東海大学紀要情報通信学部
vol.6,No2,2013,pp.15-21

Paper

Cryptography using dark-bright soliton to generate keys by orthogonal dark-bright soliton pair

by

Xaythavy LOUANGVILAY[*1], Somsak MITATHA [*2], Masahiro YOSHIDA[*3], Noriyuki KOMINE[*4] and Preecha P. YUPAPIN[*5]

(received on September 21, 2013 & accepted on February 6, 2014)

Abstract

A method of optical cryptography by using soliton as dark-bright conversion control within a modified add/drop optical filter is proposed. In principle, the coincidence (orthogonal) dark-bright soliton pair has shown promising behaviors, especially when they propagate into the $\pi/2$ phase shifter, i.e. beamsplitter, $\pi/2$ phase shift between bright and dark solitons is occurred and separated. Such behaviors can be used to form the orthogonal light modes (solitons), which can be useful for application of cryptography, where in this case the long distance cryptography can be easily managed. In this work we have derived and presented a concept of multi-orthogonal solitons generated by using dark-bright soliton pulses within the modified add/drop optical filter, which is known as a PANDA ring resonator. A pair of optical keys is randomly generated and transmitted into the transmission line, where finally the corrected keys between Alice (sender) and Bob (receiver) can be retrieved. By using the dark-bright soliton conversion control, the obtained output of the dynamic states can be used to randomly form the multi-orthogonal soliton pairs, which can be available for computer and communication security applications, especially for long distance link.

Keywords: *soliton cryptography; optical cryptography; optical security; PANDA ring.*

1. Introduction

Soliton communication has been a system for long-distance optical communication links, where the required minimum repeater is the advantage has become the key advantage of the system performance. However, in practice, the problem of soliton-soliton interaction, soliton collision, and dispersion management are required to solve.[1-3] Generally, there are two types of soliton known as bright and dark solitons,[4] where the soliton behaviors and applications are well analyzed and described by Agarwal[5]. In principle, the detection of dark soliton is extremely difficult. The dark soliton behavior has become the promising application when the transmission dark soliton can be converted after passing through into the specific add/drop filter[6], which means that the transmission signals can be transmitted in the form of dark soliton, which is hard to detect, whereas the specific end user that connects to the link via the specific add/drop filter can obtain the signals Although, the dark soliton applications have been widely investigated in various applications[7-10], the searching for further applications remains. The use of soliton, i.e., bright soliton in long-distance communication links has been in operation for nearly two decades. However, some questions still need to be answered in the area of communication safety, whereas the use of a dark soliton pulse within a microring resonator for communication security has been studied. The investigation of dark soliton behaviors[11] has been reported and one has shown the interesting result that the dark soliton can be stabilized and converted into bright soliton and finally

*1,2 King Mongkut's Institute of Technology Ladkrabang Hybrid Computing Research Laboratory Faculty of Engineering Bangkok 10520, Thailand

*3,4 Tokai University School of Information and Telecommunication Engineering Department of Embedded Engineering, Tokyo, 108-8619, Japan

*5 King Mongkut's Institute of Technology Ladkrabang Nanoscale Science and Engineering Research Alliance (N'SERA) Faculty of Science Bangkok 10520, Thailand

detected. This means that we can use the dark soliton to perform the communication transmission for security, whereas the required information can be retrieved by the dark-bright soliton conversion, in which the use of optical microcavities[12-13] or micro ring resonators[14-20] have shown the promising applications for dark soliton, where a PANDA ring resonator is a new model of them, which has been successfully used to investigate the dynamic behavior of dark-bright soliton collision. In this paper we proposed a new concept of optical cryptography by using dark-bright soliton conversion control within a modified add/drop filter (a PANDA ring), which is useful for cryptographic application. The simulation results obtained have shown that the proposed system can be used to form the security keys, where the secret keys can be retrieved and achieved, which is useful for computer and communication applications, especially, where in addition the high capacity and long distance link can be realized by using the soliton communication.

