Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Encryption and Decryption Based on Bit Scrambling Using LFSR and Chaos Masking to Combat the Security Attacks in Optical Communication

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

Research Article

Keywords: Attacks, Chaotic masking, Optical Linear Feedback Shift Register, Optical Network Security, Lorentz equation, Scrambling.

Posted Date: June 3rd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-494855/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Abstract

With the latest technological advancements and attractive features of all optical networks such as bandwidth, performance, reliability, cost efficiency, redundancy these networks have been considered as most viable solution to satisfy promptly growing bandwidth demands. With the increased demand for an optical network, there arises the need for security as well. Vulnerabilities in all optical network made to concentrate more on security issues, as an unimaginable amount of data is being transmitted across these communication links. The proposed methodology to provide the security to these links involve the design of optical linear feedback shift register (LFSR) which gives the scrambled bits also known as randomization. By this process the information signal will be in unreadable form it is highly difficult to predict for the intruder to hack the information signal. In addition to this, the chaos masking and de masking technique is preferred to secure the information. The generated chaotic signal is non- periodic and non- binary so it is not possible to predict the form of the signal. Further this work gives the performance analysis for with and without chaos masking and demasking technique for the acceptable BER of $10e^{-12}$ and Q-factor of 7. It also gives the design and study for in-band jamming and out-band jamming attacks for all-optical networks. Simulation of proposed design is done using OptiSystem version 16.0 software tool and the performance are analyzed at different data rate and for different fiber length.

I. Introduction

Optical network technologies are evolving rapidly in terms of capability, security and capacity. This paper gives an understanding for the all-optical cryptography for secured fiber-optic communication. The Internet has exhibited an explosive growth over the last 20 years and is still continuing to exhibit an exponential growth. Among the different transport network technologies, because of attractive features of optical networks such as huge bandwidth, ultra-high capacity, 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 to support the brisk growth of bandwidth demand at relatively low energy consumption. An All-Optical Network (AON) [1]-[3] is a new technology that provides very high bit rates. AONs are very often considered to be the main candidate for constituting the backbone that will carry the global traffic whose volume has been growing at astounding rates that are not expected to slow down in the near future. Without the need of Optical-to-Electrical-to-Optical (O/E/O) processing at intermediate nodes. The ability to route large amounts of data and access different channels makes AON a very appealing option for providing very high rate access in Wide Area Network, Metropolitan Area Network, and even Local Area Network. Each node of the AON is equipped with an Optical Cross-Connect or an Optical Add/Drop Multiplexer, both of which are able to pass on the optical signals without O/E/O conversion, thus eliminating electrical delay. Furthermore, one of the major key factors for the development of AON is the emergence of the Wavelength Division Multiplexing technology. These led to researches oriented to all optical networking to harness more potential bandwidth from all-optical networks. In this paper, the first section discusses about security issues. The second section discusses about the proposed block

diagram in optical domain which uses the chaos based secure communication and LFSR to secure the information. The third section deals with the system implementation using the Optisystem software. It gives the various design models to secure the information and simulation results for the same. The fourth section deals in detail about the security attacks in all optical network and countermeasures, to secure the information been transmitted and also the comparison with various techniques. Then the fourth chapter deals with various system performances with and without chaos masking message encryption technique and comparison for the same. Finally, the last section deals with the conclusion and future work.

A. Security Issues

Although optical networks offer numerous advantages for high data rate communications, they have unique features and requirements in terms of security and management control that distinguish them from conventional communication networks. In particular, the special characteristics and components of optical networks also bring forth a set of security challenges, accompanied by new vulnerabilities in the network [4], [5]. To provide secure and reliable AON various security issues should be considered including physical security and information security. Physical security prevents unauthorized access to network resources. Information security [1], on the other hand, prevents unauthorized access to information, and assures confidentiality and integrity of the information. Currently, most of the research efforts on AONs security are geared.

In general, fault and attack management consist of prevention, detection and reaction mechanisms. Prevention mechanisms in transparent optical networks usually include measures aimed at overcoming the physical vulnerabilities of optical components. In network security, vulnerability is a flaw or weakness that may be exploited by an attacker to carry out a security physical attack. The peculiar characteristics and behaviors of the main components considered in deployment of an AON, such as optical fibers, optical amplifiers, and optical switching nodes, make AONs vulnerable to various forms of attacks including high-power jamming, physical infrastructure attacks, denial of service, service disruption (degrades Quality of Service, tapping attacks (provides access to unauthorized users) [4], [5] which can be used for eavesdropping and traffic analysis.

Encryption is an effective way to secure a signal and enhance the confidentiality of a network in the physical layer[1]. As with the fiber-optical transmission channel, optical encryption also benefits from not generating an electro- magnetic signature, which makes it immune to electromagnetic-based attacks. Even if eavesdroppers were able to obtain a small portion of signal by tapping into the optical fiber or listening to a residue adjacent channel, no useful information can be obtained without the knowledge of the encryption key. Encryption is the process of disguising the message which is plain text from the unauthorized users. The process of transforming cipher text back into plain text is known as Decryption. There are different techniques for enhancing optical network security such as optical encryption, optical chaos-based communication, optical steganography, and using Fiber Bragg Grating. Among several techniques, optical encryption is considered as good candidate to facilitate secure communication

without compromising the processing speed. Optical encryption can effectively protect the confidentiality of the physical layer network and satisfy the high-speed requirements of modern networks. Encryption and decryption have been utilized by governments and defense forces to secure much of world's most sensitive data.

