A FUTURISTIC APPROACH TOWARDS SECURED OPTICAL COMMUNICATION OPTICAL PRIVATE KEY CRYPTOGRAPHY(OPKC) TECHNIQUE

Aayush Madan[1], Shekhar Saxena[2]

[1,2]*Department of Electronics & Communication Engineering, Malaviya National Institute of Technology, MNIT Jaipur, Jaipur City, Rajasthan (India)*

ABSTRACT

The paper presents an Optical Private Key Cryptography (OPKC) technique to provide security to the user data in high speed optical networks. The circuit involves the Cross Phase Modulation (XPM), a non-linear property, of Semi-conductor Optical Amplifier (SOA). The process involves encryption of the signal with a cipher signal using optical xor and transmission through an optical channel followed by the decryption process. The result shows that security is achieved with BER of ~21.4 dB.

Keywords: *Cross Phase Modulation (XPM), Dispersion Compensated Fiber (DCF), Mach-Zhender Interferometer, Optical Delay Lines (ODLs), Private Key Cryptography.*

I. INTRODUCTION

The requirement of information security during transmission is a major concern in the field of communication engineering. As the speed of communication system increases and reaches to the limit of the electronic devices, [1] demands for digital all optic signal processing is rapidly increasing. Fiber and the free space optical transmission systems are the backbone of many high speed critical data networks. In order to provide user data with security and allow only authenticated users to access the data, cryptography is employed. Electronic encryption is a well mature technique with many schemes at different costs but it is limited to a relatively lower data rate because of limitation of electronic components, circuitry and significant delay per bit. There is also a physical vulnerability at every optical-electrical-optical (OEO) conversion point[3].

Optical processing elements are attractive in order to full fill the demands of core networks with a huge core capacity because these components do not require any optoelectronic conversion. These optical processing elements [2] are useful in add drop multiplexing, clock recovery, regeneration and pattern reorganization. All of the above functions can be controlled via optical logic gates and SOA be the backbone for any optical logic gates because of its non-linearity properties viz. Four wave mixing, Cross Gain Modulation (XGM), Cross Phase Modulation (XPM) and their combinations[3].The most common method for encryption is to combine the Pseudo random bit sequence pattern with a security key in modulo 2 fashions. XPM in SOA is used to perform modulo 2 operations in optical domain [4].

II. CONCEPT BEHIND APPROACH

Exclusive-OR Boolean function gives logic “1” if the two inputs that are being compared are different. On the other hand, if the inputs are the same the output signal is logic “0”. In the case ofoptical gates, the logic “1” is represented by the presence of an optical power, whereas the logic “0” meant to absence.

SOA based all optical logic gates using XPM is implemented in which the variation on the carrier density induces a change on the refractive index [2] and so the phase of the continuous wave is modulated. This phase modulation can be converted into intensity modulation by using a Mach-Zhender Interferometry (MZI) configuration. This interferometer consists of two identical branches in which an SOA is placed.

When data signals (bit sequences to be compared) are launched into the SOAs, the carrierdensity and, thereby, the medium refractive index is modulated. This causes a phase shiftover the control signal counter-propagating through the SOAs (control signal) according tothe intensity variations of the input data signals. This phase modulation experienced by the wave[5] during propagation in the SOA is given by equation (1)

$$\Delta\emptyset = 2\pi r\left(\frac{L}{\gamma}\right) + \alpha\left[\ln(G) - \ln(G0)\right] \qquad (1)$$

Being λ the wavelength of the input data signal passing through the SOA, *L* the length of theactive region of the SOA, αis SOA linewidth enhancement factor, rthe refractive index inthe absence of optical power, *G* the saturated gain and $G_0$the linear device gain.

By setting the bias currents and optical power and design parameters of SOA in such a way that signal from the two SOAs could interfere either constructively or destructively at the output of the interferometer[3]. This directly performs the XOR operation of the two input data signals which forms the basis for the encryption and decryption circuits.

III. SOA USED IN CIRCUITS

The SOAs used in the circuits are basically Wide Band Semi-conductor Optical Amplifiers (WB-SOA)whose parameters [1,3] are listed below.

