Design and Simulation of Physical Layer Security for Next Generation Intelligent Optical Networks

valarmathi marudhai (valarmam@srmist.edu.in)
SRMIST: SRM Institute of Science and Technology
Shanthi Prince
SRM Institute of Science and Technology
Shayna Kumari
SRMIST: SRM Institute of Science and Technology

Research Article

Keywords: Cross Phase Modulation (XPM), Key Generation, Optical Encryption, Pseudo Random Binary Sequence(PRBS), Semiconductor Optical Amplifier(SOA), Wavelength Conversion

Posted Date: June 3rd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-455158/v1

Design and Simulation of Physical Layer Security for Next Generation Intelligent Optical Networks

Valarmathi Marudhai*., Shanthi Prince, and Shayna Kumari

Department of Electronics and Communication Engineering, SRM IST, Kattankulathur, 603203, Tamil Nadu, India.

valarmam@srmist.edu.in, shanthip@srmist.edu.in and shaynakb@srmist.edu.in

**Corresponding Author : ValarmathiMarudhai, Department of ECE, SRM Institute of Science and Technology, Chennai 603203, Tamil Nadu, India.*

Email: valarmam@srmist.edu.in

With the latest technological advancements and attractive features of next generation intelligent optical networks such as high bandwidth, low power consumption, and low transmission loss, etc., they have been considered as most viable solution to satisfy promptly growing bandwidth demands. However, main optical network components bring forth a set of security challenges and reliability issues, accompanied by new vulnerabilities within the network. This paper proposes a new design for an optical encryption and decryption method for enhancing optical network security using p-i-n photodiode which generates Pseudo Random Binary Sequence (PRBS) as a shot noise fluctuations and wavelength converter based design using Semiconductor Optical Amplifier (SOA) based XOR gate which utilizes Cross-Phase Modulation (XPM). The system performance based on Bit Error Rate (BER) and Q factor are analyzed at different data rates for different link lengths up to 100 km using OptiSystem. It is observed that error free transmission with a BER of 10-12 is achieved a data rate of 10Gbps for a link length of only 30 Km for the system with PIN photodiode's shot noise being used for PRBS sequence generation. However, wavelength conversion based system enables transmission of signal at 10Gbps signal up to a link length of 90Km.

Keywords: Cross Phase Modulation (XPM), Key Generation, Optical Encryption, Pseudo Random Binary Sequence(PRBS), Semiconductor Optical Amplifier(SOA), Wavelength Conversion.

1. INTRODUCTION

Today, optical networks evolved with more optical components such as optical amplifiers, optical multiplexers, so that single fiber can transmit data rate in the order of Terabits per second (Tbps). In conventional network, there is an increase in attacks because of store and forward base node. Thus, the fiber optic network has been the network of choice and it is expected to remain so for many generations to come. The next generation optical network will be more intelligent and secured with different security approach. Among the different transport network technologies, because of attractive features of optical networks such as huge bandwidth, ultra-high capacity, low energy consumption and ability to transmit optical signals through a long distance without much signal distortion, etc., they have been considered to be the most promising option [1]. In such networks, optical fiber links carry a large number of wavelength channels which are transported from sources to destinations entirely in the optical domain via all-optical channels called light paths. Each light path can be modulated at a very high data rate up to 100 Gbps [2] without the need of Optical-to-Electrical-to-Optical (O/E/O) processing at intermediate nodes [3].

A. Features of All-Optical Network

All optical networks (AON) are becoming more and more attractive compared to electro-optic and electronic networks due to their high bandwidth and avoiding O/E/O conversions [4]. AONs provide huge transmission capacities exceeding 1Tbps over each fiber while in electronic networks it is in few Gbps [5]. This makes AONs a promising technology to satisfy the ever-increasing demands on throughput, delay, low BER of 10^{-12}, low attenuation loss of 0.2 dB/Km and low noise [6].

In addition, AONs are characterized by their transparency to the transmitted traffic [7]. This refers to the absence of optoelectronic conversion within the network and hence allows the transmission of input traffic as an optical signal without interpretation and regeneration but only with optical amplification. In addition, it avoids the bottleneck with optoelectronic conversion at each

intermediate node. Each node of the AON is equipped with an optical cross connect (OXC) or optical Add/Drop Multiplexer (OADM) both of which are able to pass on the optical signals without O/E/O conversion, thus eliminating electrical delay and therefore reducing power consumption and cost based on the less use of transponders in the networks [8].

B. Security issues in All-Optical Network

Even though, optical networks are expected to be able to satisfy the promptly growing bandwidth demands, in order to make this technology completely usable to the future optical internet many issues need to be resolved. AONs come with new challenges in terms of network security [9]. Security in AONs is an important research area, and it is different from communication and computer security in general. While much of the work in the security area is concentrated on confidentiality, privacy and authentication [10], physical layer security of data in AONs is becoming more and more important [11].

Today's optical networks are highly vulnerable to various forms of attacks, including high-power jamming, physical infrastructure attacks, denial of service, service disruption (degrades QoS), tapping attacks (provides access to unauthorized users) which can be used for eavesdropping and traffic analysis. However, transparency feature of AONs also creates many security vulnerabilities [12, 13, 14, 15, 16].

In particular, AON components have different accessibility and vulnerabilities from electronic components. For example, it is quite easy to tap or jam signals at a specific wavelength by bending an optical fiber slightly and either radiating light out of it or coupling light into it. Moreover, the high data rate feature offered by optical networks makes data extremely sensitive to faults and attacks, even short failures may lead to loss or compromise of large amount of data and revenue. Therefore, the need for securing and protecting AONs has become increasingly significant. Also, Time Division Multiplexed - Passive optical network (TDM-PON) system is vulnerable to various security attacks because of its passive nature and because it lacks the intelligence to detect and counteract security attacks in access networks [14]. In TDM-PON, eavesdropping on downstream data is easily done because the central office broadcast data to all the users. Therefore, the need for securing optical networks has become increasingly significant.

Different techniques have been proposed for enhancing optical network security including optical encryption, optical chaos-based communication [17]. In this paper optical encryption and decryption method for enhancing optical network security using pseudorandom binary sequence (PRBS) generated from the shot noise fluctuations in p-i-n photo diode and XOR gate utilizing XPM in SOA is proposed and analyzed in this work. The organization of paper is as follows: Section 2 presents our proposed encryption and decryption scheme along with its implementation followed by simulation results. Section 3 concludes the paper.

2. Optical Encryption and Decryption for Enhancing Network Security

Over the past few years, there has been more concern about data security of optical networks because of brisk increase in optical network capacity. Among several techniques, optical encryption is considered as good candidate to facilitate secure communication without compromising the processing speed [18].

Encryption and Decryption have been utilized several years by governments and defense forces to secure much of world's most sensitive data. Encryption is the process of transforming original message to an unrecognizable or encoded form by using an encryption algorithm especially to hide or lock original information from unauthorized users.

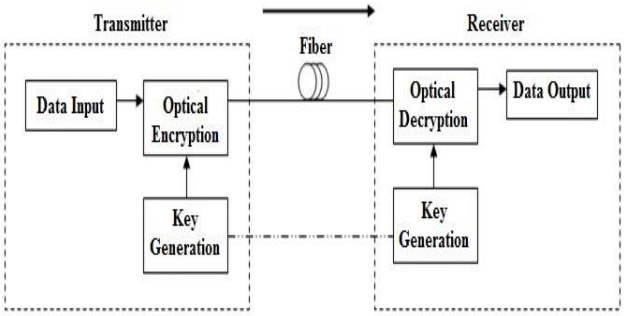

Fig. 1. Block Diagram of Secured Optical Communication System

The simplified block diagram of secured optical communication which involves optical encryption and decryption is shown in Fig 1. The schematic block diagram of the proposed Encryption and Decryption is shown in Fig. 2. Input message is referred to as plaintext and encoded information is referred to as ciphertext. The whole process needs a key stream which is generated by PRBS. All optical XOR used as a building block of all optical encryption decryption system which utilizes the cross phase modulation. By applying XOR operation twice, the original message is recovered at the receiver, i.e the ciphertext is converted back into plaintext.

The entire process generally needs an encryption algorithm and a keystream. Data protection, data privacy, security, and integrity of a system relies directly on two important parameters: strength of algorithm and length of key.

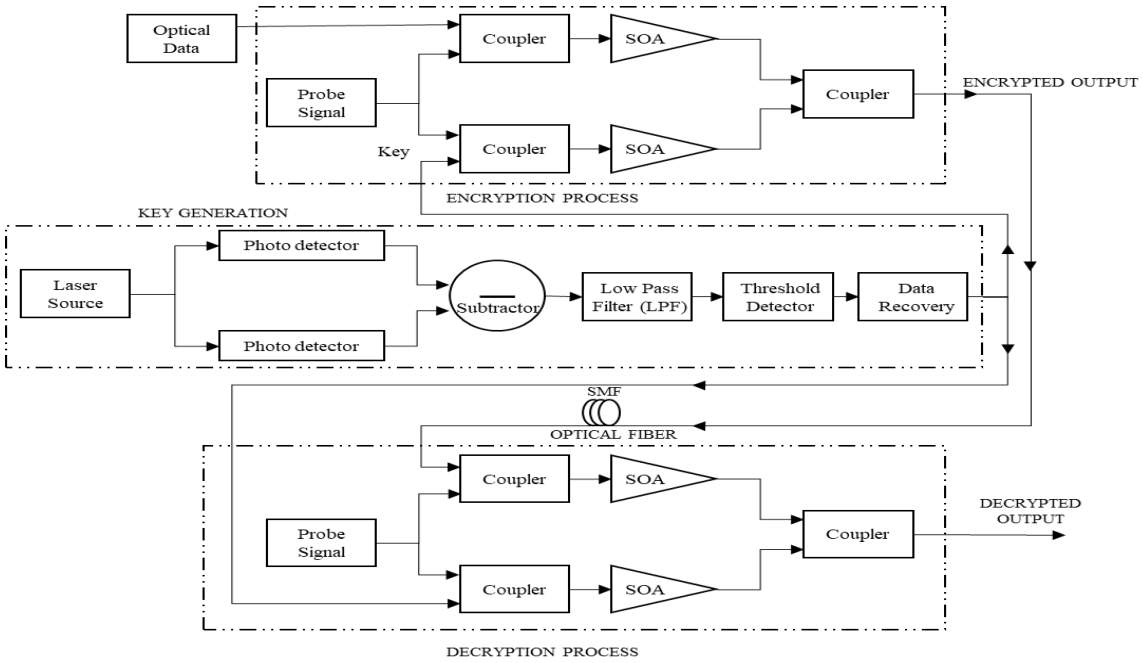

Fig. 2. Proposed Encryption and Decryption Scheme

A. Key generation Using PRBS generator and simulation setup

In encryption and decryption, the keystream plays a vital role and there are many methods for generation of pseudo random numbers which are based on either simple mathematical or physical sources [19]. In the simulation layout of the proposed design is shown in Fig. 3, PRBS is generated from the shot noise fluctuations in p-i-n photodiode.

The optical signal from CW laser source is divided equally by a beam splitter into two equal optical signals of power P_{in}, which is then made to fall on p-i-n photodiodes in the upper and lower arm, respectively. Photodiodes convert the optical signal falling on it into current proportional to the incident optical power and in addition the current due to fluctuations of the incident power.

