An Ultrafast all optical Encryption Decryption Scheme based on XOR logic for secure transmission in Optical Networks

Vipul Agarwal, Ramisetti Anurag, Hari Siva Ganesh and Yalavarthi Sitha Ramaiah

Department of Electronics and Communications, K.L. Deemed to be University, Vaddeswaram 522502, India

Abstract. An ultrafast encryption decryption scheme is proposed at 160 Gb/s for secure transmission over optical networks. Proposed Encryption decryption circuits have been designed using semiconductor optical amplifier based XOR logic with delay interferometer. Delay interferometer is used to mitigate effect of slow carrier recovery in semiconductor optical amplifier which act as a bottleneck specially for high data rate signal transmission. The system performance is evaluated and investigated in terms of extinction ratio and quality factor. The results demonstrate that proposed scheme is feasible and offers high level of security at ultrafast data rate.

1. Introduction

Encryption and Decryption have been used widely for secure communication. Encryption is the process of converting information in an unrecognizable form in order to prohibit eavesdropper from getting any meaningful information [1]-[5]. The process to convert encrypted signal back to its original form with the help of keys is known as decryption. To avoid eavesdropping, encryption decryption system must be robust, should not add excess delay and must maintain signal quality. In the last few years optical communication has seen tremendous growth due to rapid increase in internet activity and this growth is expected to rise in future due to optical network tremendous potential to fulfill ever growing demand of high bandwidth [6]-[10]. To secure optical communication there is a need for reliable optical encryption technique, that can be operated at ultrafast data rate.

Traditional electronic encryptionschemes has limited speed and requires complex and expensive optical-electrical-optical (OEO) conversion nodes [11]-[13].Use of optical signal processing elements eliminates the need of conversion points which acts as a bottleneck due to severe speed limitations. Optical signal encryption can be achieved by converting signal into noise like and at the receiver, signal is restored to its original form. Castro et. al.[14] used super structured fiber bragg grating to change signal amplitude and phase pseudorandomly such that signal produces noise like spectrum and at the receiver, reverse characteristics gratings are used to bring back signal to its original shape [14][15].
Annovazzi-Lodi et. al. [16] used chaotic laser at the transmitter side for masking information and at the receiver synchronized laser was used to decrypt the signal. Froehlich et al. [17] encrypted optical signal by converting signal into many narrow spectral sub bands with each sub band having distinct phase. Optical stagnography is another form of encryption where pulses are stretched through chromatic dispersion to an extent that it gets buried in the system noise [18]. Wu. et al. [19] proposed a technique in which ASE noise generated from erbium-doped fiber amplifiers (EDFA) carries the stealth signal and due to spectrum similarity of system noise and ASE noise, stealth signal cannot be detected. All these techniques however suffered from power penalty and signal distortion which arises due to addition of noise moreover, information hidden in such encrypted signal can be recovered by eavesdropper using advance techniques [19].

Figure 1. Optical XOR logic based on SOA-MZI

XOR logic based encryption has received widespread attention as it is easy to implement and signal can be decrypted only when keys are available[20]. XOR based encryption does not require addition of noise or deformation of original signal. In the past researchers have proposed all optical logic gates including XOR which are based on semiconductor laser amplifier loop mirror (SLALOM) [21], Highly nonlinear fiber [22], Terahertz optical asymmetric demultiplexer (TOAD) [23] and semiconductor optical amplifier (SOA) configured Mach–Zehnder interferometer (MZI) [24]. Among these techniques SOA based logic gates has outperformed other techniques due to its desirable features like high non linearity, small size, low power operation and easily integrable with other photonic components [25]. Semiconductor optical amplifier possesses strong nonlinear characteristics that can be exploited for the design of key components like logic gates which are basic building block in the design of important circuits like add drop multiplexing, clock recovery, pattern recognition, parity generator and checker, adder etc [24][25]. Despite these advantages SOA based logic gates have limited operation speed due to slow carrier recovery i.e. in the range of several hundreds of pico-seconds. Pattern effect distortion has been observed as operating speed increases beyond 100 Gb/s[26]. Surender et. al. [20] demonstrated all optical encryption decryption at 120 Gb/s without deteriorating signal quality. Much attention has been paid to improve the performance of SOA based logic gates at ultrafast data rate. Xiang Zhang et. al. [27] presented XOR based encryption decryption at 250 Gb/s by utilizing two photon absorption phase variation in semiconductor optical amplifiers. Zoiros et. al. [28] demonstrated operation of XOR logic at 40 Gb/s by employing delay interferometer in series with SOA-MZI. Delay interferometer mitigates the effect of slow carrier recovery and enhances SOA performance. Recently Kotb et al. [29] enhanced SOA-MZI-DI technique and reported XOR logic at data rate of 320 Gb/s. In this work we propose XOR logic based encryption decryption technique based on SOA-MZI-DI technique at 160 Gb/s.
This paper reports XOR logic based all optical encryption decryption scheme at 160 Gb/s. The proposed circuit utilizes non linear characteristics i.e. cross phase modulation in SOA to achieve XOR operation. XOR logic consists of SOA-MZI configuration with delay interferometer in series.