B. Proposed Secured Optical Communication System Model

This section gives the detailed study of proposed secured optical communication system. It gives two level of security first by optical LFSR and second by chaos masking message encryption technique which helps to secure the information for optical networks. The proposed block diagram in Fig. 1 explains the optical chaos based secured communication system. It consists of transmitter, receiver and the channel. The optical LFSR [6]-[8] is designed by using the shift registers and the logic gates which is used for bit scrambling also known as randomization of bits. At first level of security the input signal and the output from Optical LFSR or Pseudo Random Bit Sequence (PRBS) is XORed together. The XOR operation is used as one of the techniques for encrypting the signal which hides the signal and provide certain level of security. Further, the XORed output is treated as one of the input to chaos masking technique and other input is chaotic signal which is generated by the phase space reconstruction by using Chen Chaos [9]. The signal performs chaos masking and it is transmitted through the fiber cable for long haul communication. The chaos masking message encryption technique secure the data to be transmitted, as the chaotic signal is high-fluctuating [10] and noise like signal which is highly unpredictable to detect.

At the receiver, same chaotic signal is been generated by using the self-synchronizing property [11] of chaos-based secured communication which help them to de-mask the signal. Further, by using the XOR gate with the same Optical LFSR can get back the original signal.

C. Chaos Communication

Chaos based secured communication [10]-[13] is one method for adding security to the data. Chaos communications is one of the application of chaos theory which intends to provide security in the transmission of information performed through different communication ways. Chaotic systems provides a rich mechanism for signal design and generation, with potential applications to communications and signal processing. Because chaotic signals are typically broadband, noise-like, and difficult to predict due to its property of sensitivity to initial conditions. Initially the two states, which are very close to each other, after certain time lapse it become very different from each other. By this it is not possible to predict the form of the system with randomly high precision. It also implies that, in practice, it is not possible to determine the long-time change of a chaotic system. A particularly useful class of chaotic systems are those that possess a self-synchronization property [11].

Transmitted signal,

$$s(t) = c(t) + m(t) \quad \ldots (1)$$

where, c(t) - chaotic carrier, m(t)- information Signal

Received signal,

$m\hat{}(t) = s(t) - c(t) + noise \ldots(2)$

where, c(t) - chaotic carrier, $m\hat{}(t)$ - information Signal

The chaos communication is divided into three main categories i.e., Chaos masking is shown in Fig. 2 in which a message signal is masked with the chaotic signal also known as chaotic carrier and transmitted through a channel. At the receiver side same chaotic signal is generated and demasking is perform to get back the original message signal as shown in Fig. 3. The generation of chaotic signal is based on the Lorentz chaos and Chen chaos [9] which follows the theory of phase space reconstruction. This method uses the single scalar time series between the attractor dynamics and phase space topology is the most important basic method of phase space reconstruction. For reconstruction method, it uses the most practical approach that is Grassberger with Procaccia proposed GP algorithm [14].

The input bit sequence is given to LFSR which is used to generate bit scrambled output to provide security. The chaotic signal is generated by Lorentz set of equations to carry low amplitude scrambled signal. By using Chaos masking message encryption technique hides the original information signal as chaotic signal is noise like and highly unpredictable. At the receiver, using the self-synchronization [6] property it regenerates the same chaotic signal to get back the scrambled signal. The information or input bit can be retrieved by using the efficient algorithm known as Berlekamp-Massey Algorithm [1]. Figure 4. shows the output of LFSR for the input sequence given as in Table 1. which provides the security at first level by scrambling the bit where n = 6 so the LFSR output sequence is non periodic till 63 bits. The implementation of Chaos masking in MATLAB- Simulink and generated chaotic signal is shown in Fig. 5.a -5.f respectively. First level of security is achieved by using LFSR bit scrambling which is shown in Fig. 5.b for the information shown in Fig. 5.a and second level of security achieved by chaotic masking as shown in Fig. 5.d for the chaotic signal shown in Fig. 5.c. At the receiver side the recovered demasked and descrambled signal are shown in Fig. 5.e and Fig. 5.f.

Table 1

BIT SCRAMBLING USING LFSR IN SIMULINK

Clock cycle	Output
1	-
2	1
3	0
4	0
5	0
6	1
7	0
8	1
9	0
10	0
.	.
.	.
.	.
60	0
61	1
62	0
63	1

Ii. Encryption And Decryption Using Optisystem

This section gives the implementation of optical LFSR for scrambling of the bits. Further it also give implementation of chaotic signal by using phase space reconstruction [14] method. Various different designs are implemented to provide security to the system by using the Optisystem Software version 16.0. It is a system level simulator based on the realistic modeling of optical communication systems. It possesses a powerful new simulation environment and a hierarchical definition of components and systems.