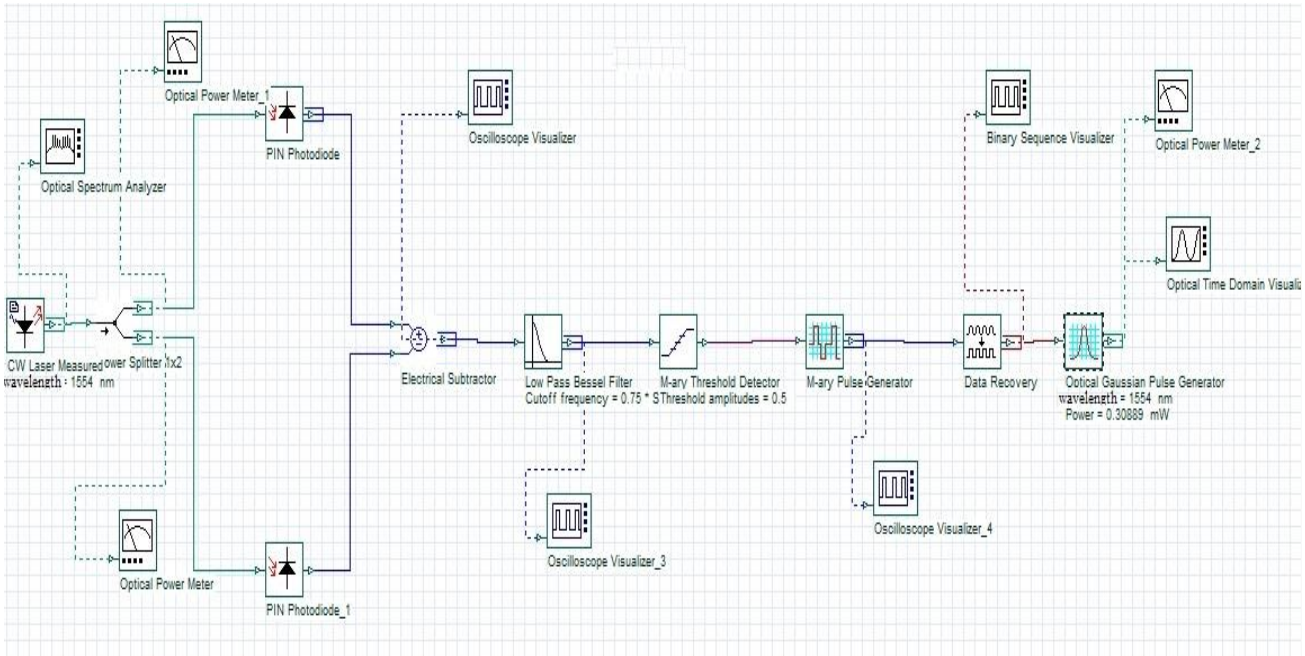

Fig. 3. Simulation Layout of PRBS Generator

Total current generated by photodiode can be written in the form

$$I(t) = \bar{I} + i_s(t) \quad \textbf{(1)}$$

where, I is the average current or photocurrent (in Ampere), $i_s(t)$ is the current fluctuation related to shot noise.

$\bar{I}$ can be calculated as

$$\bar{I} = RP_{in} \quad \textbf{(2)}$$

where, R is the responsivity of photodetector (A/W), and P_{in} is the incident optical power (Watts).

Autocorrelation and spectral density are related by

$$< i_s(t) i_s(t+\tau) >= \int_{-\infty}^{\infty} S_s(f) \exp(2\pi i f \tau) df \quad \textbf{(3)}$$

where $S_s(f)$ is the two-sided spectral density.

The noise variance is given by [20]

$$\sigma_s^{\,2} < i_s^{\,2}(t) >= \int_{-\infty}^{\infty} S_s(f) df = 2q\bar{I}\Delta f \quad \textbf{(4)}$$

where, Δf is the effective noise bandwidth of the receiver, and q is the charge of electron.

The total shot noise is then given by [20]

$$\sigma_s^{\,2} = 2q(\bar{I} + I_d)\Delta f \quad \textbf{(5)}$$

where, I_d is dark current.

However, both the photodiodes generates same photocurrent and different shot noise since fluctuating currents will be generated randomly.

The outputs of photodiodes are then subtracted in order to cancel out photocurrent so that only fluctuating current or quantum noise is present at subtractor output. The randomness of generated sequence can be checked by using monobit test [21] and is calculated as

$$P = erfc\left[\frac{S_{abs}}{\sqrt{2}}\right] \quad , \quad \textbf{(6)}$$

where, $erfc$ is the complementary error function, and S_{abs} is test statistic and is given by

$$S_{abs} = \frac{|S_n|}{\sqrt{n}} \quad \textbf{(7)}$$

where, S_n is the addition of all the bits of sequence after converting zeros and ones to values of the -1 and +1 respectively, and n is the number of bits in a sequence. After calculating the value of P the decision for randomness is made such that if

$$P = \begin{cases} P \geq 0.01, & Random\ sequence \\ else, & Non\ random\ sequence \end{cases} \quad \textbf{(8)}$$

Table 1. Simulation Results for Generation for Random Sequences

Rounds	Bits Obtained
1	0100101001
2	1101000101
3	0110010100
4	0101111100
5	1110100110
…….	…….
98	1010000011
99	0100110100

Using the generated sequence the test for randomness is performed. The generated sequence shown in Table 1 is found to be random as the obtained value for P is 0.5271. The randomness of generated sequence is discussed in our publication [22].

B. XOR based Encryption Algorithm

All optical XOR logic operation has been typically used as encryption algorithm to achieve secured data transmission. All optical XOR gate has several advantages such as immunity to electromagnetic signature, low latency, high extinction ratio etc.

The two optical signals (Data stream and Probe signal) at same or different wavelengths are coupled appropriately using 3dB couplers arranged in SOA - MZI configuration as shown in Fig. 2. In the upper arm optical data is coupled with probe signal and in the lower arm probe signal is coupled with keystream which are then launched into two SOAs in the upper and lower arm respectively. The incoming data pulses or the control signal produces the carrier density variation within SOA which provides change in refractive index of nonlinear medium and phase modulation of CW beam occurs in the upper arm depending on the control signal. Similarly, in the lower arm phase modulation is carried on due to keystream. Then, two beams are combined by coupler after passing through SOAs. Depending on the phase difference between two beams, they will interfere constructively or destructively and therefore all optical XOR operation is performed on two input data streams.

The rate equations from which the associated nonlinear optical effects and dynamics of carrier density in SOA can be analyzed using [23].

$$\frac{dN}{dt} = J - \frac{N}{\tau} - g_d(N - N_{tr})\frac{S_c}{hw_c} - g_d(N - N_{tr})\frac{S_p}{hw_p} \quad \textbf{(9)}$$

$$\frac{dS_c}{dz} = \Gamma g_d(N - N_{tr})S_c - \alpha S_c \quad \textbf{(10)}$$

$$\frac{dS_p}{ds} = \Gamma g_d(N - N_{tr})S_p - \alpha S_p \quad \textbf{(11)}$$

where, N is the carrier density, J is the rate of carrier injection through bias current, N_{tr} is the transparency carrier density, S_C is the control light power, Sp is the probe light power, w_C is the control light frequency, w_p is the probe light frequency, τ is the carrier lifetime, g_d is differential gain, h is the reduced Planck's constant, Γ is the optical confinement factor, and α is the optical loss coefficient including absorption and scattering loss. The intensity modulation in the intensity of the probe light can be obtained from above equations.

However, the phase shift experienced by the probe signal is given by

$$\frac{d\phi}{dt} = -\frac{1}{2}\alpha_N \Gamma g_d (N - N_{tr}) \quad \textbf{(12)}$$

where, ϕ is the phase of probe light and α_N is line width enhancement factor.

C. XOR based Decryption Algorithm

The two optical signals (Cipher Text and Probe signal) at same or different wavelengths are coupled appropriately using 3dB couplers arranged in SOA - MZI configuration as shown in Fig.2. In the upper arm encrypted optical data is coupled with probe signal and in the lower arm probe signal is coupled with keystream which are then launched into two SOAs in the upper and lower arm respectively. The cipher text streams produces the carrier density variation within SOA which provides change in refractive index of nonlinear medium and phase modulation of CW beam occurs in the upper arm depending on the encrypted signal. Similarly, in the lower arm phase modulation is carried on due to keystream. Then, two beams are combined by coupler after passing through SOAs. Depending on the phase difference between two beams, they will interfere constructively or destructively and therefore all optical XOR [24, 25, 26] operation is performed on encrypted signal, by which we get a decrypted signal or plain text. Same mathematical analysis holds good for the decryption process.

D. Simulation of Secured Optical communication System

Based on the schematic block shown in Fig 2, the system is simulated in Optisystem. The layout of which is shown in Fig. 4. The design comprises of subsystem of XOR gate and generated key. The simulation parameters are tabulated in Table 2.

The optical data (message signal) at the wavelength of 1540nm is encrypted into cipher text using the generated key and transmitted. The encryption is carried out based on XOR operation. The cipher text which is transmitted is received at the receiver and using the same key, decrypted using XOR operation to recover the original data.

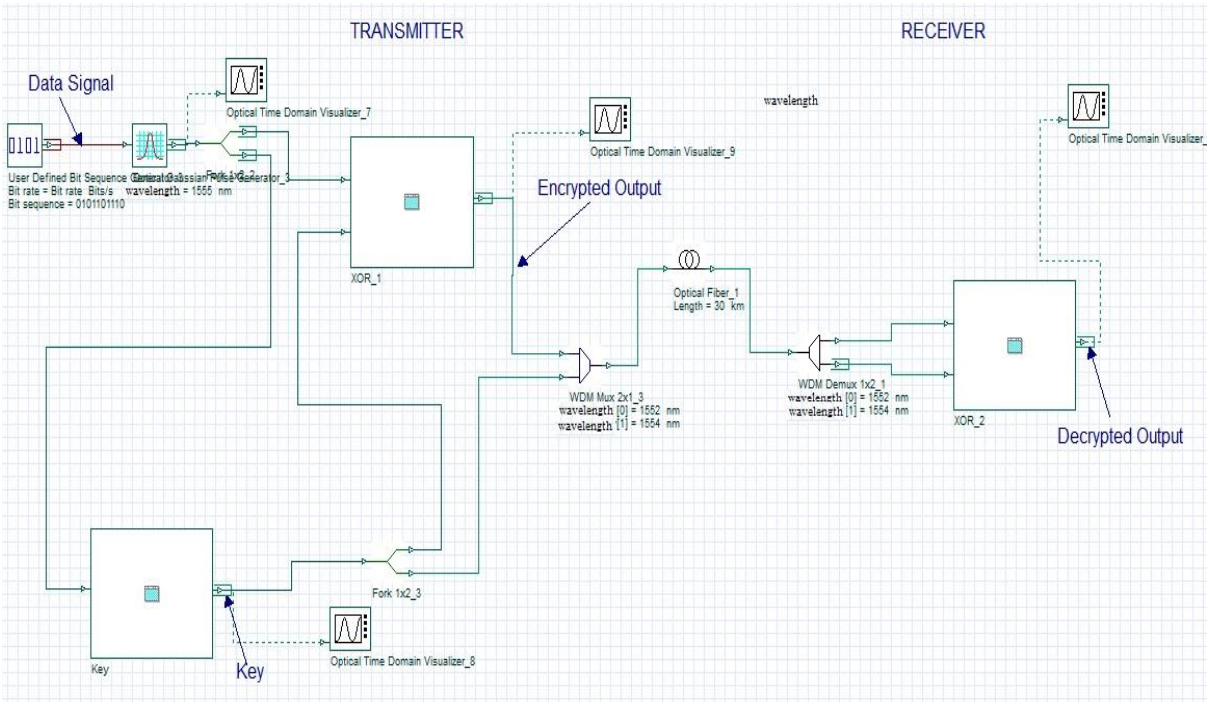

Fig. 4. Schematic Layout of the Proposed Design in Optisystem

Table 2. Simulation Parameters of the Proposed Design

Symbol	Parameter	Value
λ	Wavelength (Control Signal)	1540nm
	PD type	PIN photo diode
V	Threshold Amplitude	0.5V
p	Optical Power	0.38 mw
	Data rate	10 Gbps
SOA Specifications		
I	Injection Current	0.5 A
L	Amplifier length	500 µm
w	SOA Active area width	3 µm
d	Active area thickness	0.08 µm
Γ	Optical confinement factor	0.3
g_d	Differential gain	27.8e-021 m^2
N_{tr}	Transparency carrier density	1.4e+024 m^3
α_N	Linewidth enhancement factor	5

The simulation is carried out for different data rates and link lengths and the performance of the system is analyzed based on BER and Q factor.

1. Performance Analysis

The input Message (0101101110) at 1540nm (Fig. 5a) to be transmitted at a data rate of 10Gbps is encrypted using the key (1111001001) at 1540 nm (Fig. 5b) generated by PRBS generator. As explained earlier XOR operation is performed to get the encrypted signal (1010100111) at 1540nm (Fig. 5c). This encrypted signal is transmitted and upon reception is decrypted using XOR operation to get the original signal (0101101110) as shown in Fig. 5d.

