Computer Science and Information Technologies
Vol. 2, No. 1, March 2021, pp. 11~15
ISSN: 2722-3221, DOI: 10.11591/csit.v2i1.p11-15

Impact of encryption and decryption techniques for high speed optical domain

Rishabh Singh[1], Ghanendra Kumar[2], Chakresh Kumar[3]
[1,3]University School of Information, Communication and Technology, Guru Gobind Singh Indraprastha University,
New Delhi 110078, India
[2]Department of Electronics and Communication Engineering, National Institute of Technology, Delhi 110040, India

Article Info

Article history:

Received Mar 28, 2020
Revised Jun 21, 2020
Accepted Jul 28, 2020

Keywords:

Decryption
Encryption
Fiber bragg grating
Raman amplifier

ABSTRACT

This project proposes the design of ultrafast communication circuit which can enable the high speed secured data transmission at 50 Gb/s and 100 Gb/s by the use of distributed raman amplifier, erbium–doped fiber amplifier (EDFA), filter, single mode fiber along with fiber Bragg grating (FBG) and attenuators. The simulation of the suggested optical circuit involves the use of parameters of Raman amplifier and EDFA and other components included in the optical structure. The design also includes the use of encryption and decryption techniques to ensure secured communication. Thus, realization of these circuits at 50 Gb/s and 100 Gb/s will enable the future optical communication applications for ultrafast data transmission to large distances.

Corresponding Author:

Chakresh Kumar
University School of Information, Communication & Technology
Guru Gobind Singh Indraprastha University, New Delhi 110078, India
Email: chakreshk@gmail.com

1. INTRODUCTION

Communication is undoubtedly an integral part of our lives. We communicate through a lot of ways like through telephone, consuming information on the Internet (receiving or sending data), over FAX and numerous other ways. As the size of data and speed requirements increases day by day, the need for communication models which can sustain high speed communication is also increasing. Optical communication provides us a solution as it possess features like low attenuation rate, less interference from external sources, low power loss and much greater bandwidth. Due to the increased speed the vulnerabilities in the communication also increases. Therefore, the need of security of information in the transmission process is an important. Using conventional technique for securing our information restricts the data transfer speed to a certain level. Optoelectronics conversion (first the incoming signal is converted into the electrical signal and then all the processing is done in electrical medium and then the signal is finally converted to optical form for further transmission) increases the delay. All conventional logic circuits use optoelectronics conversion. To overcome that we need optical processing elements in which optical processing elements is not required. Use of optical logic gates (optical XOR gates) is central to the development of designing circuits which can ensure secure transmission of data. Optical communication at a speed of 10 GB/s using encryption and decryption circuits was demonstrated by Jung [2]. The security of optical signal relies mainly on the physical properties of the signal and not on the computational complexity as in software systems. The process of high-speed optical communication posses a lot of problems like requirement of optoelectronics conversion and the data rate is limited because of the inherent time constants dictating laser dynamics. Also, it has a small number of user adjustable parameters (low soft-key dimension) such that security relies almost entirely on the inability of an eavesdropper to obtain similar laser hardware (i.e. on the hard key) as explained in [3].

2. PRINCIPLE OF THE PROPOSED MODEL

The proposed model works on the principle of using optical logic gates for transmission which allows us to use the technique of optical encryption and decryption to distances upto 300 km. This can be achieved by using distributed raman amplifier. The distributed raman amplifier-based logic gate provides us a method to have high speed transmission to very large distances. The positioning of of the path length difference of the signals going to the input to raman amplifier is done in a way so that the total power goes at one output at particular optical frequency. Extreme patterns will be formed due to misadjusted beams in both outputs whose shapes will be affected by changes in path length difference. Whereas the distribution of overall powers on the outputs may not change when data signals are launched into the Raman amplifier carrier density and as a result the refractive index of the medium gets changed. This causes a change of phase over the control signal counter-propagating through the Raman amplifier (control signal) according to the changes in the intensity of the input data signals.

Appropriate adjustments of the optical powers and the bias currents or by designing the parameters of the raman distributed amplifier, the control signal from the two raman amplifiers can interfere either constructively or destructively. This directly performs the logic XOR operation of the two input data signals which is basic element used for optical encryption and decryption process. The signal received is filtered by the help of a raised cosine filter which minimizes the intersymbol interference. The encrypted signal obtained from the filter is transmitted by single mode fiber along with fiber bragg grating (which compensates for the dispersion caused). Then the encrypted signal is transmitted further using amplifiers to maintain its amplitude and is decrypted to get back the original data signal. The structure of the decryption circuit is almost same to that of the encryption and it too consists of optical couplers along with Raman amplifiers, EDFA and filters.