A. Optical linear feedback shift register (OLFSR)

The schematic block diagram Fig. 6 shows the model of optical LFSR. To design the Optical LFSR it requires the Optical D flip-flops, Optical NOT gate, Optical AND gate and Optical XOR gate. The design shown in Fig. 8 is for 3-bit which generates 7-bit scrambled output as shown in Table 2. Figure 7 shows the Optisystem simulation layout for optical LFSR and the generated bits (1001011) are shown in Fig. 8.

Table 2

BIT SCRAMBLING USING OPTICAL LFSR

Clock cycle	Output
1	-
2	1
3	0
4	0
5	1
6	0
7	1
8	1

B. Chaotic Signal Generation

The schematic for the generation of chaotic signal is shown in Fig. 9. As the generation of chaotic signal involves the continuous wave laser wavelength of 1550 nm, through the coupler with the delayed feedback loop of few ns. It uses Erbuim doped fiber amplifier in the amplifier of pump wavelength 980 nm to amplify the signal and also it uses Bessel bandpass filter to suppress the noise added to the signal which will change the dependency of the input signal frequency. The generation of chaotic signal is based on parameters which are mentioned in the Table. 3. The simulation results are shown Fig. 10. a and 10. b explains that the chaotic signal is generated in x and y which is like noise and very difficult to predict.

Table 3

SIMULATION PARAMETERS FOR ENCRYPTION AND DECRYPTION

PARAMETERS	SPECIFICATIONS
CW LASER 1	Wavelength = 1550nm, Power=-10dBm
Pseudo random bit sequence	Bit rate = 10Gbps
Coupler 1,2	Coupling ratio = 0.5
Coupler 3	Coupling ratio = 0.9
Optical Fiber Characteristics	10km, Attenuation = 0.2dB/km
CW LASER 2	Wavelength = 1552.524nm, Power=-0dBm
Optical LFSR data rate	1 Gbps
D flip flop laser 1(Tx)	Wavelength = 1540nm, Power=-0.3mW
D flip flop laser 2(Rx)	Wavelength = 1545nm, Power=-0.25mW
EDFA	Gain = 1dB, Wavelength = 980nm
Bessel optical filter (bandpass)	Bandwidth = 10GHz, Wavelength = 1556nm

C. Chaos Masking based Transmission and Reception

For secure transmission and reception, chaos-masking message encryption [11]-[13] technique is used. Here, an input signal is a message bearing signal which is masked with the chaotic signal to generate the noise-like signal. Since the chaotic signal has high fluctuation and pretends to be as noise which is difficult for the intruder to hack the information. Figure 11 shows the schematic diagram for chaos based transmission and reception. The chaos based masking technique is based on parameters which are mentioned in the Table 3. Figure 12. a represents the PRBS input signal which is combined with chaotic signal as shown in Fig. 12.b and the masked signal shown in Fig. 12.c. At the receiver side the demasked signal as shown in Fig. 12. d is recovered.

D. Encryption and Decryption based on Chaos-masking technique

The simulation layout of encryption and decryption as shown in Fig. 13 based on chaos masking using optisystem software. The input signal (1100) as shown in Fig. 14. a is user defined which XORed with the optical linear feedback shift register as shown in Fig. 14. b to provide the scrambling. The XORed gate gives is the encrypted output as shown in Fig. 14. c. Further it is masked with the chaotic signal as shown in Fig. 14. d which securely transmit the information through the fiber cable without been attack by the intruder. At the receiver using the same chaotic signal demasking is performed as shown in Fig. 14.e. The same Optical linear feedback shift register (LFSR) is designed for performing decryption and the decrypted output as shown in Fig. 14.f. The simulation parameter is shown in Table 3. The results shown in Figs. 14.a -14.f shows the encryption and decryption is performed using chaos masking technique. From the obtained simulation result Fig. 14.f verifies that the encryption and decryption based on chaos masking technique gives the security to the system without been attack by the intruder.

Iii. Security Attacks In Proposed System

A network security attack [15, 16, 17]] may be defined as an intentional action against the secure functioning of the system. A network security attack can be performed at the physical layer, exploiting vulnerabilities of the physical network infrastructure, or any higher network layer, exploiting vulnerabilities at network protocols. It focuses on the physical-layer security attacks that directly impact the physical infrastructure of AON. The physical layer attacks can be divided into two main categories: Service Disruption (SD), which prevents communication or degrades QOS [16] and Tapping, which compromises privacy by providing unauthorized access to the transmitted data, which can be used for traffic analysis purposes. Security attack methods are classified into two main types: direct and indirect.

Direct attack method can be implemented directly on certain AON components such as Optical Amplifiers, optical fibers. The attack methods include cutting of fiber for SD, fiber bending for tapping or SD etc.

The Indirect attack is most likely to be attacked indirectly to network elements because it is complicated to attack them directly or they are not easily accessible. It attempts different scenario such as taking advantage of possible vulnerabilities of AON components and other transmission effects such as crosstalk to gain access to the network.

A. Service Disruption attack

This is one of the indirect attack methods. These attacks are aimed at degrading Quality of Service (QoS) or causing service denial.

