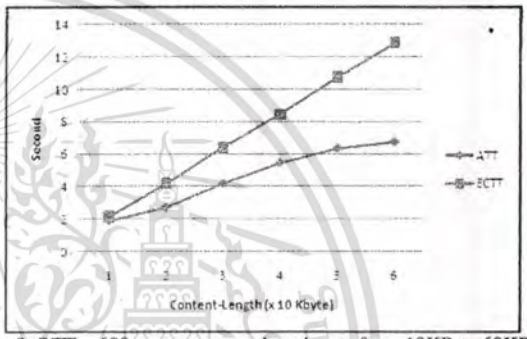

Fig 9. RTT = 600 msec , content-lengths are from 10KB to 60KB.

V. DISCUSSION

The gap between the ECTT and ATT may be possibly affected by the load of the server, the window size, the round trip time, and the congestion of the link at any time. In order to minimize the gap between the ECTT and ATT, we revise (3) as follows:

$$ECTT = \begin{cases} \alpha \frac{CL}{SW_c} \times SWTT, & CL \leq 65{,}535 \\ \beta \frac{CL}{W_c} \times FWTT, & CL > 65{,}535 \end{cases} \quad (4)$$

Let $\propto$ and β be fixed values, $\propto = 0.6$ and $\beta = 0.85$. The results show then in Fig 10-15.

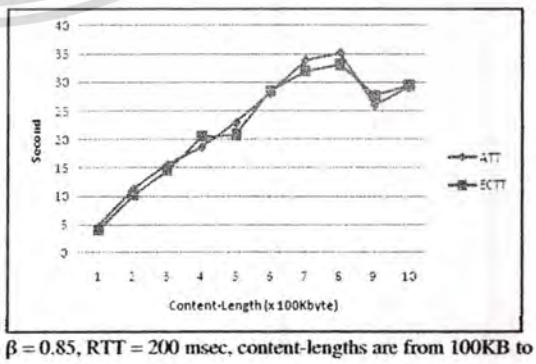

Fig 10. $\beta = 0.85$, RTT = 200 msec, content-lengths are from 100KB to 1MB.

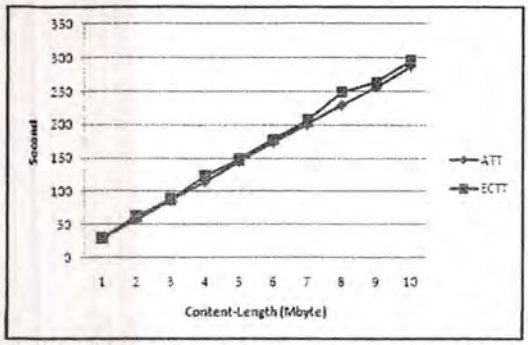

Fig 11. $\beta = 0.85$, RTT = 200 msec, content-lengths are from 1MB to 10MB.

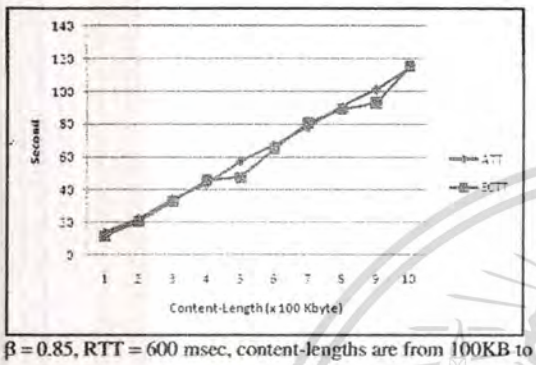

Fig 12. $\beta = 0.85$, RTT = 600 msec, content-lengths are from 100KB to 1MB.

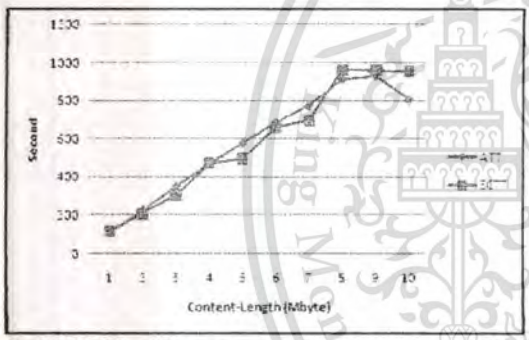

Fig 13. $\beta = 0.85$, RTT = 600 msec , content-lengths are from 1MB to 10MB.