Information technology(IT) has become the main key that can be used to develop and change the world economy; therefore the finding of new techniques for more capacity and available network is remaining. One of them is the use of high performance network that is able to offer both high security and larger bandwidth. There are many techniques have been reported,[21-24] where they have shown that the user demand can be improved. To date, optical communication has been investigated in almost every layer of information technology infrastructure: continent-to-continent, city-to-city, server-to-server, computer-to-computer, board-to-board, chip-to-chip, and finally intrachip, where all optical devices have been used as the integrated components for advanced optical technique in a lot of applications, especially in optical communication, optical sensor, and signal processing, etc. In the world information technology,communication security segment has been recognized as a promising tool for information necessitates the security and privacy requirements due to the large demand of the world networks, where there have been widely used in many applications; for instance, sensors,[25] computing[26], communication,[27] and signal processing[28]. One of them used an optical device for communication security,[29-32] which can be fabricated and made the integrated components for advanced optical technology in applications.

2. Operating Principle

In operation, the input and control fields at the input and add ports are formed by the dark and bright optical solitons and described by Eqs. (1) and (2), respectively. A dark-bright soliton conversion system using a ring resonator optical channel dropping filter is composed with two sets of coupled waveguides, as shown in Fig. 1. The relative phase of the two output light signals after coupling into the optical coupler is $\pi/2$. This means that the signals coupled into the drop and through ports have acquired a phase of π with respect to the input port signal. In application, when the coupling

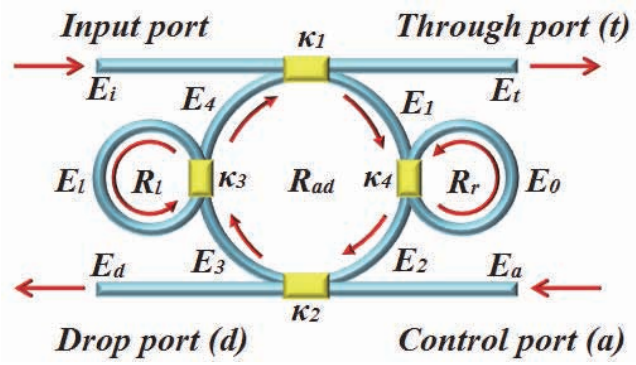


Fig. 1 A schematic diagram of a proposed PANDA ring resonator.

coefficients are formed appropriately, the optical field coupled into the through port with the resonant condition would completely extinguish the resonant wavelength, and all the power would be coupled into the drop port.

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

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

Here A_0 and z are the optical field amplitude and propagation distance, respectively. $T = t - \beta_1 z$, where β_1 and β_2 are the coefficients of the linear and second-order terms of Taylor expansion of the propagation constant. $L_D = T_0^2/|\beta_2|$ is the dispersion length of the soliton pulse. T_0 in equation is a soliton pulse propagation time of initial input (or soliton pulse width), where t is the soliton phase shift time, and the frequency shift of the soliton is ω_0.

$$E_1 = \tau_1 E_4 - jE_i \quad (3)$$
$$E_2 = \exp(j\omega T/2)\exp(-\alpha L/4)E_1 \quad (4)$$
$$E_3 = \tau_2 E_2 - j\kappa_2 E_a \quad (5)$$
$$E_4 = \exp(j\omega T/2)\exp(-\alpha L/4)E_3 \quad (6)$$
$$E_t = \tau_1 E_i - j\kappa_1 E_4 \quad (7)$$
$$E_d = \tau_2 E_a - j\kappa_2 E_2 \quad (8)$$

Here E_1, E_2, E_3, E_4 are the fields in the ring at points 1 to 4, E_a is the add (control) field, E_d is the drop field, E_i is the input field, E_t is the through field, κ_1 is the field coupling coefficient between the input bus and ring, κ_2 is the field coupling coefficient between the ring and output bus, T is the time taken for one round trip (round trip time), L is the

circumference of the ring, and α is the power loss in the ring per unit length. We assume that this is the lossless coupling, i.e., $\tau_{1,2} = \sqrt{1-\kappa_{1,2}^2}$, $T = Ln_{eff}/c$.