B. In-band jamming

A malicious signal on one of the wavelengths used by legitimate users. This result in SD without breaking or disrupting the fiber. This attack scenario is referred to as in-band jamming as shown in Fig. 15. Due to transparency feature of AONs and very low attenuation of optical fiber, in-band may propagate through the network affecting different wavelengths. The schematic diagram shown in Fig. 16 combines four different wavelength with same power level is transmitted through the cable. At the receiver side it can able to retrieve back the information signal without been affected by different wavelengths. The simulation layout is shown in Fig. 17 and the performance is analyzed for Q-factor Vs transmission distance which is shown in Fig. 17.

C. Performance analysis through in-band jamming

The performance were analyzed with different techniques such as in-band jamming without chaos masking, with chaos masking, with chaos masking and booster amplifier and with chaos masking pre-amplifier. The Q-factor vs Transmission distance for data rate of 1 Gbps with different techniques is shown in Fig. 21, which indicates that as distance increases for a specific data rate, the Q-factor degrades. With chaos masking technique, it can able to secure the data with higher transmission distance

as compared to without masking technique. With booster amplifier, able to secure data till 70kms for security attack in-band jamming.

D. Out-band jamming

The attacker inserts a high-powered malicious signal into a network fiber link. The injected attack signal may be transmitted on a wavelength different from those of legitimate user but within the fiber bandwidth known as out-band jamming signal. This attack scenario exploits fiber non-linearities [15]-[17] under high input power that leads to crosstalk effect between WDM channels. Due to transparency of AONs, a powerful jamming signal may propagate through a network, thus affecting the legitimate data channel at different locations. The schematic diagram shown in Fig. 21 combines two different wavelength with different power level is transmitted through the cable. At the receiver side it can able to retrieve back the information signal without been affected by different wavelengths.

E. Performance analysis throughout-band jamming

The performance were analyzed with different techniques such as out-band jamming without chaos masking, with chaos masking, with chaos masking and booster amplifier and with chaos masking pre-amplifier. The Q-factor vs Transmission distance for data rate of 1 Gbps with different techniques is shown in Fig. 23, which indicates that as distance increases for a specific data rate, the Q-factor degrades. With chaos masking technique, it can able to secure the data with higher transmission distance as compared to without masking technique. With booster amplifier, able to secure data till 76kms for security attack out-band jamming.

Iv. Performance Analysis At Different Launch Power For Chaos Masking Technique

The performance analysis at different power is studied. The Q-factor vs Transmission distance for different data rates as shown in Fig. 24. From Fig. 24 as data rates increases for a given distance, the Q-factor degrades. For a given data rate the Q-factor decreases as the transmission distance increases. As optical input power is increased, transmission distance increases for respective data rates. The performance dependence on system parameters by varying the data-rate, launch power for different optical fiber length from 10km to 100km in the OptiSystem simulation, the Q-factor and BER values are analyzed as shown in Table 4. From the graphs as shown in Fig. 23 and Fig. 24, it is concluded that the chaos- masking technique is preferred as compared to without chaos masking because the information signal can travel securely for longer distance. The acceptable value is taken as Q-factor of 7 for the BER $10e^{-12}$ at the data rate of 1 Gbps as shown in Table 5.

The performance analysis for different launch powers and different data rates are studied for with and without chaos masking technique. The Transmission distance vs Launch power for different data rates are shown in Fig. 25.a -25.d.

Table 4

Q-FACTOR AND BER AT DIFFERENT OPTICAL FIBER LENGTH WHEN DATA-RATE IS 1 GBPS

Fiber Length (Km)	Power 1 mw		Power 10 mw		Power 100 mw	
	Q-Factor	BER	Q-Factor	BER	Q-Factor	BER
1	30.69	2.96 e-207	224.86	0	280.28	0
10	25.83	1.92 e-147	140.01	0	217.82	0
20	16	6.34 e-58	76.24	0	79.91	0
30	10.08	3.10 e-24	43.31	0	44.59	0
40	7	1.11 e-12	31.6	1.42 e-219	34.91	3.6 e-256
50	5.41	1.14 e-9	24.27	1.99 e-130	29.48	8.58 e-189
60	3.35	8.2 e-6	19.18	2.34 e-82	27.79	4.17 e-149
70	0	1	13.17	6.13 e-40	20	6.66 e-99
80	0	1	6.93	1.85 e-23	11.23	7.4 e-49
90	0	1	5.1	7.2 e-9	7.61	3.69 e-13
100	0	1	0	1	5.2	3.1 e-9

TABLE 5

MAXIMUM FIBER REACH FOR ACCEPTABLE BER FOR 10E-12 AND Q FACTOR OF 7

Data Rate Power	1 Gbps	10 Gbps	40 Gbps	100 Gbps
1mW	40 km	32 km	4.2 km	0.45 km
10mW	80 km	68 km	5 km	0.75 km
100mW	92 km	73 km	6 km	1 km

Figure 25.a -25.d indicates that the transmission distance can be increased by increasing the launch power but as the data rate increases, the transmission distance decreases due to the non- linearities in the fiber. Chaos- masking technique is preferred because it can transmit the information for longer distance.

The proposed system is well suited for the PON in optical communication which gives the maximum link length of 40kms. From the performance analysis of the proposed system, it can be understood that the optimized result for the data rate of 1 Gbps with launch power of 1mW gives the maximum link length of 40kms. Similarly, the link length of the system can be increased by increasing the launch power at the transmitter side for the acceptable BER of $10e^{-12}$ and Q-factor of 7.