3. EXPLANATION OF CIRCUIT DIAGRAM FOR OPTICAL ENCRYPTION AND DECRYPTION PROCESS AT 50 Gb/S

In the proposed design distributed Raman amplifier is used because of the fact that Raman amplifiers possess a wider band as compared to EDFA or SOA, raman amplifier works for almost all wavelengths whereas the EDFA works for (1525-1565 nm) and (1570-1610 nm).Also it enables distributed amplification within the transmitting fiber, *i.e.* higher pump power (~>30 dBm) as compared to EDFA(~25 dBm) or SOA(~4.5 dBm) which helps us to maintain the power level up to large distances and can increase the length of spans between the amplifiers and regeneration sites. Also, Raman amplifier can be used to extend Erbium-doped Fiber Amplifier (EDFAs) and is compatible with single mode fiber. The only important drawback of Raman amplifier over other amplifier is that it requires pump lasers with high optical power (>1 watt) with related thermal management issues and it is costlier as compared to other amplifiers. Circuit diagram for optical encryption and decryption at 50 GB/s is shown in Figure 1.

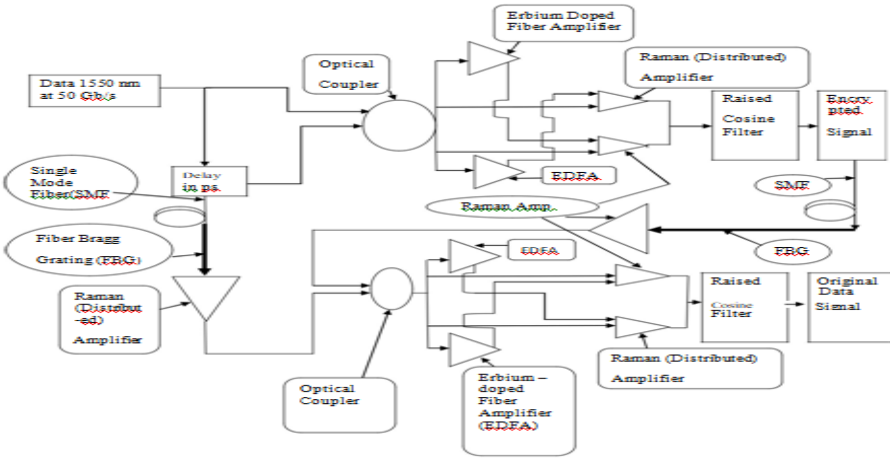

Figure 1. Circuit diagram for optical encryption and decryption at 50 GB/s

3.1. Encryption process

In this design data in the return to zero (RZ) format is given as input at 50 Gb/s with the help of a laser source. The signal is delayed and both the original and the delayed signal is given as input to the optical coupler along with the splitter which then splits the signals which is then given to the erbium doped fiber amplifier. The output signal is then given as input to the distributed Raman amplifier which then increases the output power so that the signal can be transmitted to larger distances. The output signal from the distributed Raman amplifier is filtered out by using a raised cosine filter and the encrypted signal is passed through a single mode fiber (SMF) along with fiber Bragg grating (FBG) to ensure minimum loss of signal.

3.2. Decryption process

The encrypted signal after passing it through single mode fiber along with fiber Bragg grating is again given as input to distributed Raman amplifier so as to ensure that the power level does not drop and the signal is not lost. The decryption process is quite similar to the encryption process. The signal from amplifier is given as input to the optical coupler along with the splitter and output signal is given as input to EDFA and then its output is given as input to distributed Raman amplifier. The signal from Raman amplifier is given as input to the raised cosine filter which then gives back the original data signal.

4. EXPLANATION OF CIRCUIT DIAGRAM FOR OPTICAL ENCRYPTION AND DECRYPTION PROCESS AT 100 Gb/S

The main difference between the circuit at 50 GB/s and the circuit at 100 Gb/s is that the circuit for designing the transmission circuit for 100 Gb/s is that it does not require an EDFA. Instead, it uses an attenuator so as to ensure that the power level added due to noise is not too much. Also, the signal used for encryption is different than that used in the generation of encrypted signal. Circuit diagram for optical encryption and decryption at 100 GB/s as shown in Figure 2.