Table I. Soa Parameters

S No	Parameters	Value Used in S.I. Units
1	Injection Current	200 mA
2	Active Length	600 µm
3	Width	2.5 µm
4	Height	0.2 µm
5	Input Facet Reflectivity	5.0e-005
6	Output Facet Reflectivity	5.0e-005
7	Input Coupling Loss	3 dB
8	Output Coupling Loss	3 dB
9	Optical Confinement Factor	0.3
10	Carrier Lifetime	0.15 ns
11	Active Refractive Index	3.22

IV. DESIGN AND SIMULATION

In this section, first an optical XOR gate is demonstrated in Fig. 1. Further, Encryption Process with Circuit is explained in section A and Decryption Process with Circuit is explained in section B.

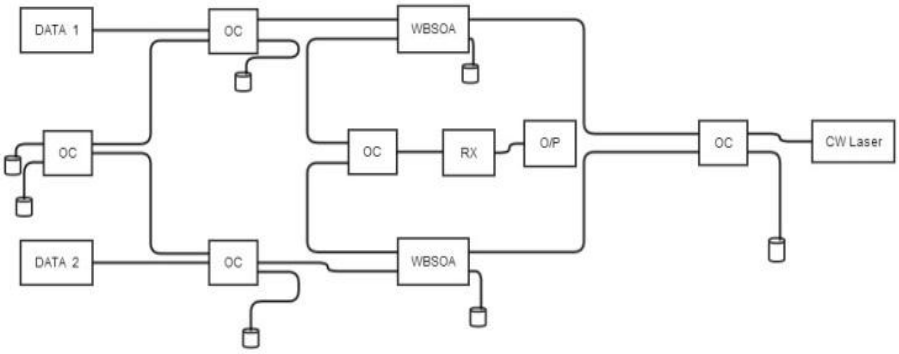

Fig.1. Optical XOR Gate

Data Signal with 30mw power is generated at 1545nm. Control signal is generated at 1535nm using a Continuous Wave (CW) laser having line-width 10MHz. These signals are combined as shown in above figure *Fig.1*, The circuit works at high speed (40Gbps).

4.1 Encryption Process

The process involves XOR operation between two signals viz. data signal and security key signal. Data Signal generated is the intensity modulated optical signal in which a Pseudo Random Binary Sequence (PRBS) is modulated at 40Gbps with a CW lorentzian laser source in return to zero format using Mach Zehnder Modulator. The original data sequence is delayed by few nano seconds (nsec) depending upon the data rate to form a security key. Since number of seconds in delay is the security, any user with the key can only decrypt the signal at decryption site. Any intruder must have to check all possible combinations so brute force is very high which makes the process reliable. The delayed signal is again modulated using same laser source in order to feed into the xor gate input end as shown in Fig.2.

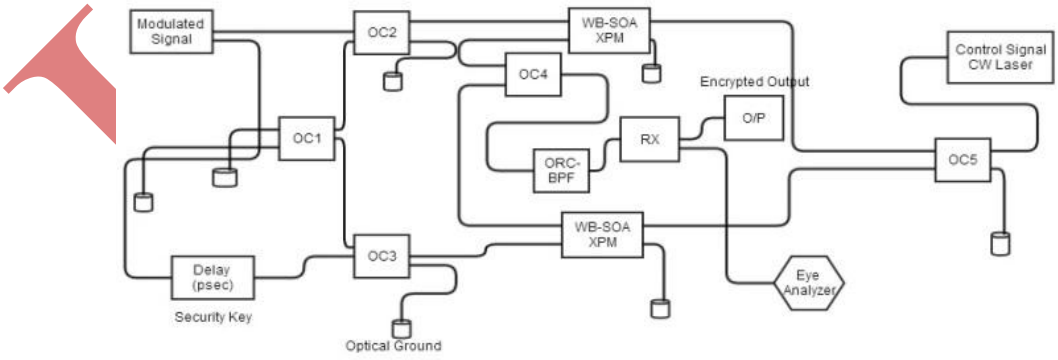

Fig.2. Encryption Process

The encrypted signal is achieved by filtering the optical signal at the output of optical coupler (OC4) using Optical Raised Cosine Band Pass Filter (ORCBPF). ORCBPF is employed to remove the effects of Inter Symbol Interference (ISI) at the output caused at higher data rate. Receiver consists of a photodiode detector with a low pass Bessel filter having 5 poles. The electrical output is analyzed by an eye diagram analyzer. Input