V. Results And Discussion

With increased demand for optical network, there arises the need for security as well. As ever before, these networks are being subjected to hacking and criminal manipulations. These vulnerabilities made to concentrate more on security issues, as an unimaginable amount of data is being transmitted across these communication links. This work focuses on the security issues related to the optical communication and countermeasures to it. It demonstrated two level of security to the system first by using Optical LFSR which is used for bit scrambling. At this level the information signal is hidden from the intruder but it is not completely secured. Chaos based secure communication is second level of security added to the data. Chaos communications is one of the applications of chaos theory which intends to provide security in the transmission of information performed through different communicating ways. It generates the chaotic signal by using the mechanism Phase space reconstruction and Lorentz Chaos. The chaotic signal generated is noise-like, highly fluctuating, difficult to differentiate for the intruder difficult to predict. 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. Further, it gives the detailed study for in-band jamming and out-band jamming security attacks in All-optical networks. Thus, the obtained results indicate that for 70km of transmission distance error free transmission and good quality of the signal reception at the receiver is achieved at 1 Gbps for optical power of 1mw.

In future, the work can be extended for securing the information by two different techniques first by modeling different message encryption technique in chaos-based secure communication and second by using the parallel Optical LFSR through these techniques the security of the information signal can be increased and it can be transmitted without being attacked by malicious user. Further, the performance analysis for different fiber length can be studied and analysed.

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. Bruce Schneier,"*Applied Cryptography second edition: protocols, algorithms and source code in C".*
2. Ben, B. J. Shastri, and P.R. Prucnal. "Secure communication in fiber-optic networks," *Emerging trends in ICT security*. Morgan Kaufmann,. 173-183, 2014.
3. P. Fok , Z. Wang , Y. Deng , P. R. Prucnal, "Optical layer security in fiber-optic networks." *IEEE Transactions on Information Forensics and Security*vol. 6,no. 3, pp.725-736, 2011.
4. Lazzez, Amor. “All-optical networks: Security issues analysis." *IEEE/OSA Journal of Optical Communications and Networking*7 no. 3, pp: 136-145, 2014.
5. Marija, N. S. Kapov, S.Zsigmond, and Lena Wosinska. "Vulnerabilities and security issues in optical networks." *16th International Conference on Transparent Optical Networks (ICTON*), pp. 1-4. IEEE, 2014.
6. Chattopadhyay, Tanay, Tamer A. Moniem, and Hirak Kumar Maity. "All-optical pseudorandom binary sequence (PRBS) generator using the hardlimiters." Optik vol. 124 no. 20 pp. 4252-4256, 2013
7. Ahmad, Afaq, S. S. Al-Busaidi, and M. J. Musharafı. "On Properties of PN Sequences generated by LFSR–a Generalized Study and Simulation Modeling." Indian Journal of Science and Technology vol. 6, no. 10, pp. 5351-8. 2013.
8. Lurina, Manda, Sugondo Hadiyoso, and Rina Pudji Astuti. "Scrambling and De-Scrambling Implementation Using Linear Feedback Shift Register Method on FPGA." International Journal of Applied Information Technology vol. 1. no. 01, pp 59-67, 2017.
9. Qun Ding, J., and B. Du. "A new improved scheme of chaotic masking secure communication based on Lorenz system." International Journal of Bifurctaion and Chaos vol. 22, no.5, pp. 1250125, 2012.

10. Ekhande, Rahul, and Sanjay Deshmukh. "Chaotic signal for signal masking in digital communications." International organization of Scientific Research Journal of Engineering vol. 4. no. 2, pp. 29-33, 2014
11. Pecora, Louis M., and Thomas L. Carroll. "Synchronization in chaotic systems." International organization of Scientific Research Journal of Engineering vol. 4. no. 2, pp. 29-33,
12. Oppenheim, A.V. and Cuomo, K.M. "Chaotic Signals and Signal Processing" Digital Signal Processing Handbook Ed. Vijay K. Madisetti and Douglas B. Williams Boca Raton: CRC Press LLC, 1999.
13. Alvarez, Gonzalo, and Shujun Li. "Some basic cryptographic requirements for chaos-based cryptosystems." International journal of bifurcation and chaos vol. 16, 08, pp. 2129-2151, 2006.
14. Di, Chongli, et al. "An improved Grassberger-Procaccia algorithm for analysis of climate system complexity." Hydrology & Earth System Sciences vol. 22, no.10, 2018.
15. Yang, Xuelin, et al. "Chaotic encryption algorithm against chosen-plaintext attacks in optical OFDM transmission." IEEE Photonics Technology Letters vol. 28, no. 22, pp. 2499-2502, 2016.
16. Skorin-Kapov, Nina, Jiajia Chen, and Lena Wosinska. "A new approach to optical networks security: Attack-aware routing and wavelength assignment." IEEE/ACM transactions on networking vol.18, no.3, pp. 750-760, 2009.
17. Deng, Tao, and Suresh Subramaniam. "Covert low-power QoS attack in all-optical wavelength routed networks." IEEE Global Telecommunications Conference, 3, 2004.