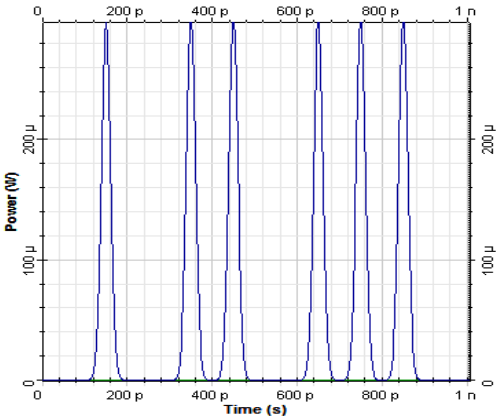

Fig. 5a. Input Data Sequence 0101101110

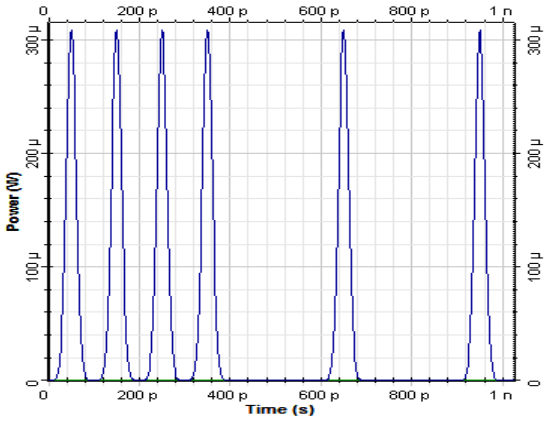

Fig. 5b. Generated Key 1111001001

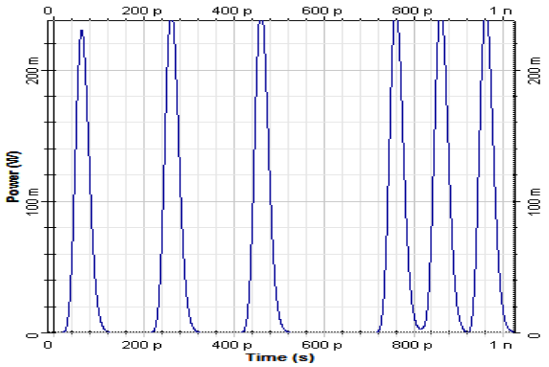

Fig. 5c. Encrypted signal 1010100111

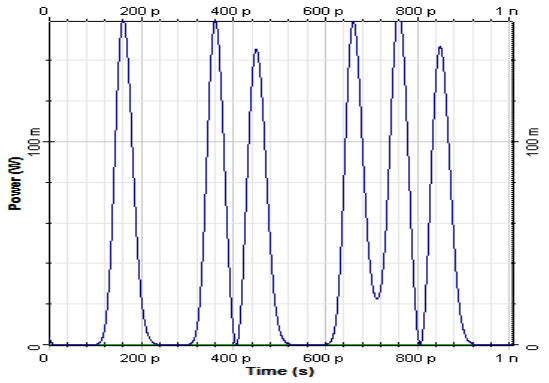

Fig. 5d. Decrypted signal 0101101110

The performance parameters of the proposed optical encryption and decryption system are listed in Table 3. Q-factor and the Bit-Error Rate (BER) are most commonly used performance measures. Q-factor is another way to represent the signal to noise relationship. In optical system, the BER is typically too small to measure and hence Q factor is more suitable to be used. It represents signal quality and allows simplified analysis of system performance. Obviously, the larger the Q is, the less will be the bit error rate. Bit error rate and Q factor relationship is given as

$$\text{BER}=\frac{1}{2}\text{erfc}\left(\frac{Q}{\sqrt{2}}\right)\approx\frac{1}{\sqrt{2\pi}\,Q}\exp\left(-\frac{Q^2}{2}\right) \quad \textbf{(13)}$$

Table.3. Performance parameters of the proposed secured Optical communication system based on XOR encryption and decryption at a data rate of 10 Gbps

Fiber length (Km)	Encrypted signal		Decrypted signal	
	Max. Q-factor	Min. BER	Max. Q-factor	Min. BER
10	60.395	0.2165e-90	50.374	0.3892e-75
20	35.365	0.4962e-65	19.486	0.8427e-30
30	13.583	0.3726e-20	6.964	0.9392e-11

Simulation results are analyzed for 10, 20 and 30km of fiber length. As the optical fiber length i.e. distance between transmitter and receiver, increases BER increases and Q-factor decreases. When optical fiber length of 30km is used, the minimum BER and maximum Q-factor of encrypted signal are 0.3726e-20 and 13.583, respectively whereas that of decrypted signal are 0.9392e-11 and 6.964 respectively at 10 Gbps. Implemented encryption and decryption system gives satisfactory result for optical fiber length up to 30km.

3. All Optical Encryption and Decryption using wavelength Conversion

The schematic of proposed design is shown in Fig. 6. In this work, SOA-MZI structure based on XPM is utilized to realize all optical XOR logic operation [27, 28]. The optical data streams (P_i) and security key (Ki) which is generated by delaying data signal (P_i) at same wavelength λ_1 (1554nm) are launched into two SOAs. A CW signal at different wavelength λ_2 (1552nm) is split into two beams which are injected into upper and lower branch of MZI respectively. The data stream produces the carrier density variation within SOA which provides change in refractive index which leads to phase modulation of CW beam. Then, two beams are combined by coupler after passing through SOA. Depending on the phase difference between two beams, they will interfere constructively or destructively and give encrypted output at the CW laser wavelength λ_2 (1552nm)

Decryption of encrypted data is achieved by first performing the wavelength conversion of delayed signal (K_i) which is at wavelength λ_1 to the encrypted data (C_i) wavelength λ_2 and then performing XOR logic operation between C_i and K_i, i.e., $P_i = C_i$ XOR K_i.

In the proposed design, all optical wavelength conversion is the key for encryption and decryption along with XOR operation. By utilizing the nonlinear characteristics, XPM wavelength conversion is achieved. XPM relies on the dependency of the refractive index of the carrier density in the active region of the SOA. An incoming signal that depletes the carrier density will modulate the refractive index and thereby result in phase modulation of a CW signal, resulting in wavelength conversion. Data initially carried by wavelength λ_1 will be completely preserved and transmitted further along at the new wavelength λ_2. The simulation layout for all optical wavelength conversion using cross phase modulation XPM is shown in Fig. 7.

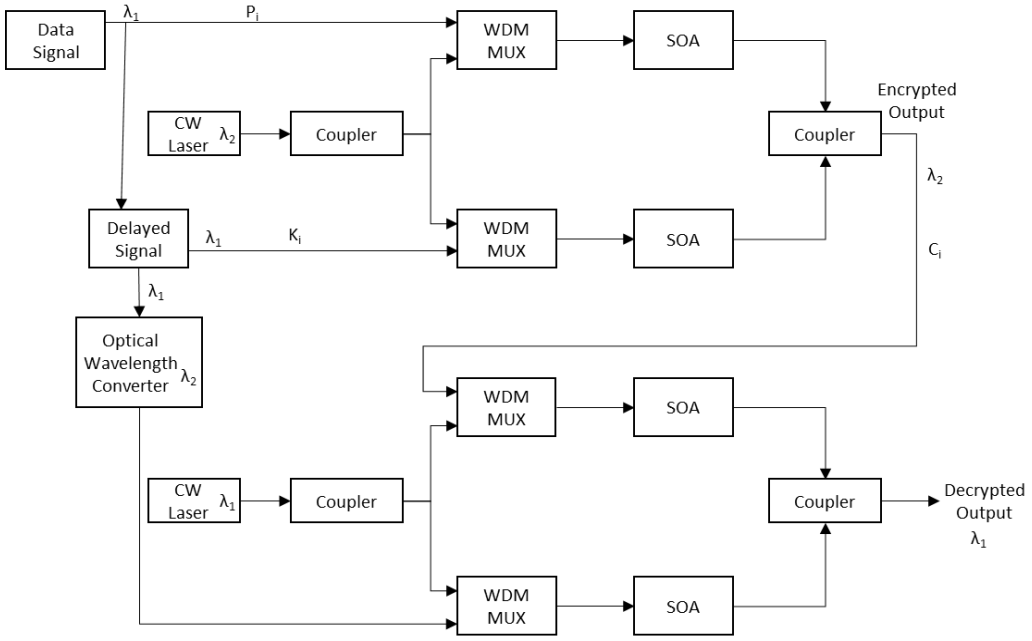

Fig. 6. Proposed All Optical Encryption and Decryption based on Wavelength Conversion

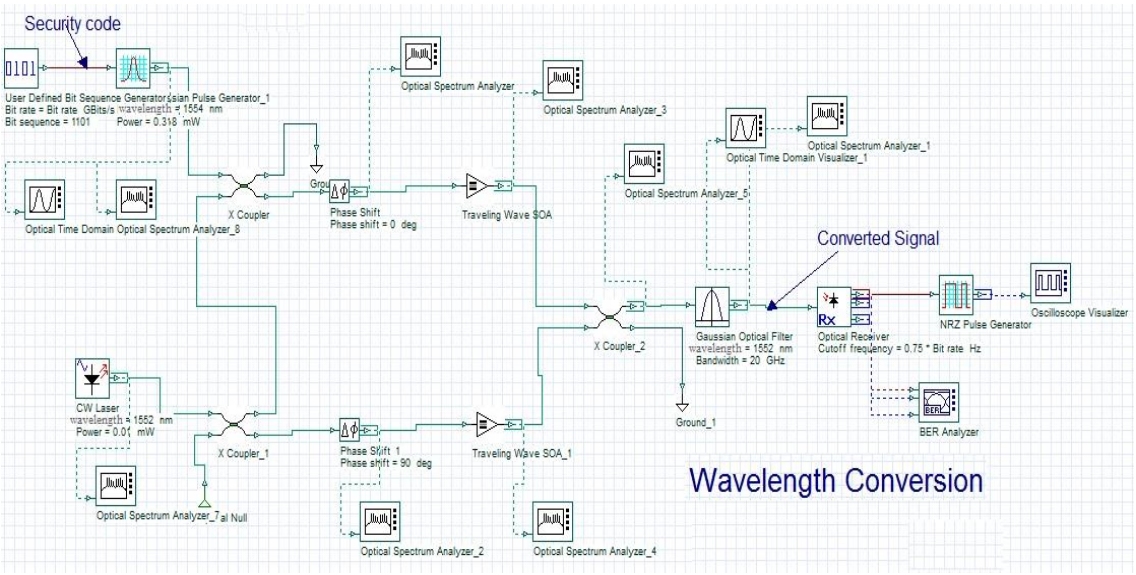

Fig. 7. Simulation Layout for XPM based Wavelength Converter

The design uses SOA-MZI architecture. Wavelength conversion is achieved in the following way: a delayed signal or security code at the wavelength λ_1 is coupled into upper arm of the MZI along with the data signal. As the signal propagates through the upper SOA, it modulates the carrier density, causing a change in the refractive index, and thereby a phase modulation. CW light at the wavelength λ_2 is sent through coupler acting as splitter, and is subsequently split equally and sent to the two interferometer arms. In the lower arm the CW light will experience a constant phase change according to the biasing of the lower SOA. However, in the upper arm the CW light will experience a phase change depending on the bit pattern of the input data signal. Thus, the CW light will combine constructively or destructively at the interferometer output depending on the modulation of the input signal. In this way, the bit pattern of the security code is transferred to the CW light, which is selected at the output using a filter and one of these wavelength as a new signal carrier and the initial data will be completely preserved and transmitted along at the new wavelength λ_2. After performing wavelength conversion at the receiver end, XOR operation is performed between security code and encrypted output both at same wavelength λ_2 to recover the original input message.

A. Simulation of Wavelength conversion based Encryption and Decryption

The simulation layout for optical encryption and decryption is shown in Fig. 8. Here, two XOR gate, a key and a wavelength converter are used to perform encryption and decryption at transmitter and receiver side respectively. The input data to be transmitted and key are fed to XOR gate. By applying bitwise XOR operation between every bit in the signal and a given key, encoded data is obtained at the output of XOR gate. At the receiver, after performing the wavelength conversion of the key, XOR operation is again performed between encoded data and the key, the original data is obtained at the receiver. Simulation parameters are displayed in Table 4.