Sequence is shown in Fig.3 and Fig.4 shows the cipher key signal. Spectrum of the input signal is shown in Fig.5

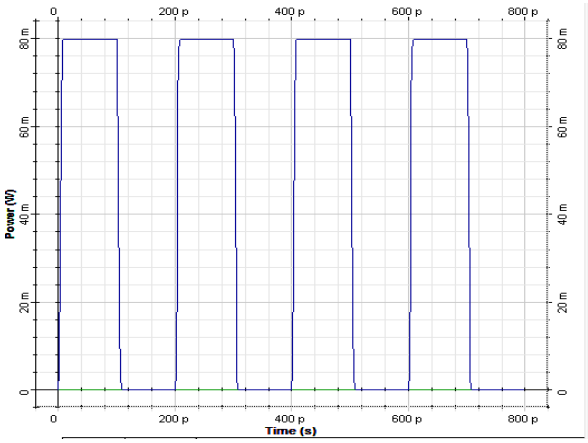

Fig.3. User Data Sequence (10101010)

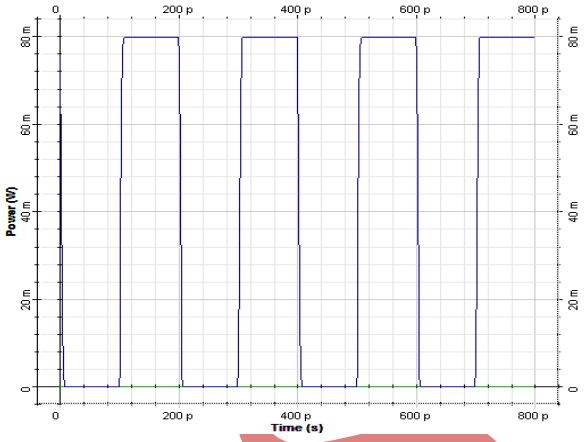

Fig.4.Cipher Key Signal (01010101)

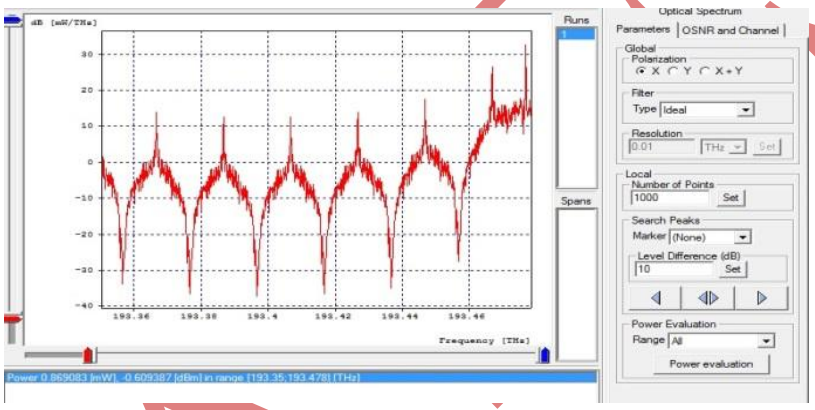

Fig.5. Input Optical Signal Spectrum

The encrypted signal of the input is shown in Fig.6 which is nothing but the output and filtering after the XOR operation.