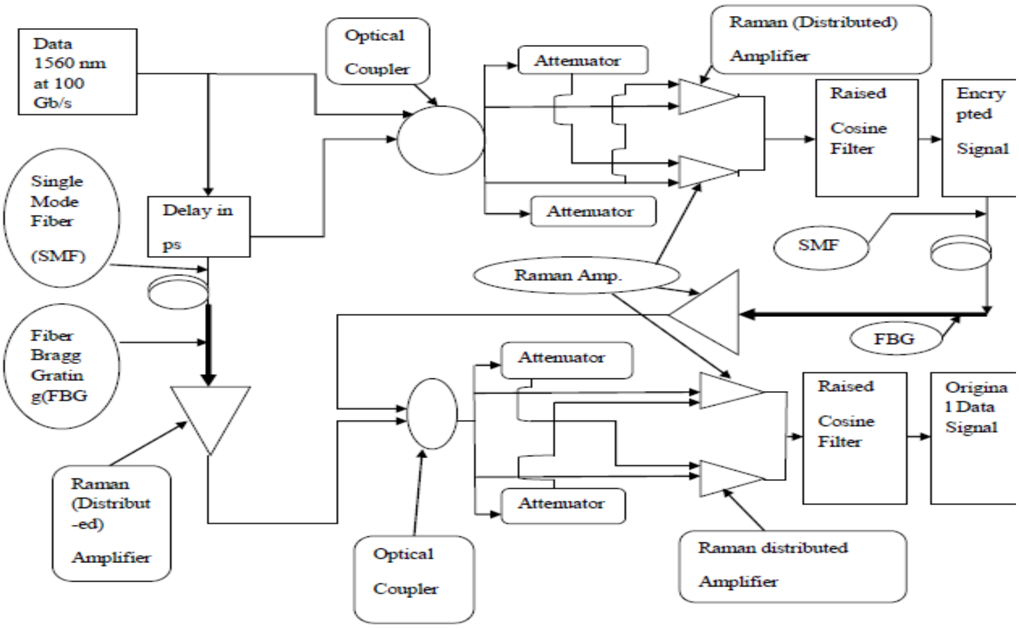

Figure 2. Circuit diagram for optical encryption and decryption at 100 GB/s

4.1. Encryption process

In this design data in the RZ format is given as input at 100 Gb/s with the help of a laser source. The signal is delayed and both the original and the delayed signal is given as input to the optical coupler along with the splitter which then splits the signals which is then given to the attenuator. The output signal is then given as input to the distributed Raman amplifier which then increases the output power so that the signal can be transmitted to larger distances. The output signal from the distributed Raman amplifier is filtered out by using a raised cosine filter and the encrypted signal is passed through a SMF along with FBG to ensure minimum loss of signal.

4.2. Decryption process

The encrypted signal after passing it through single mode fiber along with Fiber Bragg grating is again given as input to distributed Raman amplifier so as to ensure that the power level does not drop and the signal is not lost. The decryption process is quite similar to the encryption process. The signal from amplifier is given as input to the optical coupler along with the splitter and output signal is given as input to attenuator and then its output is given as input to distributed Raman amplifier. The signal from Raman amplifier is given as input to the raised cosine filter which then gives back the original data signal.

5. RESULTS AND DISCUSSION

5.1. Output figure at 50 Gb/s

The graph is a plot of power of input signal, delayed signal and the encrypted signal at 50 Gb/s with respect to the time in nanoseconds, as shown in Figure 3.

5.2. Output figure at 100 Gb/s

The above graph is a plot of power of input signal, delayed signal and the encrypted signal at 100 GB/s with respect to the time in nanoseconds, as shown in Figure 4.