Figure 2. All optical Encryption Decryption circuit based on SOA-MZI-DI Configuration

2. Operating Principle of proposed encryption decryption system
Semiconductor optical amplifier nonlinear characteristics has been exploited in the design of XOR logic. SOA not only act as non linear element, it also amplifies the incoming signal. The couplers used at the input and output produces $\pi$ phase shift if signal comes out of the opposite port. Continuous wave signal and intensity dependent signal are multiplexed together to the input of SOA. Due to presence of pulse SOA refractive index will change and will introduce $\pi$ phase shift to continuous wave signal [25]. This feature enables SOA to act as a non linear element and this principle is known as cross phase modulation. The phase modulation that occurs in SOA can be expressed by [24]

$$\Delta \Phi = 2\pi N_0 \frac{1}{\lambda} + \alpha [\log G - \log G_0]$$  \hspace{1cm} (1)$$

Here $\lambda$ represents wavelength, $N_0$ is refractive index of SOA without input power, $l$ represents length of active region, $\alpha$ corresponds to linewidth enhancement factor, $G$ is saturated gain and $G_0$ is the linear device gain.

The design of SOA-MZI with couplers are designed such that when two input are different, continuous wave signal will overlaps at the output of coupler 2 constructively while if the inputs are same, continuous wave signal forms destructive interference at the output. Constructive and destructive interference corresponds to 1 and 0 respectively. The optical XOR logic design is shown in figure 1. For Case $A=0$, $B=0$ refractive index of upper and lower SOA remains same so no phase is introduced.
in continuous wave by SOA while $\frac{\pi}{2}$ phase shift is introduced in CW by coupler 1 opposite arm and another $\frac{\pi}{2}$ phase shift is introduced by coupler 2 as signal from lower arm of MZI comes out from opposite port of coupler 2. So, phase difference of continuous wave at the output of coupler 1 is $\pi$ which corresponds to destructive interference. For Case A=0 and B=1 Refractive index of lower arm SOA changes due to presence of pulse resulting in $\pi$ phase shift of CW signal. Due to contributions of two couplers additional $\pi$ phase shift is introduced to continuous wave propagating in lower arm. Hence two continuous wave meet constructively at the out of interferometer. Considering case A=1 and B=0 Upper arm SOA will introduce $\Pi$ phase shift and after taking couplers phase shift, CW meet at the output with constructive interference. For last possible combination A=1 and B=1 both SOA in upper and lower arm will add phase in CW wave so phase difference remains 0 but due to coupler phase shift CW overlaps each other with destructive interference.

In order to mitigate the effect of slow carrier recovery in SOA, delay interferometer is used at the output of SOA-MZI. The delay interferometer consists of two 3 db couplers with unequal upper and lower arms such that length difference is equal to relative time delay $D_t$ as shown in figure. The phase information of switched signal from SOA is exploited by subtracting temporally offset copy of switched signal with itself using DI [28][29]. By properly adjusting $D_t$, the switched signal is made to interfere with its delayed counterpart constructively or destructively such that pulses with sufficient height is clamped while low pulses height is increased, analogous to [28]. In this manner unequal height pulses, generated due to slow carrier recovery of SOA is restored to constant height pulses.