Figures

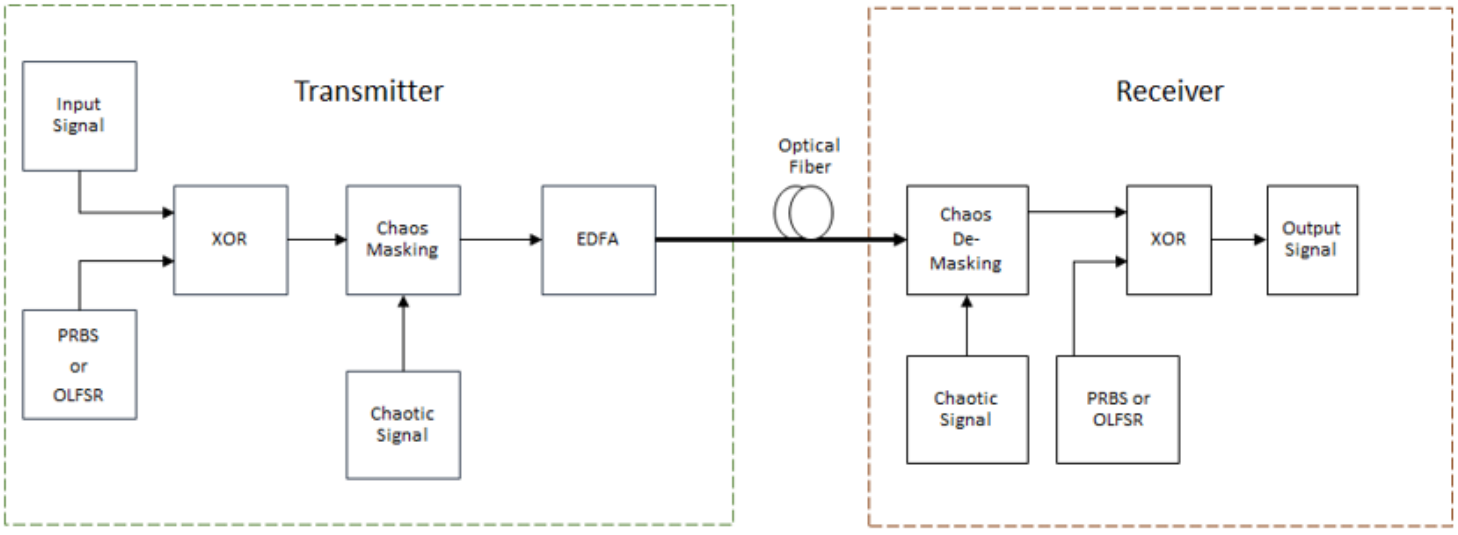


Figure 1

Block Diagram for Proposed secured optical communication system

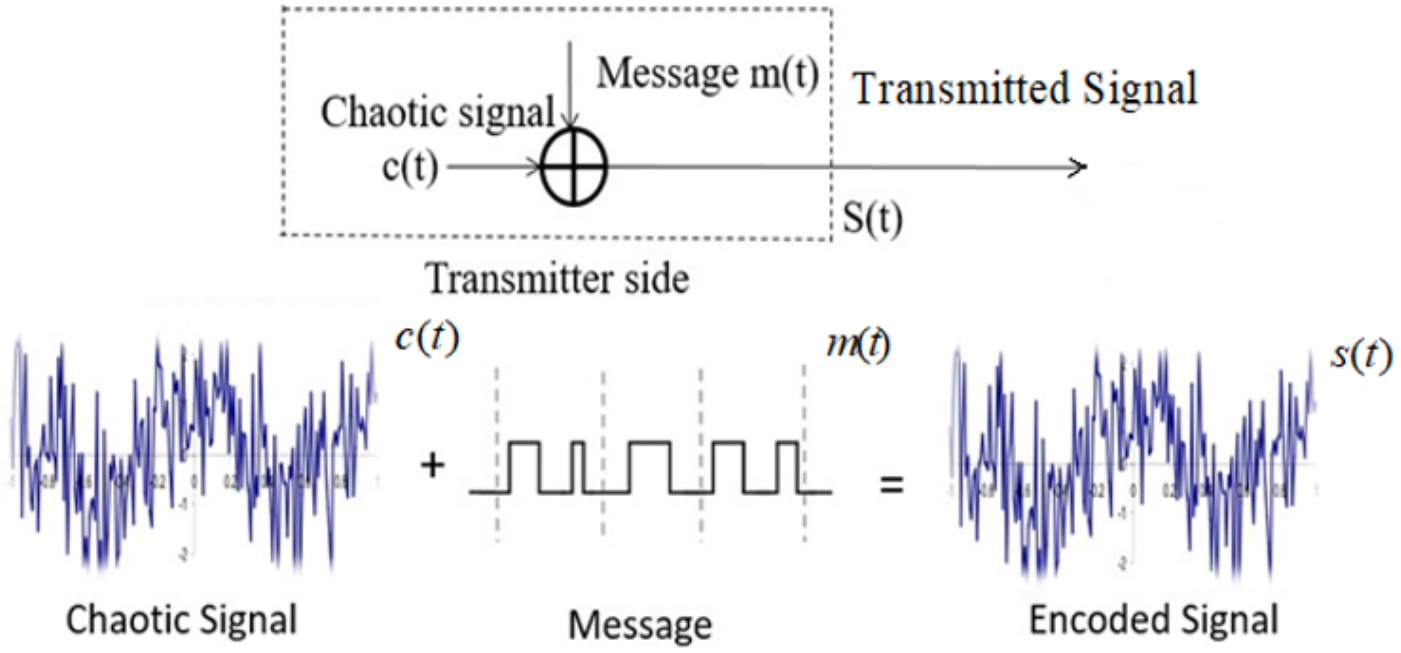


Figure 2

Schematic diagram for chaotic masking