The output intensities at the drop and through ports are given by

$$\left|E_d\right|^2 = \left|E_i \frac{-\kappa_1\kappa_2 A_{1/2}\Phi_{1/2}}{1-\tau_1\tau_2 A\Phi} + E_a \frac{\tau_2 - \tau_1 A\Phi}{1-\tau_1\tau_2 A\Phi}\right|^2 \quad (9)$$

$$\left|E_t\right|^2 = E_i \frac{\tau_2 - \tau_1 A\Phi}{1-\tau_1\tau_2 A\Phi} + E_a \frac{-\kappa_1\kappa_2 A_{1/2}\Phi_{1/2}}{1-\tau_1\tau_2 A\Phi} \quad (10)$$

Here A is the effective mode core area of device and Φ is nonlinear phase shift of device

To form the broad soliton spectrum output, two nonlinear ring resonators are introduced as shown in Fig. 1. We have γ the fractional coupler-intensity loss, $k_n = 2\pi/\lambda$ the wave propagation number. λ the input wavelength light field. The circulated round-trip light fields at the point 1(after through κ_4) and 2 (before through κ_4) of the right ring radii, E_{r1} and E_{r2}, are given in Eqs. (11) and (12), respectively.

$$E_{r1} = (j\sqrt{1-\gamma}\sqrt{\kappa_4}E_1)\left[1-\sqrt{1-\gamma}\sqrt{1-\kappa_4}e^{-L_1(2^{-1}\alpha+jk_n)}\right]^{-1} \quad (11)$$

$$E_{r2} = \left[j\sqrt{1-\gamma}\sqrt{\kappa_4}E_1 e^{-L_1(2^{-1}\alpha+jk_n}\right] \times\left[1-\sqrt{1-\gamma}\sqrt{1-\kappa_4}e^{-L_1(2^{-1}\alpha+jk_n)}\right]^{-1} \quad (12)$$

Thus the output circulated light field, E0, for the right ring is given by

$$E_0 = E_1\left[\sqrt{(1-\kappa_4)(1-\gamma)} - (1-\gamma)e^{-L_1(2^{-1}\alpha+jk_n)}\right] \times\left[1-\sqrt{(1-\kappa_4)(1-\gamma)}e^{-L_1(2^{-1}\alpha+jk_n)}\right]^{-1} \quad (13)$$

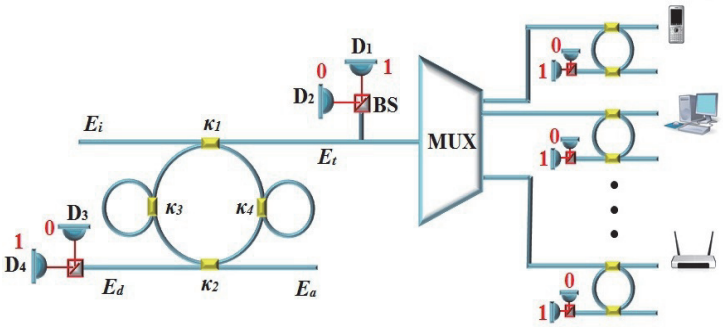


Fig. 2. Schematic diagram of dark-bright soliton generation, where D_n: photodetectors, κ_n: coupling coefficients, E_n: electric field, BS: Beamsplitter.

Similarly, the output circulated light field, E0L, for the left ring at the left side of the add/drop optical multiplexing system is given by

$$E_{0L} = E_3\left\{\left[\sqrt{(1-\kappa_3)(1-\gamma)} - (1-\gamma_3)e^{-L_1(2^{-1}\alpha+jk_n)}\right] \times\left[1-\sqrt{(1-\kappa_3)(1-\gamma)}e^{-L_1(2^{-1}\alpha+jk_n)}\right]^{-1}\right\} \quad (14)$$

3. Results

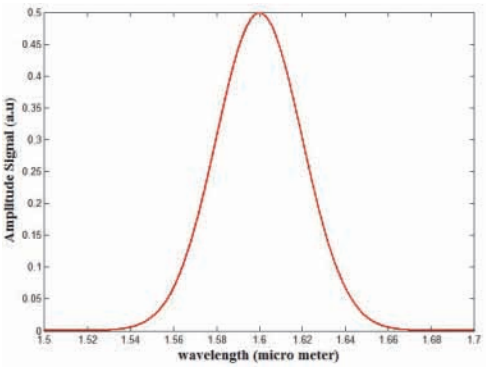
A schematic diagram of dark-bright soliton generation consists of two parts such as transmission and receiver parts as shown in Fig. 2.