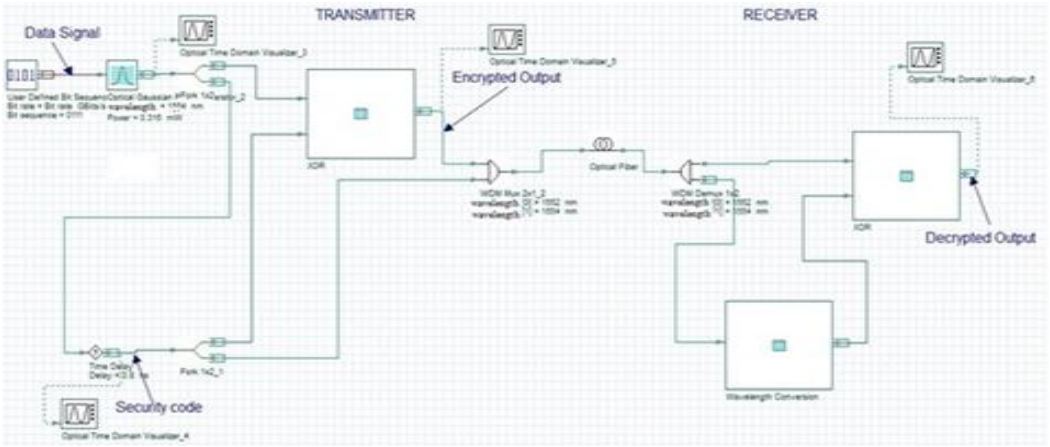

Fig. 8. Simulation Layout for Encryption and Decryption Process using Subsystem

Table 4. Simulation Parameters of the Proposed Design

Symbol	Parameter	Value
λ_1	Message wavelength	1554nm
λ_1	Key wavelength	1554nm
λ_2	Encrypted output wavelength at the Transmitter side	1552nm
λ_2	Key wavelength using XPM ar Receiver side	1552nm
λ_1	Decrypted output wavelength	1554nm
	Data rate	2.5Gbps , 5Gbps and 10 Gbps
d	Transmission length	10km to 100km
P	Power	0.38mw

The optical signal representation and optical spectrum of the input data sequence (0111) at 1554nm to be transmitted are shown in Fig. 9a and Fig. 9b respectively. The data signal is generated at bit rate of 2.5Gbps, 1554nm wavelength (192.91 THZ frequency). The optical signal representation and optical spectrum of the security key (1101) at 1554nm generated by delaying data signal are shown in Fig. 9c and Fig. 9d respectively. Therefore, the security code is also generated at bit rate of 2.5 Gbps, 1554 nm wave- length (192.91 THz frequency).

The resultant encrypted signal (1010) is obtained at 1552 nm wavelength (192.16 THz frequency) after performing XOR operation between data signal (0111) and security key (1101) both at 1554 nm wavelength (192.91 THz frequency). The optical signal representation and optical spectrum of encrypted signal are shown in Fig. 9e and Fig. 9f respectively. From Fig. 9e, it can be observed that the encrypted signal wavelength is different from that of key and message. Hence it is clear that the encrypted message is transmitted at different wavelength.

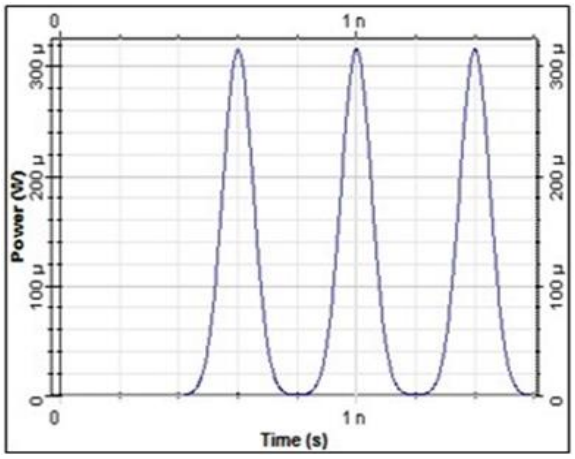

Fig. 9a. Optical Data Signal (0111) At 1554nm

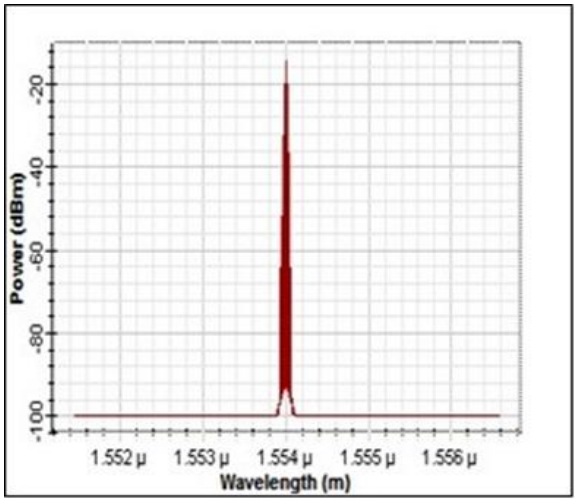

Fig. 9b. Optical Spectrum of data signal

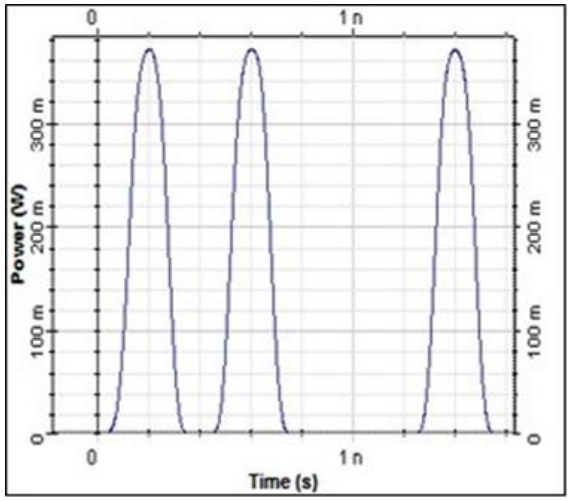

Fig. 9c. Optical Key (1101) at 1554nm

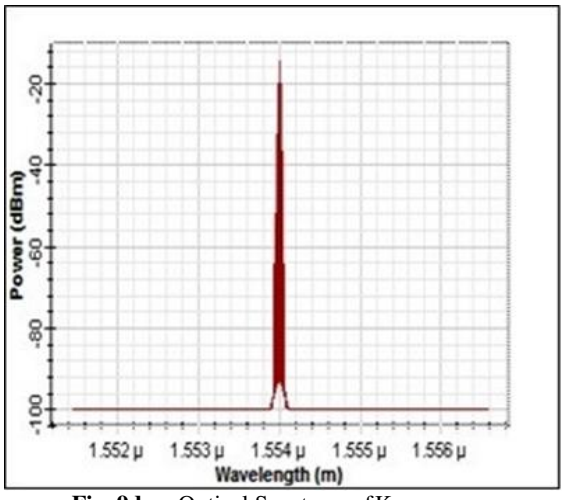

Fig. 9d. Optical Spectrum of Key

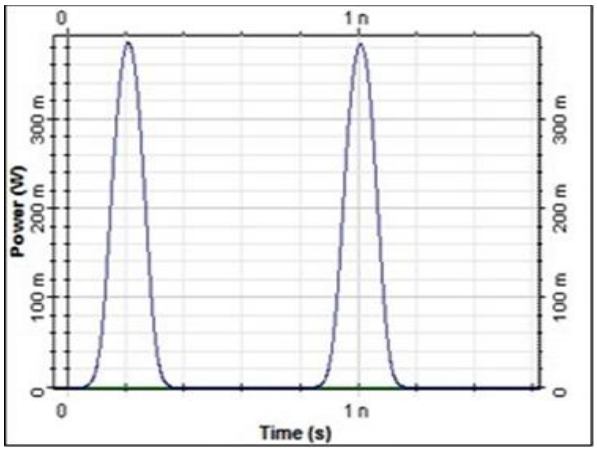

Fig. 9e. Encrypted Output (1010) at 1552nm

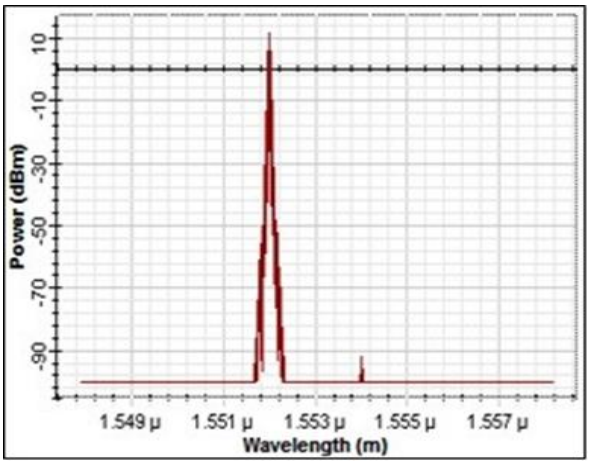

Fig. 9f. Optical Spectrum of Encrypted Output

At the receiver side by using cross-phase modulation (XPM) based wavelength converter, the wavelength of security key is changed to 1552 nm without altering the key data (1101) carried by signal. The optical signal representation and optical spectrum of the security key (1101) after performing wavelength conversion are shown in Fig. 10a and Fig.10b respectively.

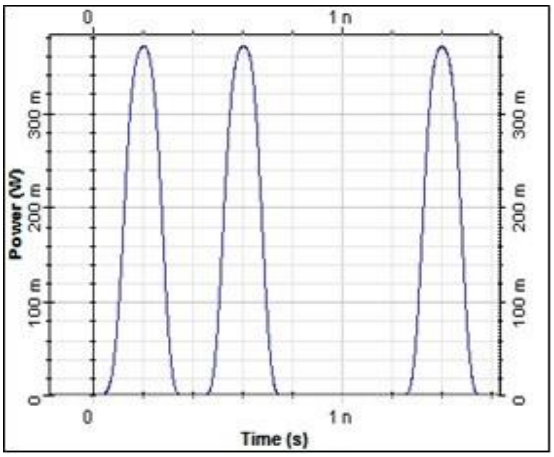

Fig. 10a. Optical Key (1101) at 1552nm

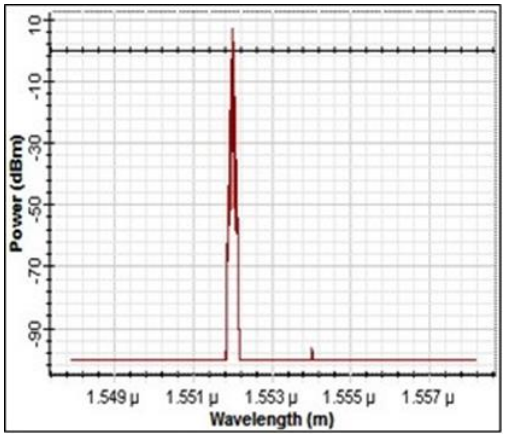

Fig. 10b. Optical Spectrum of Key

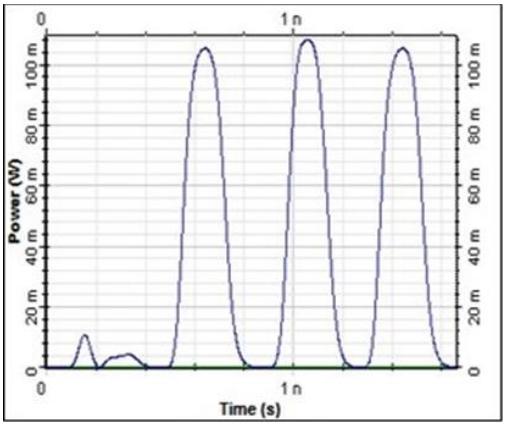

Fig. 10c. Decrypted Output 0111 at 1554nm

After performing XOR operation between encrypted output (1010) and security key (1101) both at 1552 nm wavelength, the original data (0111) is obtained at 1554 nm wavelength.

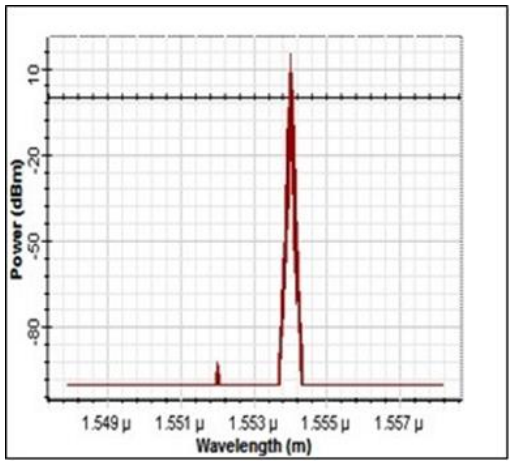

Fig. 10d Optical Spectrum of Decrypted Output

The optical signal representation and optical spectrum of decrypted signal are shown in Fig. 10c and Fig. 10d respectively. From Fig. 10c, it can be observed that the decrypted output obtained at the same wavelength at 1554nm as the original message wavelength.