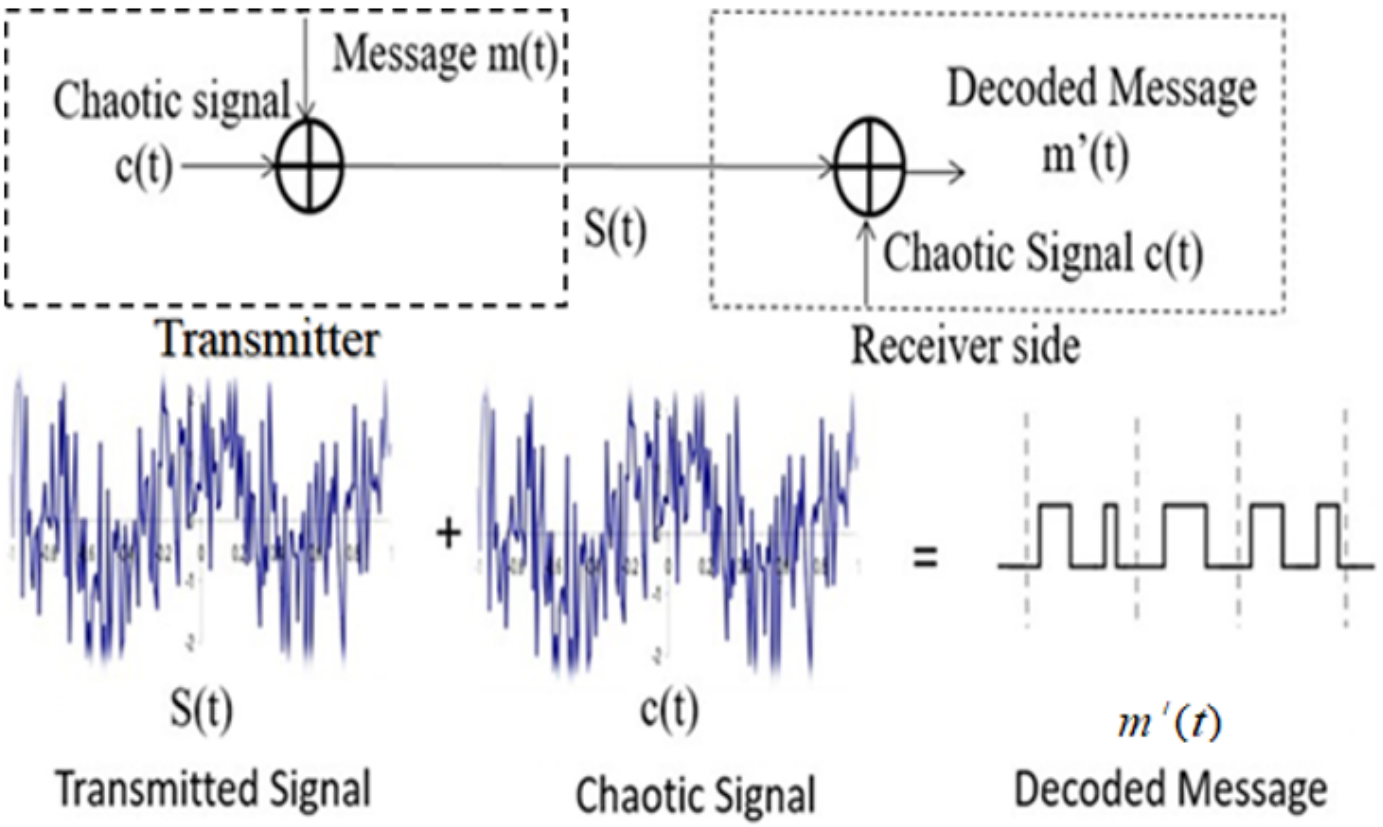


Figure 3

Schematic representation of chaotic demasking

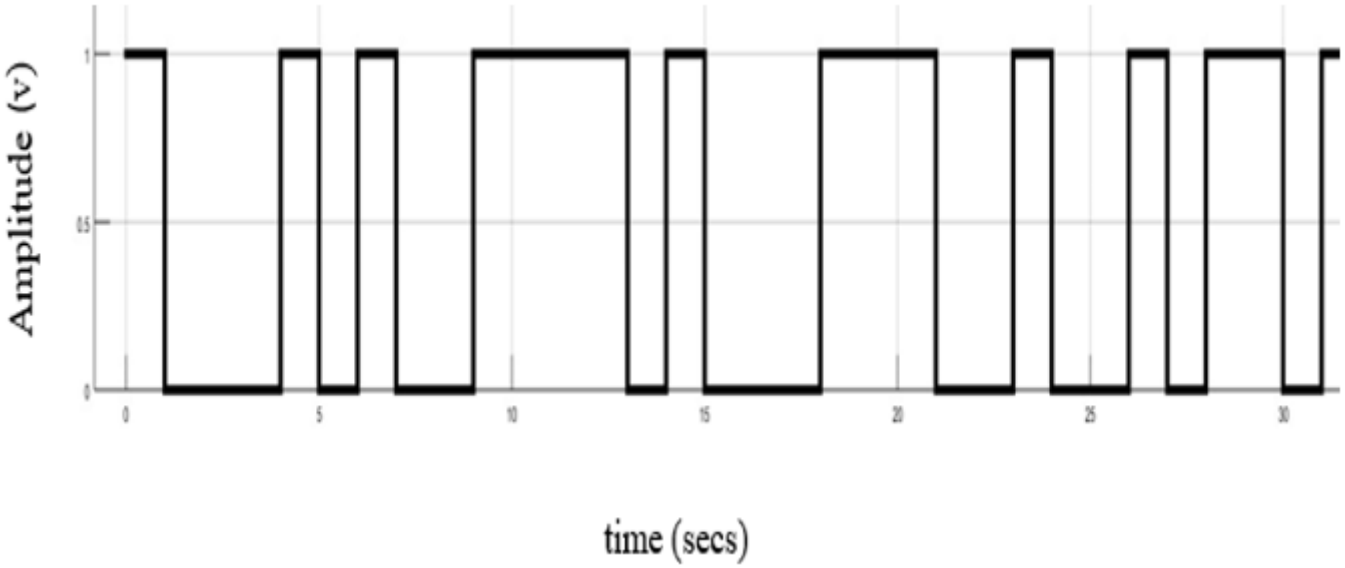


Figure 4

Output of Linear feedback shift register