When light propagates within the nonlinear material (medium), the refractive index n of light within the medium is given by

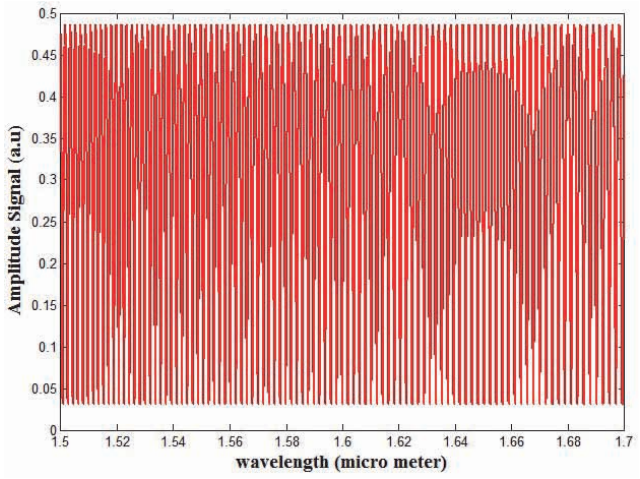
$$n = n_0 + n_2 I = n_0 + \frac{n_2}{A}P \quad (15)$$

Here n_0 and n_2 are the linear and nonlinear refractive indexes, respectively. I and P are the optical intensity and power.

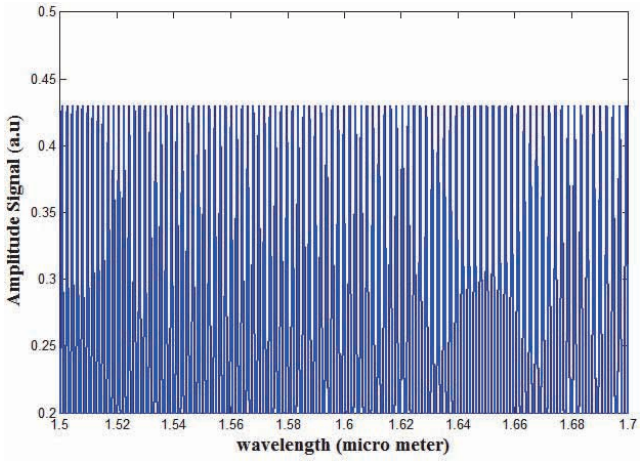
The basic proposed PANDA ring resonator parameters are fixed to be $n_0 = 3.34$ (InGaAsP/InP), and $\alpha = 0.2 dBmm^{-1}$, the coupler intensity loss is $\gamma = 0.1$. The bright soliton input pulse with center wavelength of 1.4 μm, and an amplitude signal of 0.5 W is input into the system. The coupling coefficient of the microring resonator is varied from 0.1 to 0.98, the nonlinear refractive index is $n_2 = 2.2\times10^{-17}$. The other used parameters of the first add/drop filter (optical multiplexer, PANDA ring resonator) are fixed to be $\kappa_1 = 0.15$, $\kappa_2 = 0.35$, $\kappa_3 = 0.7$, and $\kappa_4 = 0.2$, respectively. The ring radii are $R_{ad} = 15\mu m$, and $R_r = R_l = 5\mu m^2$ 5. A_{eff} are 0.50, 0.25 and 0.25 μm^2, respectively. Moreover, the selected parameters have been chosen closely to the practical device parameters, in which the optical key suppressed and recovery system should be possible to be fabricated.



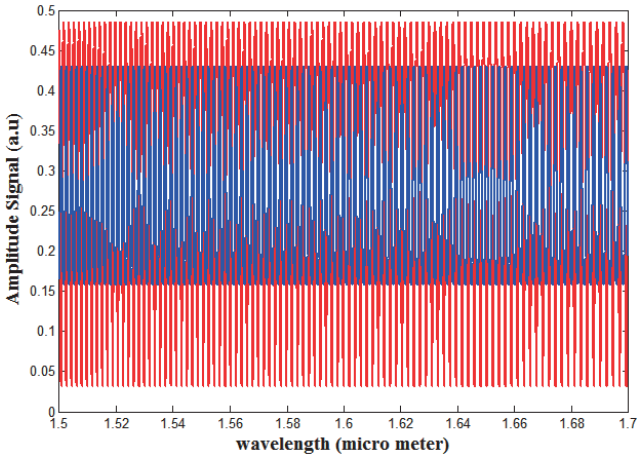
(a)



(b)



(c)



(d)