3. Simulation parameters of SOA
SOA parameters used in the simulation is presented in Table 1. SOA employed in encryption and decryption circuit has same simulation parameters. The simulation parameters are in accordance with ref [30].

| Symbol | SOA Parameter          | Value | Unit  |
|--------|------------------------|-------|-------|
| I      | Bias current           | 120   | mA    |
| $\tau$ | Carrier lifetime       | 100   | ps    |
| L      | Amplifier Length       | 800   | $\mu$m|
| $\lambda_A$ | Wavelength of data A   | 1545  | nm    |
| $\lambda_B$ | Wavelength of data B   | 1545  | nm    |
| $\lambda_{CW}$ | Wavelength of CW      | 1555  | nm    |
| $P_{sall}$ | Saturation Power       | 20    | mW    |
| $\Gamma$ | Confinement factor     | .3    | -     |
| $M_L$  | Material loss          | 1000  | m$^{-1}$|
| T      | Active layer Thickness | .2    | $\mu$m |
| $N_0$  | Carrier density at transparency | $1 \times 10^{20}$ | m$^{-3}$ |
| a      | Material Gain constant | $2 \times 10^{-20}$ | m$^2$ |
| T      | Bit Period             | 3     | ps    |

4. SOA-MZI-DI based all optical encryption decryption at 160 Gb/s
Optisystem Optiwave is used to simulate the proposed setup at ultrafast data rate of 160 Gb/s. Figure 2 demonstrates schematic of all optical encryption decryption of simulation bandwidth of 300 Ghz. $2^7-1$ pseudorandom generator is used to generate random data bits which amplitude modulates a laser centred at 1545 nm with input power of 10 mW and FWHM of 1 Mhz. Continuous wave signal is generated by
laser source at 1555 nm with 8 mW power. The key is generated by delaying data signal by 8.7 ps and it is transmitted to decryption circuit also to retrieve original signal from encrypted signal. Attenuator of .2 dB is used just before SOA to avoid gain saturation at high data rate [20]. Bandpass filter with two poles, tuned to CW signal wavelength is employed at the output of interferometer. Delay of .2 ps is selected in delay interferometer as quality factor of encrypted signal is maximum for this delay.

4.1. Encryption process at the transmitter side

Encryption process is performed through XOR operation between input signal A with signal B which corresponds to key. The encrypted signal is obtained at the output of bandpass filter with 1.1mW power. Eye diagram of encrypted signal with quality factor 11.2 and extinction ratio of 10.1 dB is obtained as shown in the figure 3. To understand the contribution of delay interferometer, proposed circuit is simulated without delay interferometer with same parameters. The eye diagram of proposed circuit without DI is shown in figure 4 and quality factor obtained is only 7. It is impractical to send a signal to receiver with such poor quality factor as this value will further deteriorate due to fiber dispersion and attenuation. It is evident from both eye diagrams that DI plays a significant role in mitigating the effect of slow carrier recovery and obtained result justifies use of delay interferometer moreover the result is consistent with [29].

Figure 3. Encrypted signal eye diagram for SOA-MZI-DI based XOR logic.

4.2. Decrypted process at the transmitter side

Encrypted signal is transmitted through 100 Km SMF DCF. Total loss in SMF fiber is .2 dB/km and dispersion parameter is taken as 16/ps/km/nm. Figure 5 presents the clear eye diagram of decrypted signal with quality factor 9 and extinction ratio of 8.1 dB is shown in figure 5. In optical communication, quality factor above 7 is considered to be acceptable by researchers.
Figure 4. Encrypted signal eye diagram for SOA-MZI (without delay interferometer) based XOR logic.

Figure 5. Decrypted signal eye diagram for SOA-MZI-DI based XOR logic with a quality factor of 9.