B. Performance Analysis

The system parameters such as the Q-factor and BER values are analyzed by varying the data rate for different transmission distance from 10 km to 100 km using OptiSystem. As transmitted bit rates increases, BER increases and hence degrades the Q-factor. Also, for smaller transmission ranges, higher bit rates gives affordable BER and Q- factor; but as range increases higher data rates may not be preferred. The Q-factor v/s Transmission distance for different data rates is given in Fig. 11 which indicates that for 100 Km of transmission distance error free transmission and good quality of the signal reception at the receiver is achieved at 10 Gbps. For optimum Q factor and lower data rates more than 100 Km fiber length can be used.

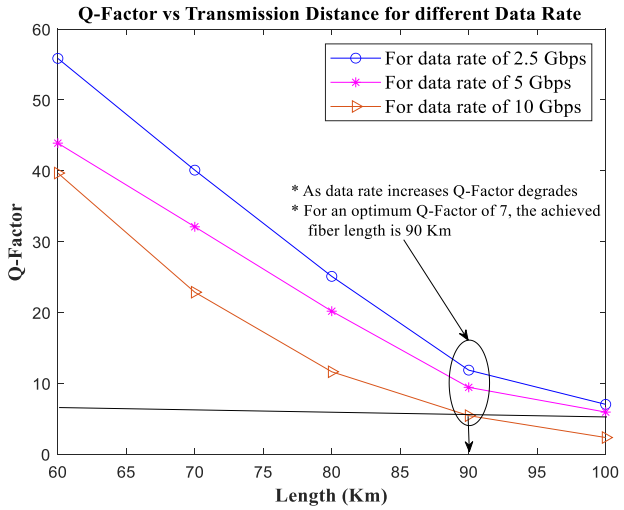

Fig. 11.Q-Factor vs Transmission Distance for Different Data Rate

Table 5. Q-Factor and BER for a link length of 90Km

Data Rate (Gbps)	Q- Factor	BER
2.5	11.853	6.959e-55
5	9.426	4.876e-18
10	5.432	1.984e-9

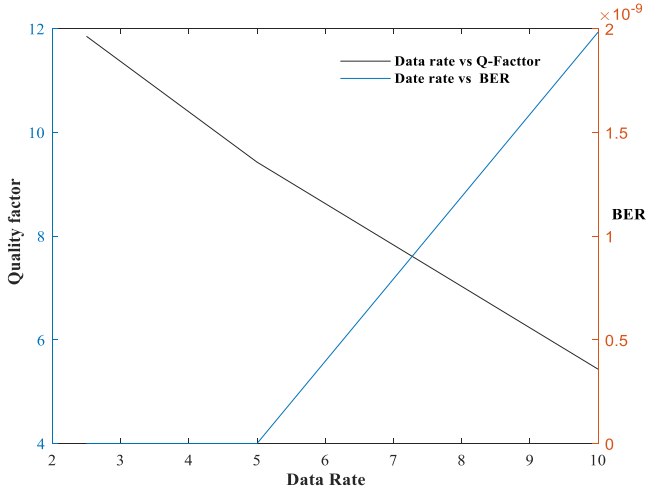

Fig. 12. Q-Factor and BER for Link Length of 90 km

Table 5 lists the Q- Factor and BER for a link length of 90 km for different data rates. From Fig. 12, the Q Factor and BER for link length of 90 km are analyzed and indicate that as transmission bit rates increases, the Q-factor degrades and BER increases. For 90 km of transmission distance, error free transmission and good quality of the signal reception at the receiver is achieved at different data rates.

5. CONCLUSIONS

In this paper, two different methods are presented to achieve optical encryption and decryption. In the first method, pseudorandom binary sequence (PRBS) generated from shot noise fluctuations in p-i-n photodiode is utilized. Implemented encryption and decryption system gives satisfactory result for optical fiber of length upto 30 Km at 10Gbps. Therefore, can be used to protect the integrity of downstream data in optical access networks. The results show that decryption by an eavesdropper becomes impossible because large number of possible permutations of different parameters are used in our system.

In the Second method, optical encryption and decryption system using wavelength converter is designed in OptiSystem simulation. The performance analysis of the system, in terms of received signal Q-factor and BER, and its dependence on system parameters are analyzed based on the simulation results. The obtained results indicate that for 90 Km of transmission distance transmission with a BER of 10e-9 at the receiver is achieved at 10 Gbps. In future different techniques networks such as chaos-based communication to enhance the robustness of data transmission against narrow band interference can be designed.

Declarations

Funding There is no funding provided to prepare the manuscript.

Conflict of Interest There is no conflict of Interest between the authors regarding the manuscript preparation and submission.

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors.

Informal Consent Informed consent was obtained from all individual participants included in the study.

References

1. Alferness, R. C. (2000). “The all-optical networks.” In Proc. of IEEE International Conference on Communication Technology, Vol. 1, 14–15.

2. Berthold, Joseph, et al. "Optical networking: past, present, and future." *Journal of lightwave technology* 26.9 (2008): 1104-1118.

3. Marciniak, Marian. "Optical transparency in next generation IP over all-optical networks." *Proceedings of 2001 3rd International Conference on Transparent Optical Networks (IEEE Cat. No. 01EX488)*. IEEE, 2001.

4. Medard, M. (1998). “Secured optical communication.” In Proc.of IEEE Lasers and Electro-Optics Society Annual Meeting, 323–324.

5. Medard, Muriel, et al. "Security issues in all-optical networks." IEEE network 11.3 (1997): 42-48.

6. Furdek, Marija. "Physical-layer attacks in optical WDM networks and attack-aware network planning." *European Journal of Operational Research* 178.2 (2011): 1160-1167.

7. Mas, Carmen, Ioannis Tomkos, and Ozan K. Tonguz. "Failure location algorithm for transparent optical networks." *IEEE Journal on Selected Areas in Communications* 23.8 (2005): 1508-1519.

8. Rejeb, R., Leeson, M. I., and Tomkos, I. (2010). “Control and management issues in all-optical networks.” IEEE Journal on Selected Areas in Communications, 5(2), 132–139.

9. Rejeb, R., et al. "Securing all-optical networks." *Proceedings of 2003 5th International Conference on Transparent Optical Networks, 2003.*. Vol. 1. IEEE, 2003.

10. Thomas, Stephen, and David Wagner. "Insecurity in ATM-based passive optical networks." *2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No. 02CH37333)*. Vol. 5. IEEE, 2002.

11. Patel, Dimpal S., and Parita N. Pancholi. "Security issues and attack management in AON-A review." *2012 1st International Conference on Emerging Technology Trends in Electronics, Communication & Networking*. IEEE, 2012.

12. Rejeb, Ridha, Mark S. Leeson, and Roger J. Green. "Multiple attack localization and identification in all-optical networks." *Optical Switching and Networking* 3.1 (2006): 41-49.

13. Rejeb, Ridha, Mark S. Leeson, and Roger J. Green. "Fault and attack management in all-optical networks." *IEEE Communications Magazine* 44.11 (2006): 79-86.

14. Shaneman, Keith, and Stuart Gray. "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection & prevention." *IEEE MILCOM 2004. Military Communications Conference, 2004*. Vol. 2. IEEE, 2004.

15. Lazzez, Amor. "Notice of Violation of IEEE Publication Principles: All-optical networks: Security issues analysis." *IEEE/OSA Journal of Optical Communications and Networking* 7.3 (2015): 136-145.

16. Kartalopoulos, Stamatios V. *Security of information and communication networks*. Vol. 15. John Wiley & Sons, 2009.

17. Argyris, Apostolos, et al. "Chaos-based communications at high bit rates using commercial fibre-optic links." *Nature* 438.7066 (2005): 343-346.

18. Fok, M. P., & Prucnal, P. R. (2009). All-optical encryption based on interleaved waveband switching modulation for optical network security. Optics letters, 34(9), 1315-1317.

19. Tawfeeq, Shelan Khasro. "A random number generator based on single-photon avalanche photodiode dark counts." *Journal of Lightwave Technology* 27.24 (2009): 5665-5667.

20. Agrawal, G. P. (2012). Fiber-optic communication systems (Vol. 222). John Wiley & Sons.

21. Bassham III, Lawrence E., et al. *Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications*. National Institute of Standards & Technology, 2010.

22. Kumari, Shayna, M. Valarmathi, and Shanthi Prince. "Generation of pseudorandom binary sequence using shot noise for optical encryption." *2016 International Conference on Communication and Signal Processing (ICCSP)*. IEEE, 2016.

23. Ishikawa, Hiroshi, ed. *Ultrafast all-optical signal processing devices*. John Wiley & Sons, 2008.

24. Zhang, M., Wang, L., and Ye, P. (2008). “All-optical xor logic gates: Technologies and experiment demonstrations.” IEEE Communications Magazine, 43(5), 19–24.

25. Kang, I., C. Dorrer, and J. Leuthold. "All-optical XOR operation of 40 Gbit/s phase-shift-keyed data using four-wave mixing in semiconductor optical amplifier." *Electronics Letters* 40.8 (2004): 496-498.

26. Ya-Ping, Wang, et al. "An encryption-decryption method using XOR gate based on the XPM between O-band and C-band light waves." *Chinese Physics Letters* 26.7 (2009): 074219.

27. Sarker, B. C., T. Yoshino, and S. P. Majumder. "All-optical wavelength conversion based on cross-phase modulation (XPM) in a single-mode fiber and a Mach-Zehnder interferometer." *IEEE Photonics Technology Letters* 14.3 (2002): 340-342.

28. Honzatko, Pavel. "All-optical wavelength converter based on fiber cross-phase modulation and fiber Bragg grating." *Optics communications* 283.9 (2010): 1744-1749.

Dr. Shanthi Prince received the M.S. degree in biomedical engineering from the Indian Institute of Technology, India, in 1995 and the Ph.D. degree in bio-photonics from SRM University, India, in 2010. Since 2011, she is a Professor in Electronics and Communication Engineering Department, SRM Institute of Science and Technology, Chennai, India. She is the recipient of Career Award for Young Teacher (CAYT) from AICTE, New Delhi, India in the year 2005. She is the author of five book chapters, and more than 40 research articles. Her research interests include diffuse reflectance spectroscopy studies on tissues, development of non-invasive instrumentation for biomedical applications, underwater optical wireless communication, Optical wireless channel modeling, optical security, OCDMA, and Passive Optical Networks. She is doing funded projects from DRDO, ISRO. She has patents, coauthored over 130 journals and conference publications. She is also a journal reviewer for Elsevier, Springer, and OSA.

M.Valarmathi is currently an Assistant professor at SRM University, ECE department, Chennai, India. She received her B.Tech ECE in 1998 from Regional Engineering College (NIT-Trichy), Tiruchirappalli, Tamilnadu, India and M.Tech VLSI design from SASTRA University, Tanjore, Tamilnadu, India. Currently she is doing Ph.d in hardware security in VLSI and Optical. Primary areas of research includes signal processing, ASIC design of hardware security in VLSI and optical cryptography.

Shayna Kumari received the Master's degree in Communication Systems from SRM Institute of Science and Technology in 2016. She is currently working towards a Ph.D degree in the department of Electronics and Communication Engineering, SRM Institute of Science and Technology. Her research interests include wireless optical communication, optical cryptography, and integrated photonics.