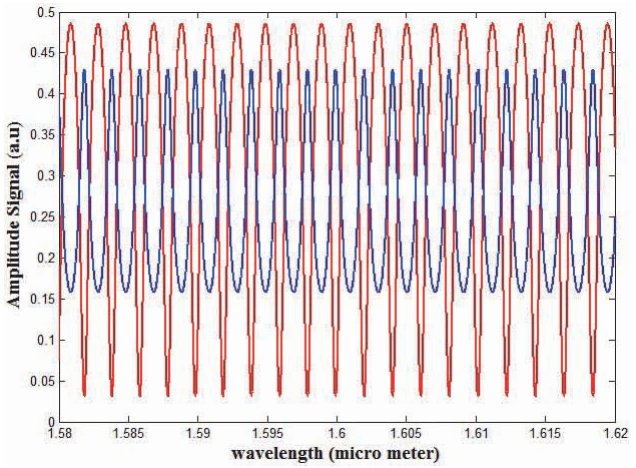
Fig. 3. A schematic diagram of dark-bright soliton generation, where (a) is the input pulse (bright soliton), (b) is the Through port (Et1) signal, (c) is the Drop port signal, and (d) is the comparison between Though port and Drop port signals.

The key suppressed and recovery system should be possible to be fabricated.

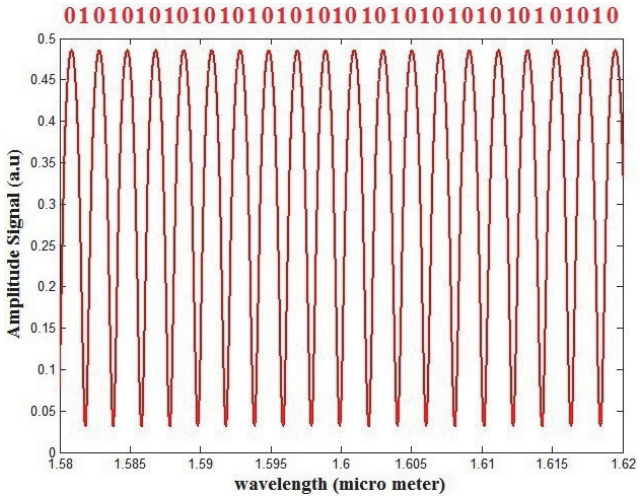
The simulation results of generating signals in a PANDA ring resonator are as shown in Fig. 3, which is used in the transmission part, where (a) is the input pulse (bright soliton), (b) is the through port (E_{t1}) signal, (c) is the drop port signal, and (d) is the comparison between though port and drop port signals. Here (b) and (c) show the amplitude at the through and drop ports for signal recovery, respectively. The referencing multisoliton pairs are generated as shown in Fig. 4(a)–4(c), in which the multisoliton pairs detected by D_1 and D_2 are "1010101010101" for D_1 and "bbbbbb" for D_2. Similarly, D_1 and D_2 at the through ports are detected and the multisoliton pairs seen, where the D_3 and D_4 codes such as "1010101010101" and "bbbbbb" are obtained as shown in Fig. 2, respectively. At the receiver part, the

add/drop filter parameters are fixed to be $n_0 = 3.34$ (InGaAsP/InP), and $\alpha = 0.2 dBmm^{-1}$, the coupler intensity loss is $\gamma = 0.1$. The other used parameters of the first add/drop filter is fixed to be $\kappa_5 = \kappa_6 = 0.13$. The coupling coefficient of the microring resonator is varied from 0.1 to 0.98 and the nonlinear refractive index is $n_2 = 2.2\text{X}10^{-17}$.