5. Conclusion
This paper presents all optical encryption decryption scheme based on SOA-MZI-DI. Cross phase modulation in SOA has been exploited for XOR logic design. The performance of delay interferometer is investigated, and it is shown that presence of delay interferometer assists in mitigating the effect of slow carrier recovery in SOA that acts as bottleneck in high speed applications. In the absence of delay interferometer Q factor of encrypted signal obtained is 7 but when delay interferometer is used Q factor of encrypted signal was enhanced. Encrypted and decrypted signal at 160 Gb/s exhibited clear eye diagram with quality factor of 11.2 and 9 respectively. Extinction ratio for encrypted and decrypted signal is 10 dB and 8.1 dB respectively. It is impossible for eavesdropper to retrieve information from encrypted signal as key and SOA parameters are mandatory requirements to decrypt the signal. The proposed scheme offers secure communication in fiber optics network at ultrafast data rate.
References

[1] F. Noorbasha, Y. Divya, M. Poojitha, K. Navya, A. Bhavishya, K. Koteswara, K. Hari, “FPGA design and implementation of modified AES based encryption and decryption algorithm,” International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 6, pp. 132-136, 2019.

[2] Ernest Ravindran, K. Priyadarshini, A. Sai, P. Shiny, S. Sabeeha, “Design of finite field multiplier for efficient data encryption,” International Journal of Advanced Science and Technology, vol. 28, no. 20, pp. 42-52, 2019.

[3] F. Noorbasha, K. Deepthi, G. Jhansi, Hari Kishore, “Implementation of high secured low power advance encryption standard (AES) implementation with DNA cryptography,” International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 6, pp.110-114, 2019.

[4] A. Murali, Hari Kishore, “Efficient and high speed key-independent AES-based authenticated encryption architecture using FPGAs,” International Journal of Engineering and Technology(UAE), vol. 7, no 1.5, pp. 230- 233, 2018.

[5] Murali Krishna, G.L. Madhumati, H. Khan, “Stochastic key generation mechanism in cryptography applications through partial reconfiguration,” Journal of Advanced Research in Dynamical and Control Systems, vol. 9, no.12, pp.1566-1586, 2017.

[6] G.R.K. Prasad, T. Vivek, Phani Rohith, Y. Yashwanth, “Verilog implementation on cryptography encryption and decryption of 8 bit data using ECC algorithm,” Journal of Advanced Research in Dynamical and Control Systems, vol. 9, no.14, pp. 2711-2719, 2017.

[7] Durga Indira, K. Sony, S. Krishna, G.Vinayak, T. Pavan, T. Gurunadham “Analysis of optical link using 4x1 WDM,” International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 6, pp. 1682-1685, 2019.

[8] G. Immadi, M. Venkata Narayana, S.K. Kotamraju, A. Sree Madhuri “Estimating the Performance of Free Space Optical Link Under Adverse Weather Conditions by Using Various Models,” Wireless Personal Communications, vol.103, no. 2, pp. 1603- 1613, 2018.

[9] G. Palai, B. Nayak, S.K. Sahoo, S.R. Nayak, S.K. Tripathy, “Metamaterial based photonic crystal fiber memory for optical computer,” Optik, vol.171, pp. 393- 396, 2018.

[10] M.K. Chhipa, D.S. Priya, M. Radhouene, B. Suthar, K.Srimannarayana, “Fractal structure ring resonator based channel drop filter for optical networks using InP dielectric material,” Journal of Engineering and Applied Sciences, vol. 12, no. 2, pp. 6195-6200, 2017.

[11] C. A. Barrios and M. Lipson, “Silicon photonic read-only memory,” J.Lightw. Technol., vol. 24, no. 7, pp. 2898–2905, 2006.

[12] G. C. Valley, “Photonic analog-to-digital converters,” Opt. Exp., vol. 15, no. 5, pp. 1955–1982, 2007.

[13] F. F. Froehlich, C. H. Price, T. M. Turpin, and J. A. Cooke, “All-optical encryption for links at 10 Gb/s and above,” in Proc. IEEE Military Commun. Conf., vol. 4. Atlantic City, pp. 2158– 216, 2005.