Figures

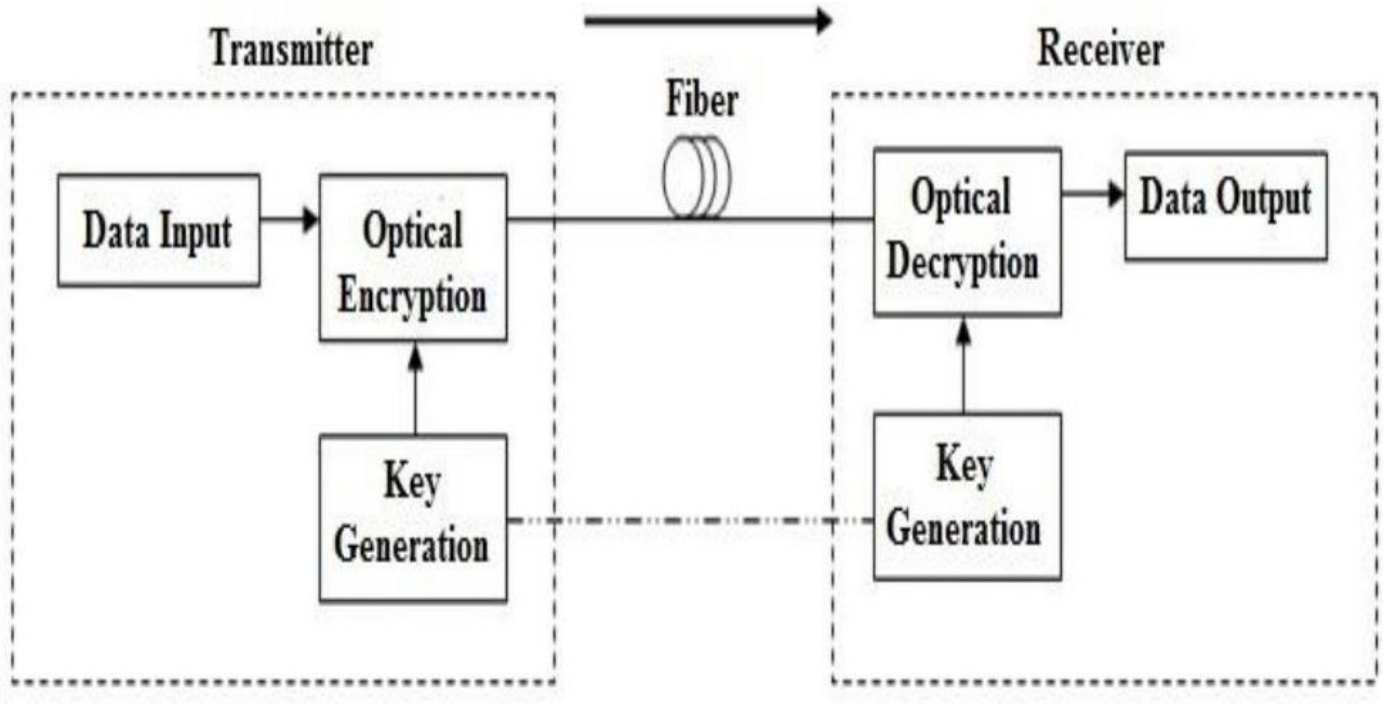

Figure 1

Please see the Manuscript PDF file for the complete figure caption

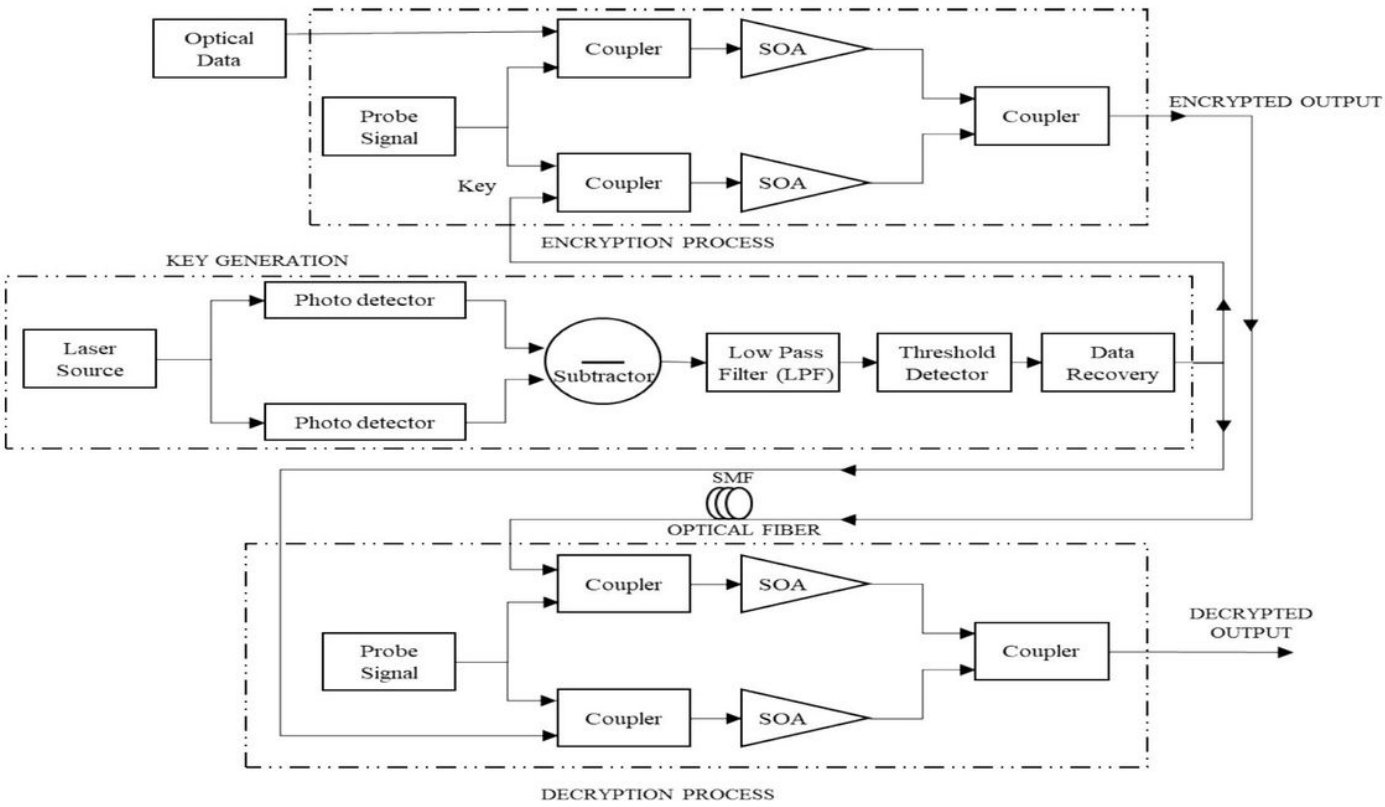

Figure 2

Please see the Manuscript PDF file for the complete figure caption

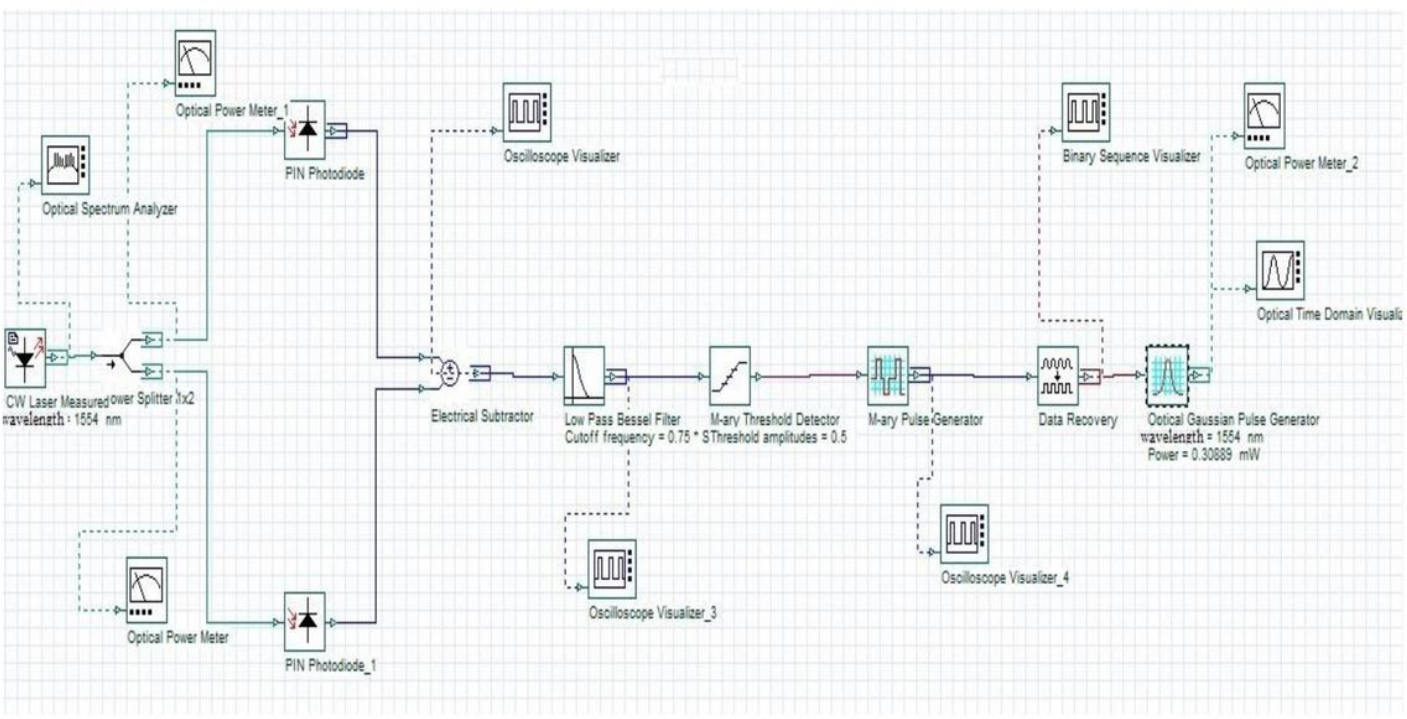

Figure 3

Please see the Manuscript PDF file for the complete figure caption

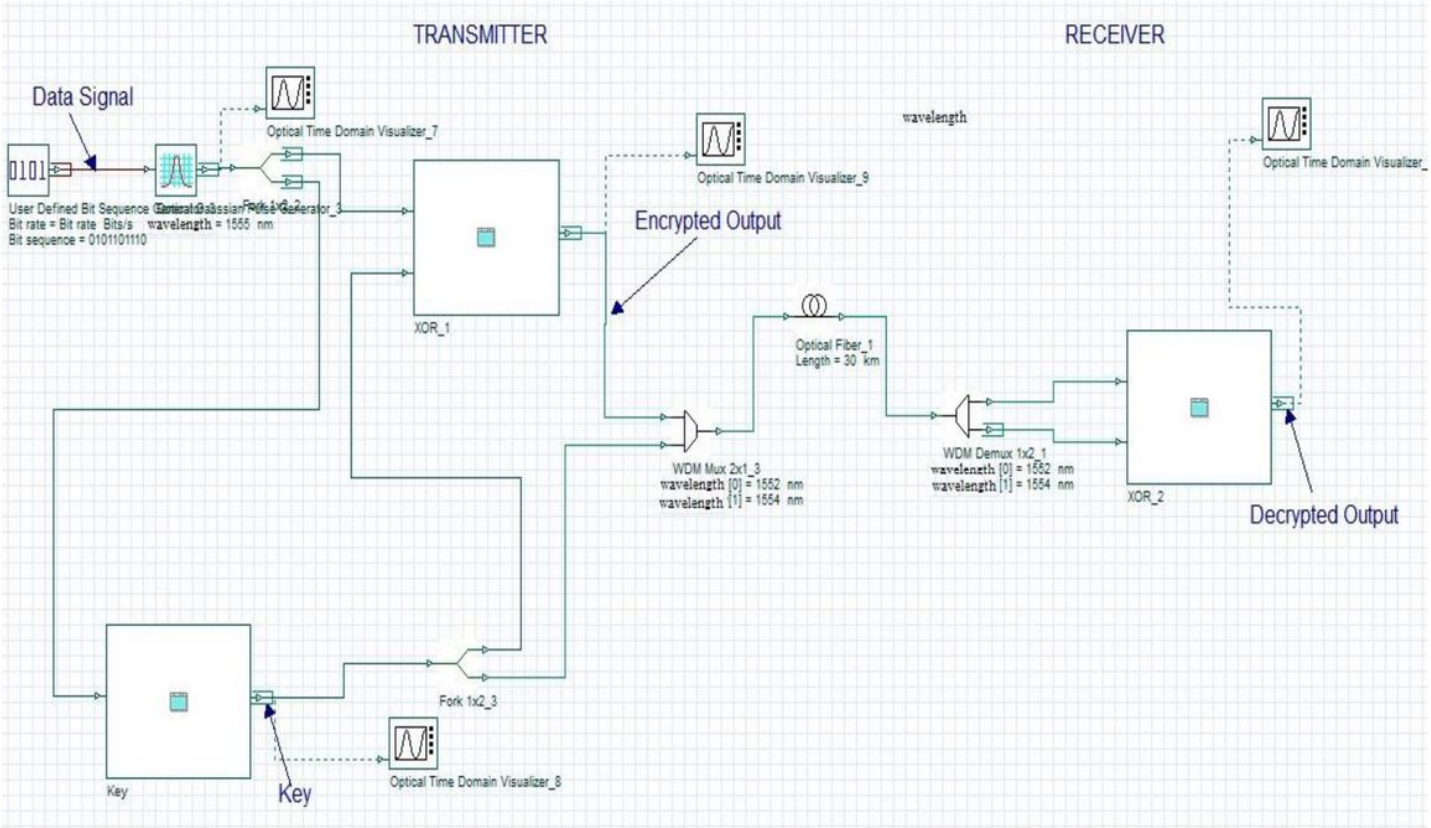

Figure 4

Please see the Manuscript PDF file for the complete figure caption

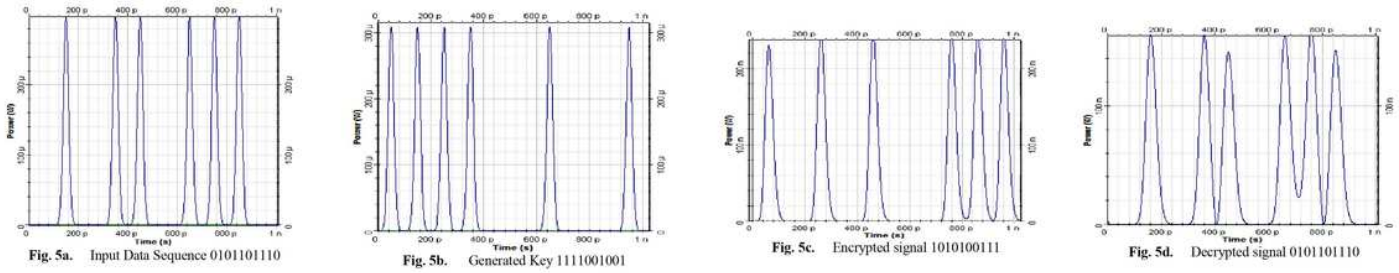

Figure 5

Please see the Manuscript PDF file for the complete figure caption

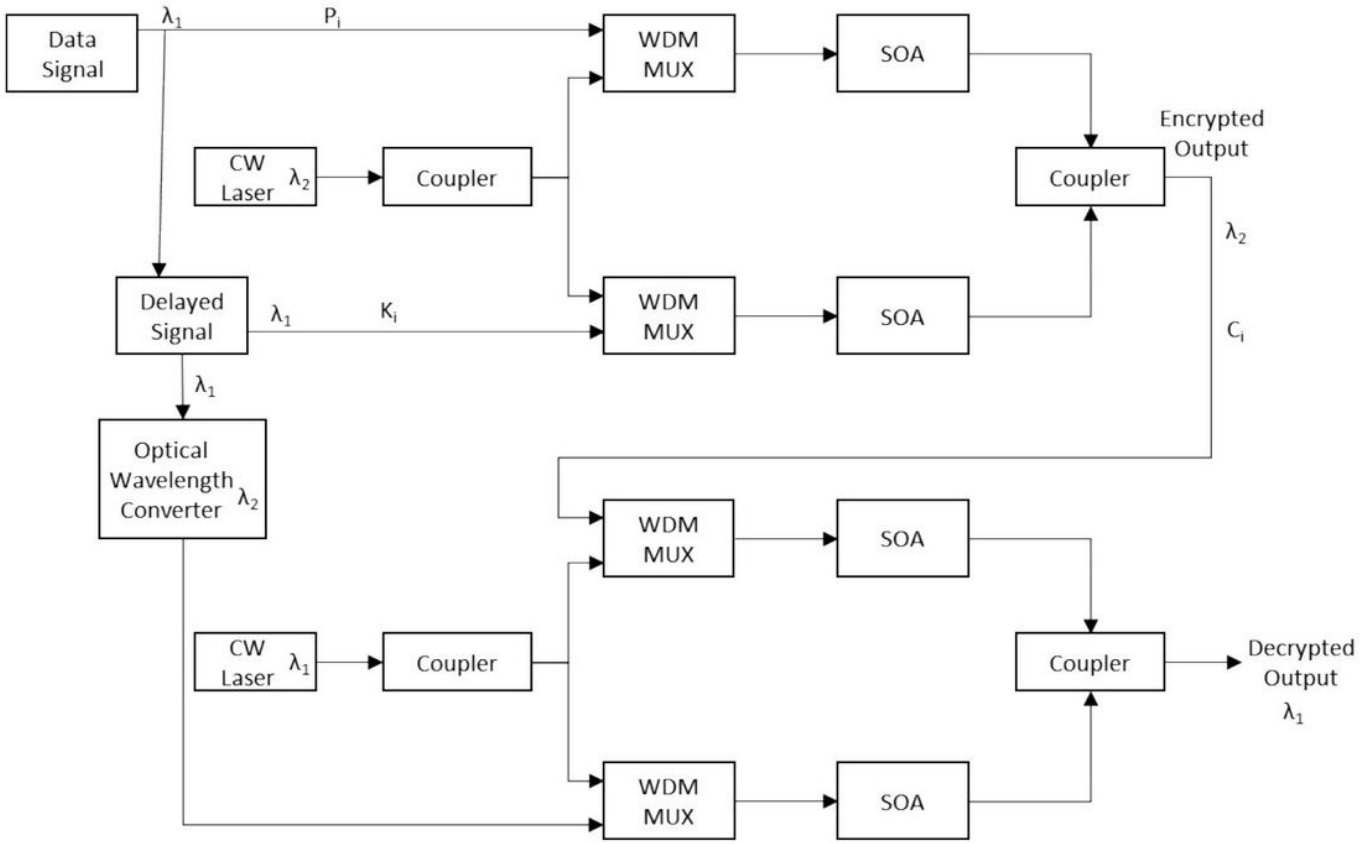

Figure 6

Please see the Manuscript PDF file for the complete figure caption