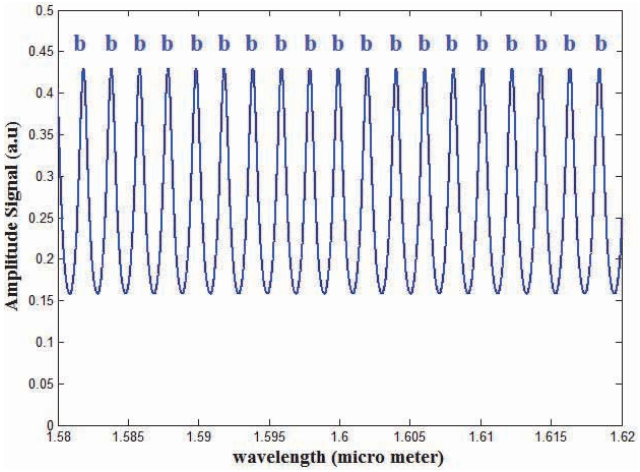
Generally, when a bright or dark soliton is propagated into a $\pi/2$ phase shifter device (beamsplitter or an optical coupler), the dark-bright soliton conversion (pair) can be randomly generated and detected. The multi-dark-bright soliton conversion is also seen when the input soliton is chopped to be many soliton pulses by the nonlinear effects, where in this case the nonlinear devices are formed by the two small ring resonators of the center ring (add/drop filter), which is formed a PANDA ring. In application, the signal is sent into the input port by the transmitter as shown in Fig. 3. Where (a) is the input pulse (bright soliton), (d) is the comparison between Though port and Drop port signals which are used as key and data for encryption. in Fig. 3(b) is the Through port (Et) signal, 3(c) is the Drop port signal.Then both of them are sent into the input port at the receiver part, where the signal is decrypted to separate key and data. The decryption key is used for the ciphertext decryption, which is also sent by the transmitter. By using the orthogonal (coincidence) dark and bright soliton pair; thus our proposed system can be claimed as a new security technique for optical cryptographic design in which the information either analog or digital signals can be encoded and formed the secret keys introduced by a random dark-bright soliton pair.



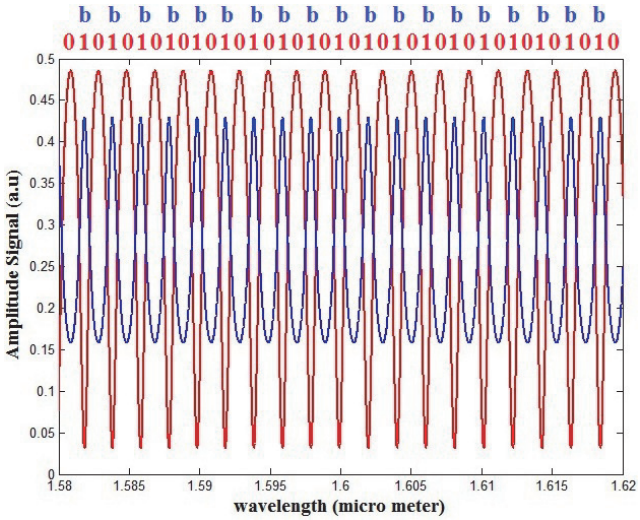
(a)



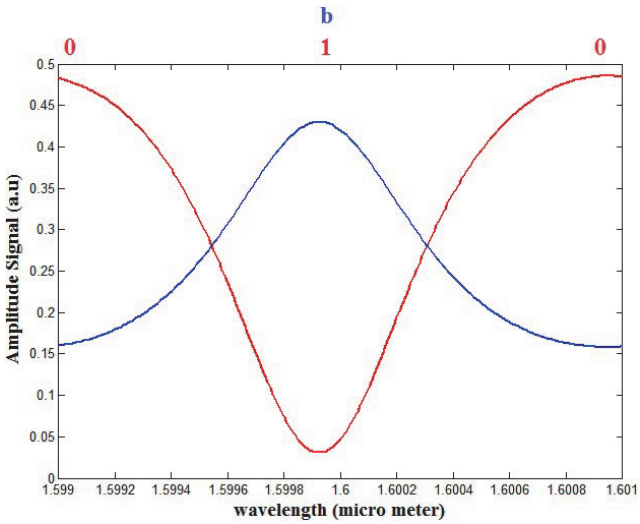
(b)



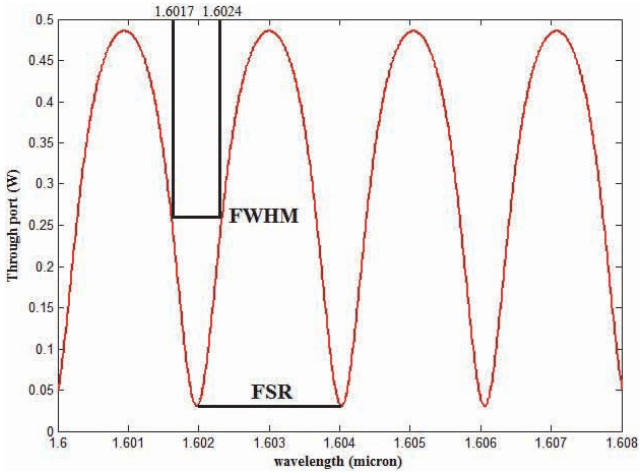
(c)