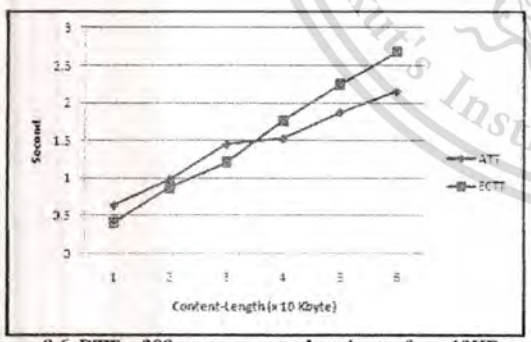

Fig 14. $\alpha = 0.6$, RTT = 200 msec , content-lengths are from 10KB to 60KB.

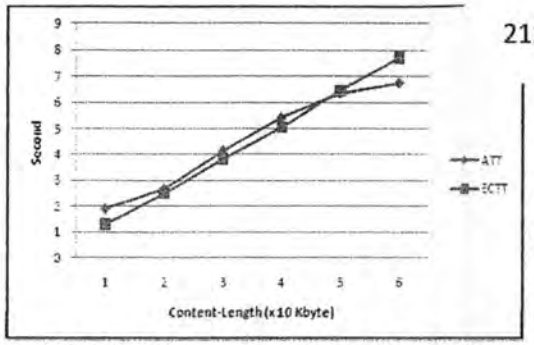

Fig 15. $\alpha = 0.6$, RTT = 600 msec , content-lengths are from 10KB to 60KB.

As shown in Fig 10-15 after we have added α and β to (4), then the ECTT is very close to ATT for all content-lengths.

VI. Conclusion

We have presented our algorithm which it aims to estimate the transfer time of the static web content. The estimated transfer time then will be used as the job size for the size-based scheduling polices. With our algorithm in place, the size-based scheduling policies will be able to calculate simply the estimated transfer time in advance, so then they can be widely used and simply implemented in practice. We evaluated our algorithm with various content-lengths ranged from 10Kbyte to 10Mbyte. The results have shown that the estimated transfer time of the static web content using our algorithm (4) is very close to the actual transfer time.

In the future works, first we will implement at least one of the size-based scheduling policies with our algorithm in order to prove that the algorithm can be effectively applied in practice, and can really improve the quality of the web services. Second instead of using the fixed α and β, the dynamic algorithm will be proposed to calculate both α and β. Finally the dynamic web contents will also be covered in the near future.

References

[1] N. Bansal and M. Harchol-Balter, "Analysis of SRPT Scheduling: Investigating Unfairness,". Available: https://www.aladdin.cs.cmu.edu/papers/pdfs/y2001/sigmetrics01.pdf

[2] I. A. Rai, E. W. Biersack, and G. Urvoy-Keller, "Size-based Scheduling to Improve the Performance of Short TCP Flows," *IEEE Network*, Vol. 19, Jan. 2005.

[3] Hypertext Transfer Protocol -- HTTP/1.1 [Online]. Available: http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

[4] M. Harchol-Balter, "Queueing Disciplines,", *Research Showcase, Carnegie Mellon University*, 2009.

[5] Wikipedia website [Online]. Available: http://en.wikipedia.org/wiki/Sliding_window_protocol

[6] D. Gourley, B. Totty, M. Sayer,S. Reddy, and A. Aggarwal, ***HTTP The Definitive Guide***, **1st ed., O'Reilly Media, US, 2002.**

[7] **Wikipedia website [Online]. Available: http://en.wikipedia.org/wiki/Transmission_Control_Protocol**

[8] M. Welzl, and L. Franzens, *Network Congestion Control Managing Internet Traffic*, John Wiley & Sons, UK, 2005

BIOGRAPHY

Name : Mr. Rattipong Putthacharoen
Date of Birth: 10 December 1977
Born: Bangkok, Thailand.
Current Address: 8 Chokchai 4 Soi 14 Yak 3-6, Ladphrao, Bangkok 10230.
E-mail: rattipong@yahoo.com, rattipong.p@hotmail.com

Qualification

Education

- Bachelor degree of Computer engineering, King Mongkut's Institute of Technology Ladkrabang, 2001.
- Master degree of Computer engineering, King Mongkut's Institute of Technology Ladkrabang, 2005.

Position and Office

Senior System Engineer, Bluecoat System Thailand Inc., 571 Sukhumvit Soi 31,10th Floor, RSU Tower, Klongtoey-Nua, Wattana, Bangkok 10110,Thailand

Skilled Works

- Computer Security
- Cryptography
- Computer Network
- Data Communication
- Fiber optics
- Nonlinear optics
- Chaos-based Communication