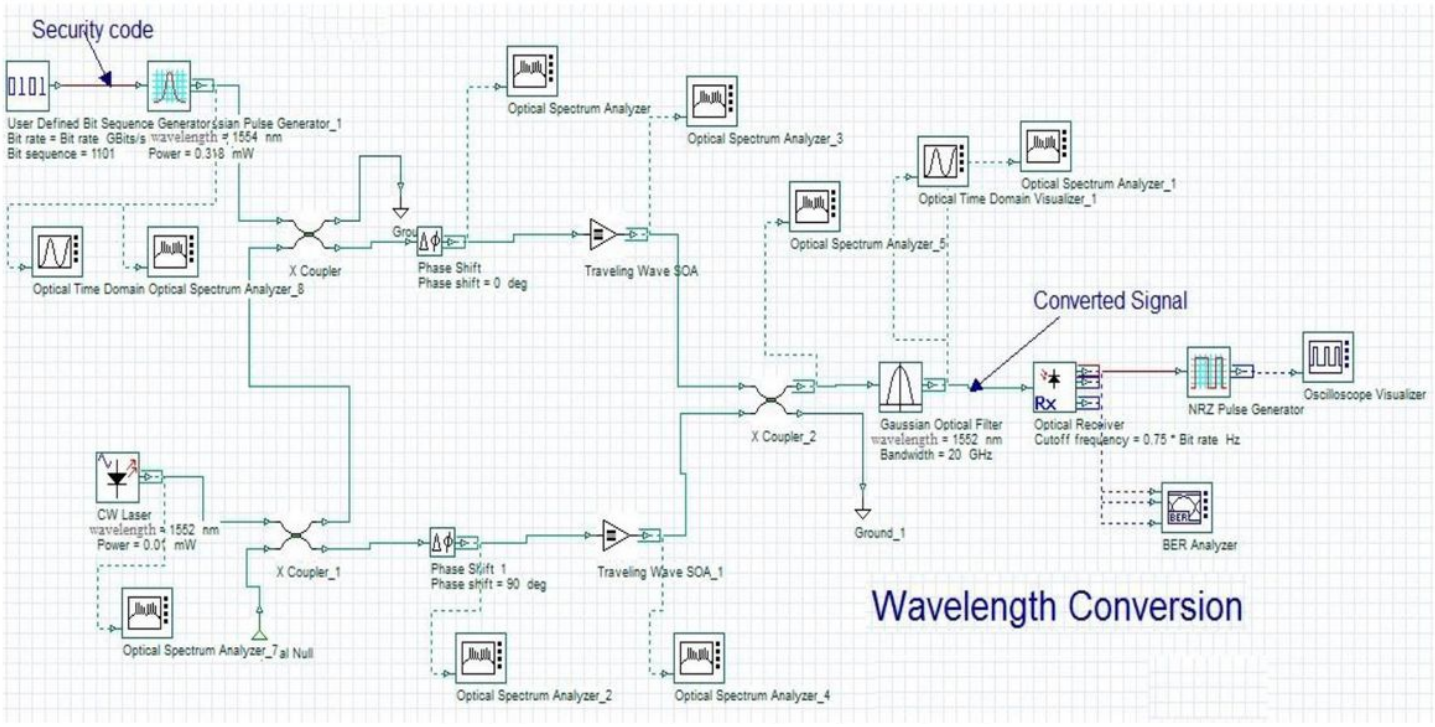

Figure 7

Please see the Manuscript PDF file for the complete figure caption

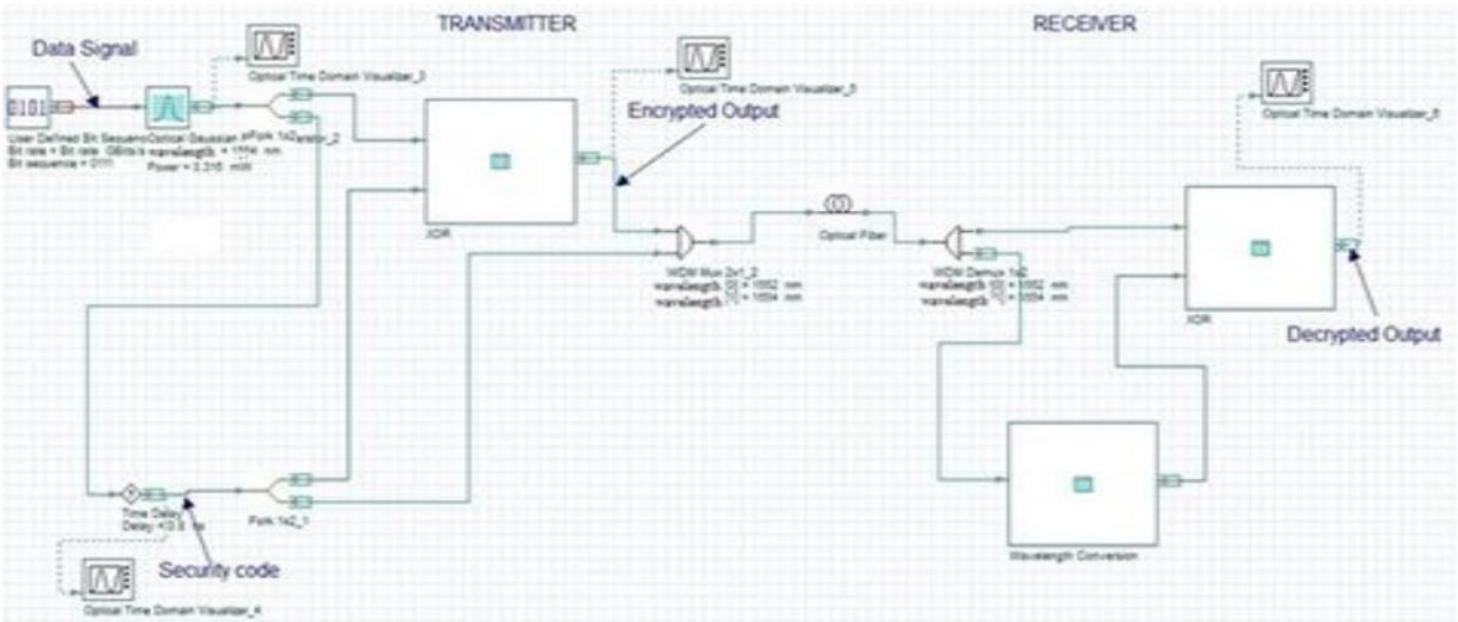

Figure 8

Please see the Manuscript PDF file for the complete figure caption

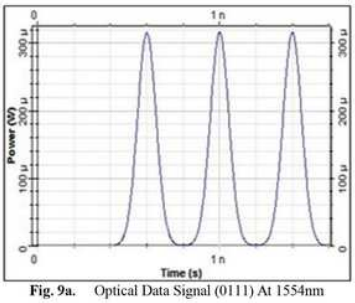

Fig. 9a. Optical Data Signal (0111) At 1554nm

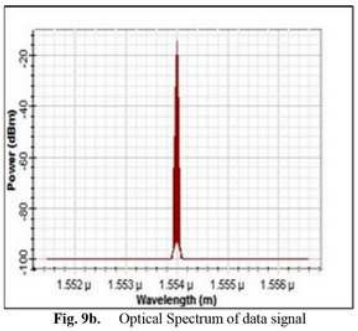

Fig. 9b. Optical Spectrum of data signal

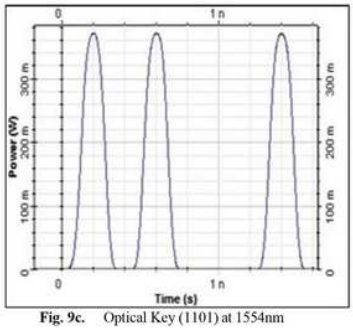

Fig. 9c. Optical Key (1101) at 1554nm

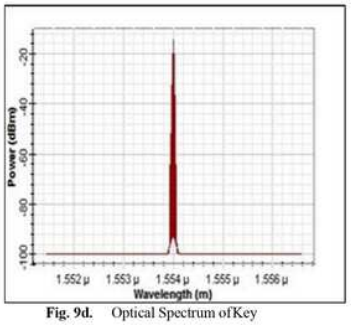

Fig. 9d. Optical Spectrum of Key

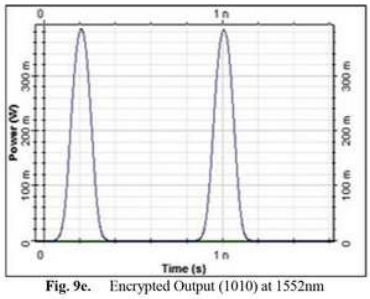

Fig. 9e. Encrypted Output (1010) at 1552nm

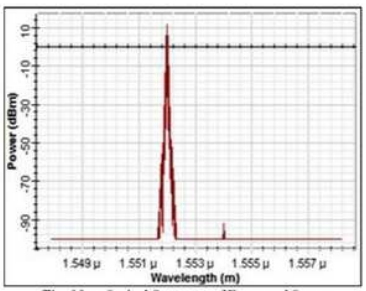

Fig. 9f. Optical Spectrum of Encrypted Output