(d)



(e)



(f)

Fig. 4. Simulation results that can be used for encryption key and data, where (a) and (c) are the keys, (b) and (d) are the data signals, (e) is the orthogonal dark-bright soliton pair(key), (f) are shown Full Width at Half Maximum, (FWHM) and free spectrum range (FSR).

Moreover, this triple security functions can be realized when the security is formed by using the suppressed optical key, in which the optical key changing in every data frame and new optical cryptography technique. Fig.4 shows the simulation result of optical cryptography at the receiver side, where (a) and (c) are the keys, (b) and (d) are the data signals, (e) is the orthogonal dark-bright soliton pair (keys), where the selected wavelength center can be made by using the designed add/drop filter, whereas the required spectral width (full width at half maximum, FWHM) and free spectrum range (FSR) are obtained as shown in Fig. 4(f) The channel spacing and channel capacity are represented by FSR and FWHM, respectively; for instance, the FSR and FWHM of 0.002 μm and 0.00007 μm are obtained, which means that there are many channels are filtered by PANDA ring resonator

4. Soliton Cryptography Protocol

Generally, when a bright or dark soliton is propagated into a $\pi/2$ phase shifter device (beamsplitter or an optical coupler), the dark-bright soliton conversion (pair) can be randomly generated and detected. Dark-bright soliton pair has shown the interesting concept in the same way of orthogonal signal behaviors [Eqs. (16)]. By using the orthogonal dark-bright soliton pair, the random binary bits can be established, which can be described by the following relations.

$$|\Delta B\|\Delta D| \le 1 \tag{16a}$$

$$|B|-|D| \ge 0, |B| \ge |D| \tag{16b}$$

$$|B|^2 + |D|^2 \le 1 \tag{16c}$$

Here B and D bright and dark solitons. From Fig. 2, the dark-bright soliton pair is generated by the transmission part then encoded by the referencing bits and propagated into the network, where finally, the decoded bits will be detected and retrieved by the individual end user. According to the conditions in Eq. (16), the optical network security can be formed as following details. In operation, the sender (Alice) and receiver (Bob) have to perform the secret keys that can be avoided the eavesdropper (Eve), in which the reference bits (codes) are initially generated by the transmission part, where the retrieved codes can be detected and characterized by each end user. By using the normalized signal condition, the end user can use the signal conditions in Eq. (16) to select the corrected and required information. The selected keys have to satisfy the Eq. (16), in which the information can be retrieved. Otherwise, it is not the required information. In addition, the different wavelengths and codes can be applied to large network applications.

5. Conclusion

We have proposed a novel design optical cryptography, which is the interesting concept of the optical key generation that can be used in either analogue or digital communication, where the long-distance link by using a soliton communication is the other advantage. The random keys are generated by the dark-bright soliton pair within a PANDA ring resonator, in which the high-capacity keys are also available due to the nonlinear behavior of the PANDA ring. In applications, the required information between Alice and Bob can be obtained privately without eavesdropping by using the proposed system, where the use of such a system for large scale and long-distance networks is also available.

Acknowledgments

We would like acknowledge the AUN/SEED-Net for the full financial support of Mr. Xaythavy Louangvilay in higher education and thanks King Mongkut's Institute of Technology Ladkrabang (KMITL), Bangkok, Thailand. for providing the excellent research facilities.

Reference

[1] M. Ballav and A. R. Chowdhury, "On a study of diffraction and dispersion managed soliton in a cylindrical media," PIER 63, 33–50 (2006).

[2] S. Konar and A. Biswas, "Soliton-soliton interaction with power law nonlinearity," PIER 54, 95–108 (2005).

[3] R. Gangwar, S. P. Singh, and N. Singh, "Soliton based optical communication," PIER 74, 157–166 (2007).

[4] F. G. Gharakhili, M. Shahabadi, and M. Hakkak, "Bright and dark soliton generation in a left-handed nonlinear transmission line with series nonlinear capacitors," PIER 96, 237–249 (2009).