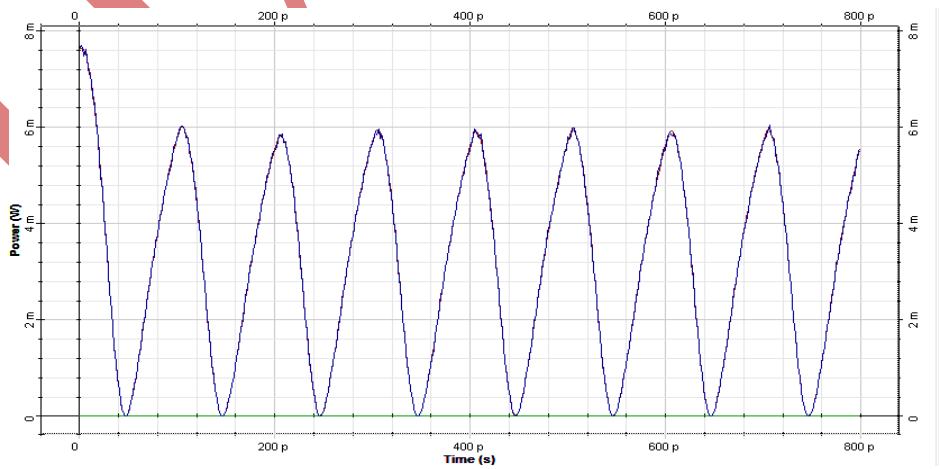

Fig.6. Encrypted Signal (11111111)

Now, Fig.7 and Fig.8 shows the eye diagram analysis of both input and encrypted stream. Using eye diagram one can easily check Q factor, Bit Error Rate (BER) and Jitter.

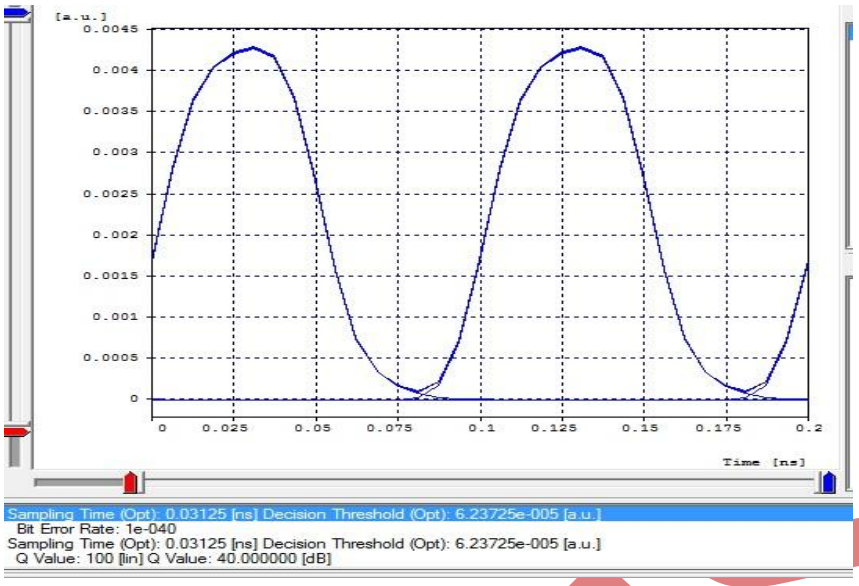

Fig.7. Eye Diagram of Input Signal

The Input stream has Q factor 40 dB and BER of order of 10^{-40}as shown in Fig.7.