Figure 9

Please see the Manuscript PDF file for the complete figure caption

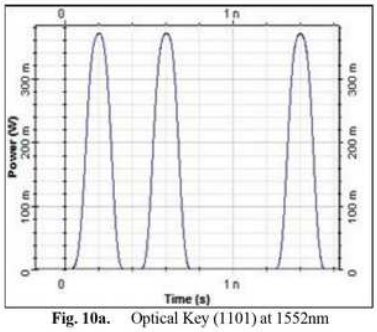

Fig. 10a. Optical Key (1101) at 1552nm

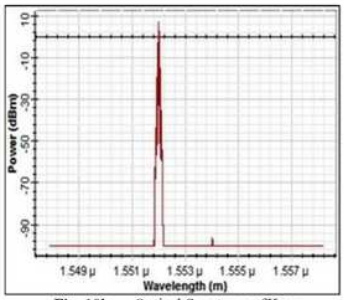

Fig. 10b. Optical Spectrum of Key

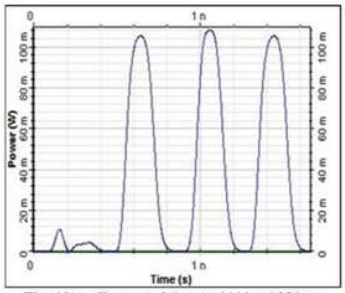

Fig. 10c. Decrypted Output 0111 at 1554nm

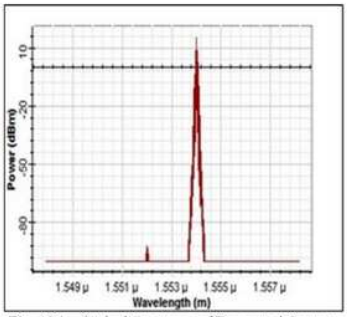

Fig. 10d Optical Spectrum of Decrypted Output

Figure 10

Please see the Manuscript PDF file for the complete figure caption

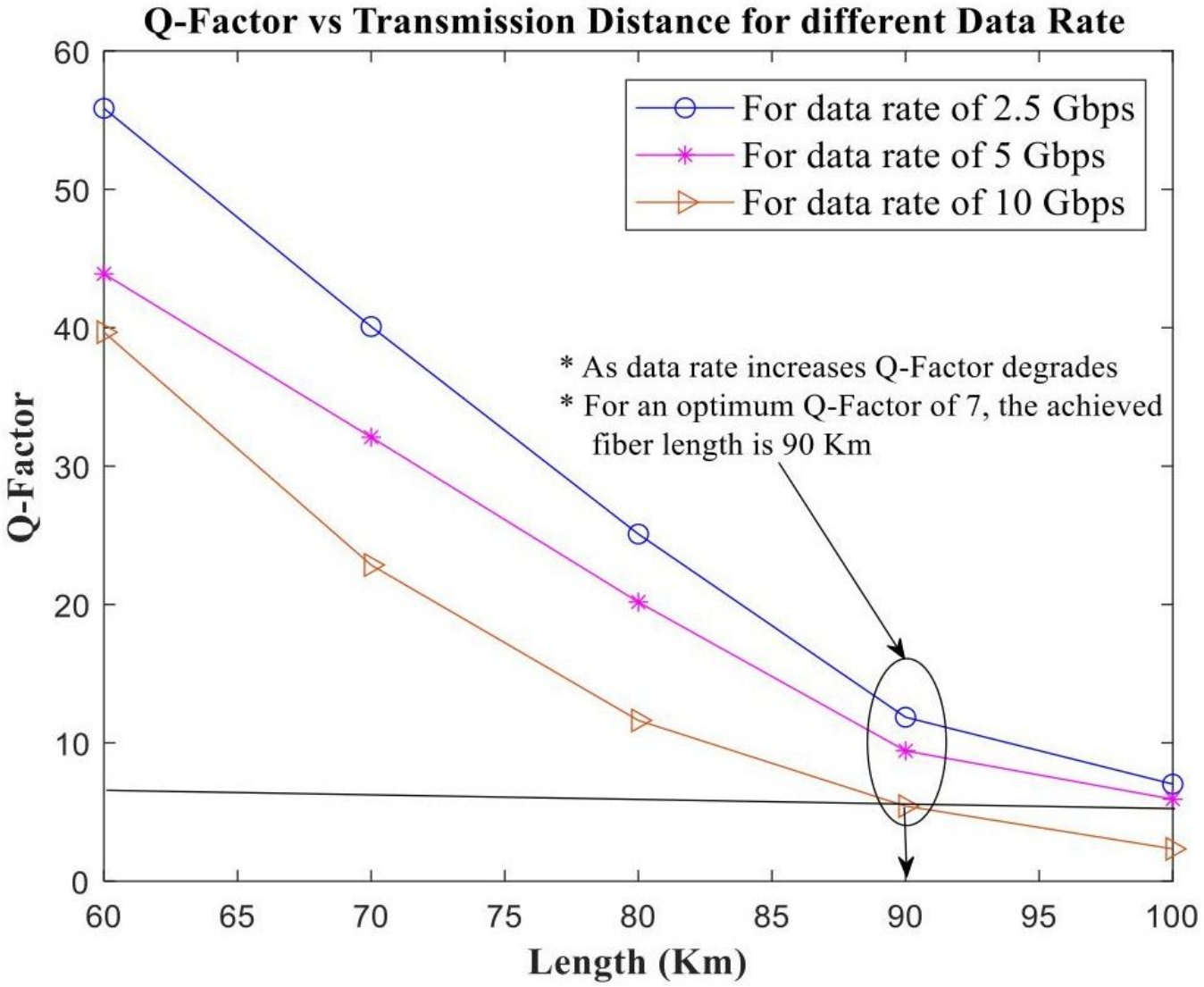

Figure 11

Please see the Manuscript PDF file for the complete figure caption

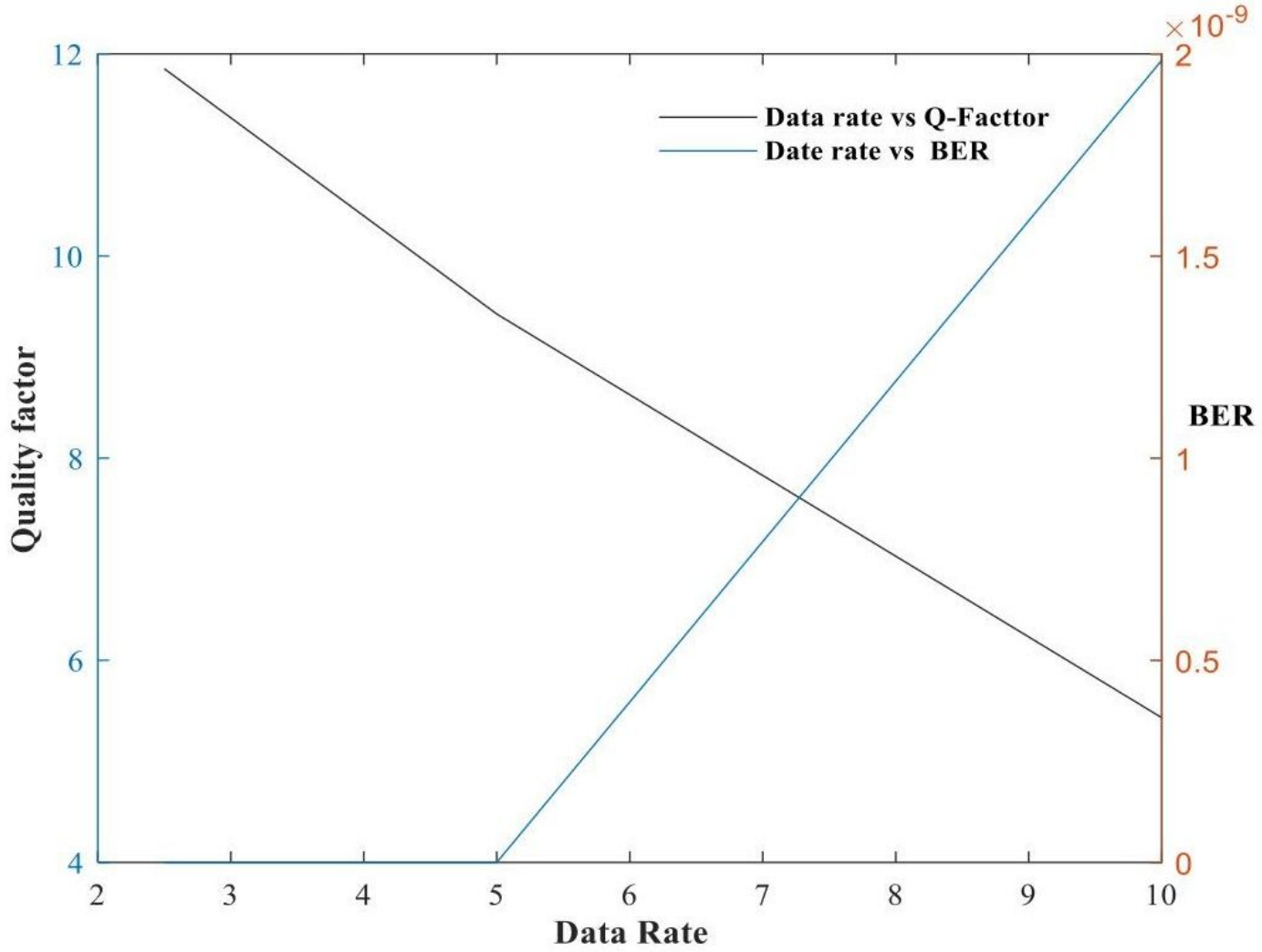

Figure 12

Please see the Manuscript PDF file for the complete figure caption