[5] G. P. Agarwal, Nonlinear Fiber Optics, 4th ed., Academic Press, New York (2007).

[6] Y. S. Kivshar and B. Luther-Davies, "Dark optical solitons: physics and applications," Phys. Rep. 298, 81–197 (1998).

[7] D. N. Christodoulides et al., "Theory of incoherent dark solitons," Phys. Rev. Lett. 80, 5113–5115 (1998).

[8] S. Mitatha, "Dark soliton behaviors within the nonlinear micro and nanoring resonators and applications," PIER 99, 383–404 (2009).

[9] S. F. Hanim, J. Ali, and P. P. Yupapin, "Dark soliton generation using dual Brillouin fiber laser in a fiber

optic ring resonator," Microw. Opt. Technol. Lett. 52, 881–883 (2010).

[10] A. M. Weiner et al., "Experimental observation of the fundamental dark soliton in optical fibers," Phys. Rev. Lett. 61, 2445–2448 (1988).

[11] K. Sarapat et al., "Novel dark-bright optical solitons conversion system and power amplification," Opt. Eng. 48, 045004 (2009).

[12] T. J. Kippenberg and K. J. Vahala, "Cavity opto–mechanics," Opt. Express 15, 17172–17205 (2007).

[13] B. Dayan et al., "A photon turnstile dynamically regulated by one atom," Science 319, 1062–1065 (2008).

[14] Q. Xu, P. Dong, and M. Lipson, "Breaking the delay-bandwidth limit in a photonic structure," Nature Photon. 3, 406–410 (2007).

[15] J. S. Levy et al., "CMOS-compatible multiple-wavelength oscillator for on-chip optical interconnects," Nature Photon. 4, 37–40 (2009).

[16] D. K. Armani et al., "Ultra-high-Q toroid microcavity on a chip," Nature 421, 925–928 (2003).

[17] T. Aoki et al., "Observation of strong cooling between one atom and a monolithic microresonator," Nature 443, 671–674 (2006).

[18] P. DelHaye et al., "Optical frequency comb generation from a monolithic microresonator," Nature 450, 1214–1217 (2007).

[19] S. M. Spillane, T. J. Kippenberg, and K. J. Vahala, "Ultralow-threshold Raman laser using a spherical dielectric microcavity," Nature 415, 621–623 (2002).

[20] G. Anetsberger et al., "Ultralow-dissipation optomechanical resonators on a chip," Nature Photon. 2, 628–633 (2008).

[21] K. J. Vahala, "Optical microcavities," Nature 424, 839–846 (2003).

[22] Y. H. Lee and J. Wu, "Integration network for wireless communication and CATV broadcasting with fiber optic star-ring hierarchical structure," Microw. Opt. Technol. Lett. 18, 41–44 (1998).

[23] F. Matera et al., "Proposal of a high-capacity all-optical TDMA network,"Microw. Opt. Technol. Lett. 18, 132–141 (1998).

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

[25] P. Camarda et al., "Proposal of all-optical shuffle multihop networkswith dedicated and shared channels," Microw. Opt. Technol. Lett. 6, 889–892 (1993).

[26] P. Hua et al., "Integrated optical dual Mach–Zehnder interferometer sensor," Sensors Actuators B. 87, 250–257 (2002).

[27] C. Kostrzewa et al., "Tunable polymer optical add/drop flter for multiwavelength networks," Photon Technol Lett. 9, 1487–1489 (1997).

[28] P. D. Townsend, "Quantum cryptography on optical fiber networks," Opt. Fiber Technol. 4, 345–370 (1998).

[29] T. Carmon et al., "Feedback control of ultra-high-Q microcavities: application to micro-Raman lasers and microparametric oscillators," Opt. Express 13, 3558–3566 (2005).

[30] W. Siririth et al., "A novel temporal dark-bright solitons conversion system via an add/drop filter for signal security use," Optik. 121, 1955–1958 (2010).

[31] B. Knobnob et al., "Dark–bright optical solitons conversion via an optical add/drop filter for signals and networks security applications," Optik. 121, 1743–1747 (2010).

[32] P. P. Yupapin, "Generalized quantum key distribution via micro ring resonator for mobile telephone networks," Optik. 121, 422–425 (2010).