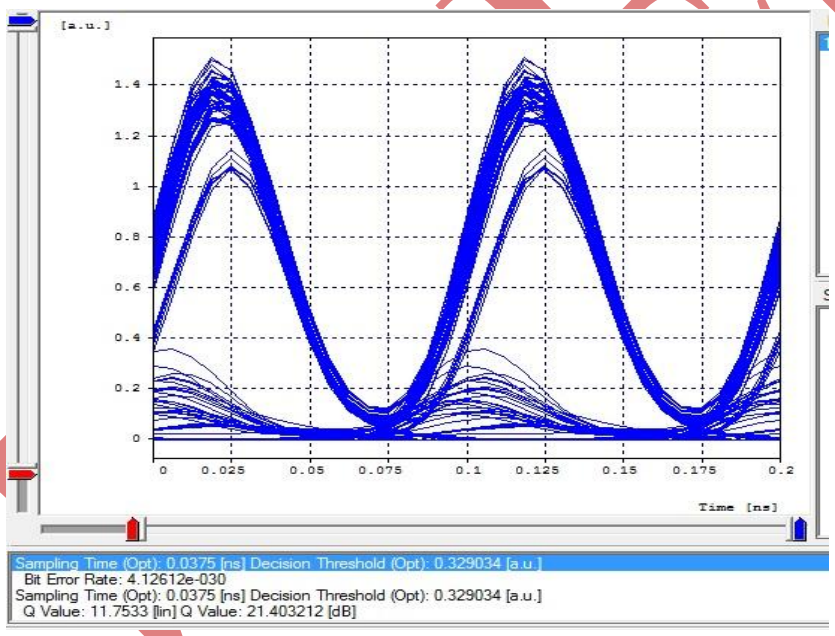

Fig.8. Eye Diagram of Encrypted Signal

The encrypted signal has Q factor of ~21.40 dB with BER of the order of 10^{-30}as shown in Fig.8.

4.2 Decryption Process

The received encrypted signal together with the cipher key signal is fed to the decryption circuit after passing through an optical guide as shown in Fig.9. In this system, the encrypted signal is first passes through a combination of an Optical Fiber, Dispersion Compensating Fiber viz. DCF and an amplifier stage viz. Erbium Doped Fiber Amplifier, EDFA. DCF is used to compensate for the dispersion caused by the system so that ISI can be reduced. The EDFA is used to boost up the signal to an energy level of cipher signal. A fiber of length 5km and dispersion coefficient -102ps/nm/km is used as the DCF. Gain of EDFA used is 15 dB with Noise Figure of 3 dB.

The complete system is analyzed at four different points viz. before encryption (transmitted signal), after encryption (encrypted signal), before decryption (after transmission through channel) and after decryption (receiver).

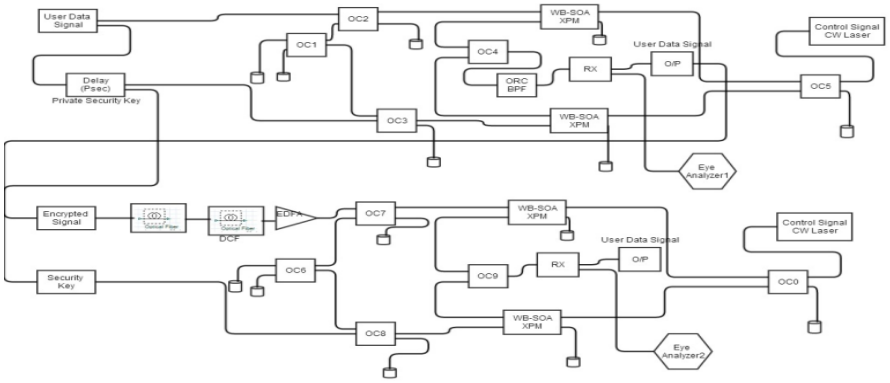

Fig.9. Complete System Encryption plus Decryption

The signal after passing through fiber but before decryption as shown in Fig.10 is passed along with cipher key signal in the decryption circuit. The signal after decryption is shown in Fig.11. Decrypted signal is received at output of optical coupler OC9 which can be easily converted to electrical domain using a photo-detector and a low pass filter. It is impossible to retrieve by unknown without using the encrypted and decrypted circuits and the required conditions. The eye diagram of the received decrypted signal is shown in Fig.12.