[14] M. Castro, Ivan B. Djordjevic, and David F. Geraghty, "Novel Super Structured Bragg Gratings for Optical Encryption," J. Lightwave Technol., vol. 24, pp 1875- 1880, 2006.

[15] P. Torres, L. C. G Valente, and M. C. R Carvalho, “Security systemfor optical communication signals with fiber Bragg gratings,” IEEE Trans. Microw. Theory Tech., vol. 50, no. 1, pp. 13–16, 2002.

[16] V. Annovazzi-Lodi and A. Scire, “Synchronization of chaotic injected laser systems and its application to optical cryptography,” IEEE J. Quantum Electron., vol. 32, no. 6, pp. 953–959, 1996.
[17] F. Froehlich, C. Price, T. Turpin, J. Cooke, “All optical encryption for links at 10 Gb/s and above,” IEEE Photon. Technol. Lett. Vol. 19, no. 4, pp 1–7, 2005.
[18] M. Fok, P. Prucnal, “A compact and low-latency scheme for optical steganography using chirped fiber Bragg grating,” Electron Lett., vol. 45, no. 3, pp. 179-180, 2009.
[19] B. Wu and E. Narimanov, “A method for secure communications over a public fiber-optical network,” OptExpress vol. 14 pp no 9 3738-3751, 2006.
[20] S. Singh, Lovkesh, X. Ye and R. S. Kaler, "Design of Ultrafast Encryption and Decryption Circuits for Secured Optical Networks," IEEE Journal of Quantum Electronics, vol. 48, no. 12, pp. 1547-1553, 2012.
[21] Y. H. Kao, I. V. Goltser, M. N. Islam and G. Raybon, "Ultrafast optical logic gate using a semiconductor laser amplifier operating at transparency in a loop mirror," CLEO Summaries of Paper, pp. 94-95, USA, 1997.
[22] J. Qiu, K. Sun, M. Rochette and L. R. Chen, "Reconfigurable All-Optical Multilogic Gate (xor, and, and or) Based on Cross-Phase Modulation in a Highly Nonlinear Fiber," IEEE Photonics Technology Letters, vol. 22, no. 16, pp. 1199-1201, 2010.
[23] K. Maji and K. Mukherjee, "Performance analysis of optical logic XOR gate using dual-control Tera Hertz Optical Asymmetric Demultiplexer (DCTOAD)," Devices for Integrated Circuit (DevIC), Kalyani, pp. 58-60, India, 2019.
[24] S. Singh and Lovkesh, "Ultrahigh Speed Optical Signal Processing Logic Based on an SOA-MZI," IEEE Journal of Selected Topics in Quantum Electronics, vol. 18, no. 2, pp. 970-977, 2012.
[25] V. Agarwal and M. Agrawal, "Characterization and optimization of semiconductor optical amplifier for ultra high speed applications: A review," Conference on Signal Processing And Communication Engineering Systems (SPACES), pp. 215-218, India 2018.
[26] F. Ginovart and J. Simon Gain, “Dynamics study of a semiconductor optical amplifier,” Pure Appl. Opt. vol 4, 2002.
[27] X. Zhang, W. Li, H. Hu and N. K. Dutta, "High-speed all-optical encryption and decryption based on two-photon absorption in semiconductor optical amplifiers," IEEE/OSA Journal of Optical Communications and Networking, vol. 7, no. 4, pp. 276-285, 2015.
[28] K. Zoiros and C. Demertzis, “On the data rate extension of semiconductor optical amplifier-based ultrafast nonlinear interferometer in dual rail switching mode using a cascaded optical delay interferometer,” Opt. Laser Technol. vol.43, pp. 1190–1197, 2011.
[29] A. Kotb, K. Zoiros, C. Guo, “320 Gb/s all-optical XOR gate using semiconductor optical amplifier-Mach–Zehnder interferometer and delayed interferometer,” Photon Network Communication, vol. 38, pp. 177–184, 2019.
[30] G. P. Agrawal: Fiber-Optic Communication System, Singapore: Wiley, 2010.