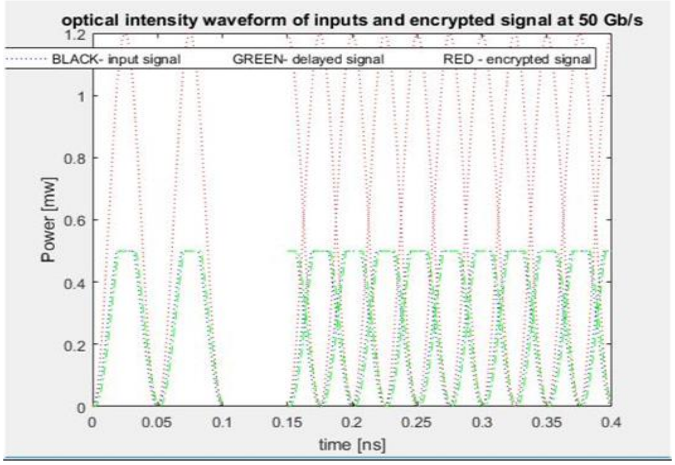

Figure 3. Output figure at 50 Gb/s

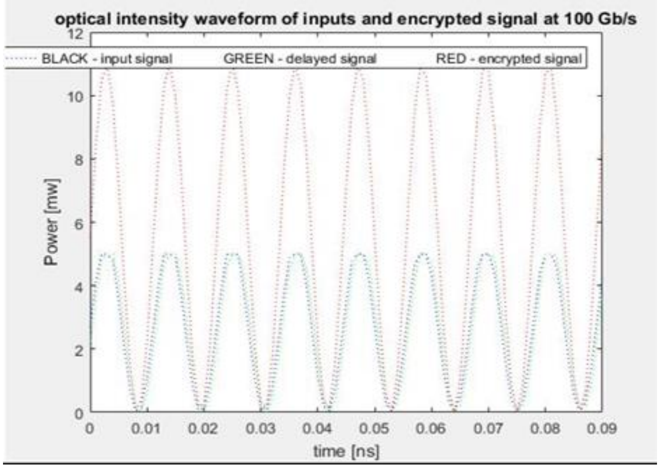

Figure 4. Output figure at 100 Gb/s

6. CONCLUSION

This paper proposed the circuit for carrying out the optical communication at 50 Gb/s and 100 Gb/s along with the use of encryption and decryption techniques to ensure secured transmission. The simulation results for the circuits at ultrafast speeds are also demonstrated in the paper. The secured signal can be successfully transmitted to more than 300 km without any decrease in the quality of signal. The suggested circuit includes the use of distributed Raman amplifier, Erbium-doped fiber amplifier (EDFA), single mode fiber along with fiber Bragg grating and optical combiners and attenuators. These results are obtained in accordance with the expectations and according to the behavior shown by the elements used in the proposed circuit and can be used in future optical communication circuits to enable high speed secured optical communication to large distances.

REFRENCES

[1] S. Singh, Lovkesh, X. Ye, R. S. Kaler. “Design of Ultrafast Encryption and Decryption Circuits for Secured Optical Networks,” in *IEEE Journal of Quantum Electronics*, vol. 48, no. 12, pp. 1547-1553, Dec. 2012, doi: 10.1109/JQE.2012.2222633.

[2] Y.J. Jung, C.W. Son, S. Lee, S. Gill, H.S. Kim, N. Park. “Demonstration of 10 GB/s all-optical encryption and decryption system utilizing SOA XOR logic gates,” *Optical and Quantum Electronics,* vol. 40, no. 56, pp. 425–430, Apr 2008, doi:10.1007/s11082-008-9224-7.

[3] O. Bushkila, A. Eyal and M. Shatif. “Secure communication inn fiber optic systems via transmission of broad-band optical noise,” *Optics Express*, vol. 16, no. 5, pp. 3382-3396, Mar.2008, doi: 10.1364/OE.16.003383.

[4] G.D. VanWiggeren, R. Roy. “Communication with Chaotic lasers,” *Science*. vol. 279, no. 5354, pp. 1198-1200, 1998, doi: 10.1126/science.279.5354.1198.

[5] Nuha Mahmoud Ibrahim, Amin Ambedkar. “A Comparison of Optical Amplifiers in Optical Communication Systems, EDFA, SOA and RAMAN,” *International Journal of Current Research*. vol. 6, no. 9, pp. 8738-8741, 2014.

[6] L. Tancevski, I. Andonovic and J. Budin, "Secure optical network architectures utilizing wavelength hopping/time spreading codes," in *IEEE Photonics Technology Letters*, vol. 7, no. 5, pp. 573-575, May 1995, doi: 10.1109/68.384548.

[7] T.H. Shake. “Security performance of optical CDMA against eavesdropping,” *Journal of Lightwave Technology,* vol. 23, no. 2, pp. 655-670, 2005.

[8] Yogesh Chaba, R.S. Kaler, “Comparison of various dispersion compensation techniques at high bit rate using CSRZ format” *Optik*, vol. 121, no. 9, pp. 813-817, 2010.

[9] A. Argyris, D. Syvridis, L. Larger *et al*. “Chaos-based communications at high bit rates using commercial fibre-optic links,” *Nature*. vol. 438, p. 343-346, 2005, doi: 10.1038/nature04275.