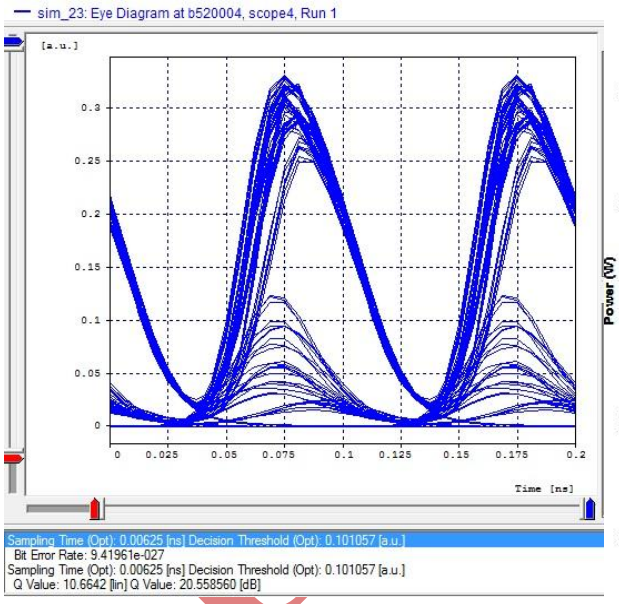

Fig.10. Eye Diagram of Signal before Decryption

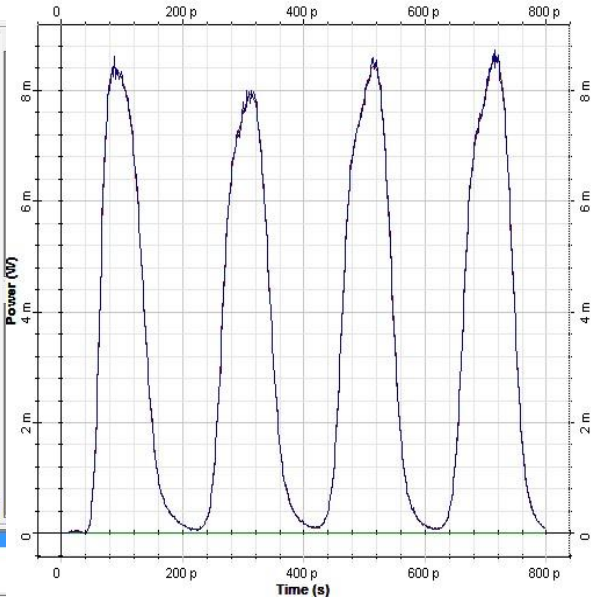

Fig.11. Signal after Decryption (10101010)

Electrical properties of the received signal can be analyzed using eye diagram analyzer. Fig.12 shows eye diagram of the signal after decryption. A user can easily check Q Factor, BER and Jitter properties of the received signal.

V. CONCLUSION

The need of secured communication at high speed is achieved with these encryption and decryption circuits. The signal after encryption with cipher key is transmitted through fibers etc. The system results show better performance in the signal processing without deteriorating the quality of the signal in terms of BER and Q factor.

The system to be compensated against the dispersion caused in the encrypted signal otherwise Q factor of the decrypted signal will be diminished.

VI. ACKNOWLEDGMENT

This paper is made possible through the help and support from everyone including: parents, teachers, colleagues and in essence, all sentient beings. The author would like to thank the Synopsys Inc., Rsoft design group and Optiwave Inc. group for providing the OptSim and the OptiSys software simulation tools for optical communications. They would also like to thank reviewers of this paper for their valuable suggestions which greatly improved the manuscript.

REFERENCES

[1] Young Jin Jung, Chang Van Son, Seok Lee, Sangkeun Gil, Hyung Seok Kim and Namkyoo Park "Demonstration of 10 Gbps, all Optical encryption and decryption system utilising SOA XOR logic gates," J. Opt. Quantum Electron., vol.40, pp. 425-430, April 2008.

[2] Jose M. Martinez Canet "Photonic logic gates: boosting all optical header processing in future packet switched networks," pp. 45-65.

[3] G. P. Aggarwal "Fiber Optic Communication Systems," 3rd edition, pp. 250-260.

[4] F. F. Froehlich, C. H. Price, T. M. Turpin, and J. A. Cooke, "All-opticalencryption for links at 10 Gb/s and above," in Proc. IEEE Military Commun. Conf., vol. 4. Atlantic City, NJ, Oct. 2005, pp. 2158–2164.

[5] M. Zhang, L. Wang, and P. Ye, "All optical XOR logic gates: Technologies and experiment demonstrations," IEEE Commun. Mag., vol. 43,no. 5, pp. S19–S24, May 2005.

[6] S Singh, Lovkesh, Xiaohua 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, Dec 2012.

[7] E. Iannone, R. Sabella, L. de Stefano, and F. Valeri, "All-optical wavelength conversion in optical multicarrier networks," IEICE Trans. Commun., vol. 44, no. 6, pp. 716–724, 1996.