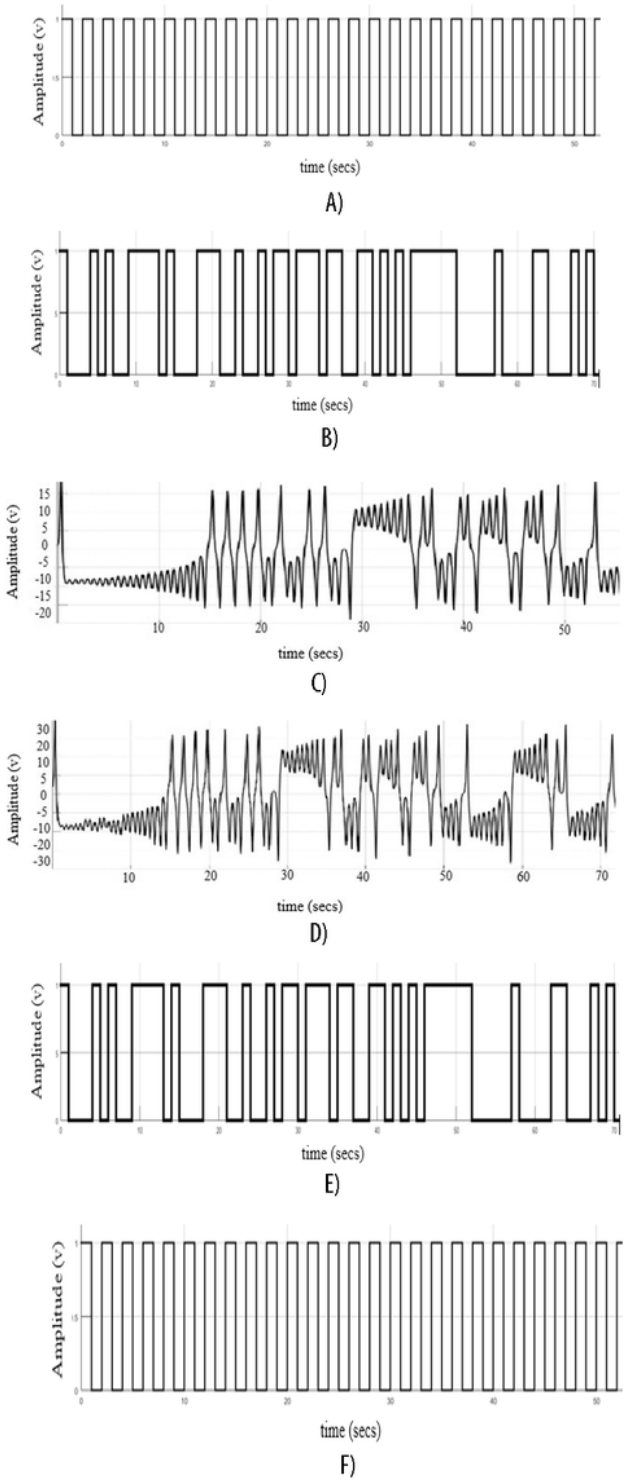


Figure 5

a. Information signal m(t) b. Bit Scrambled Signal c. Chaotic signal c(t) d. Masked Signal s(t) e. De-masked Signal f. Descrambled Signal

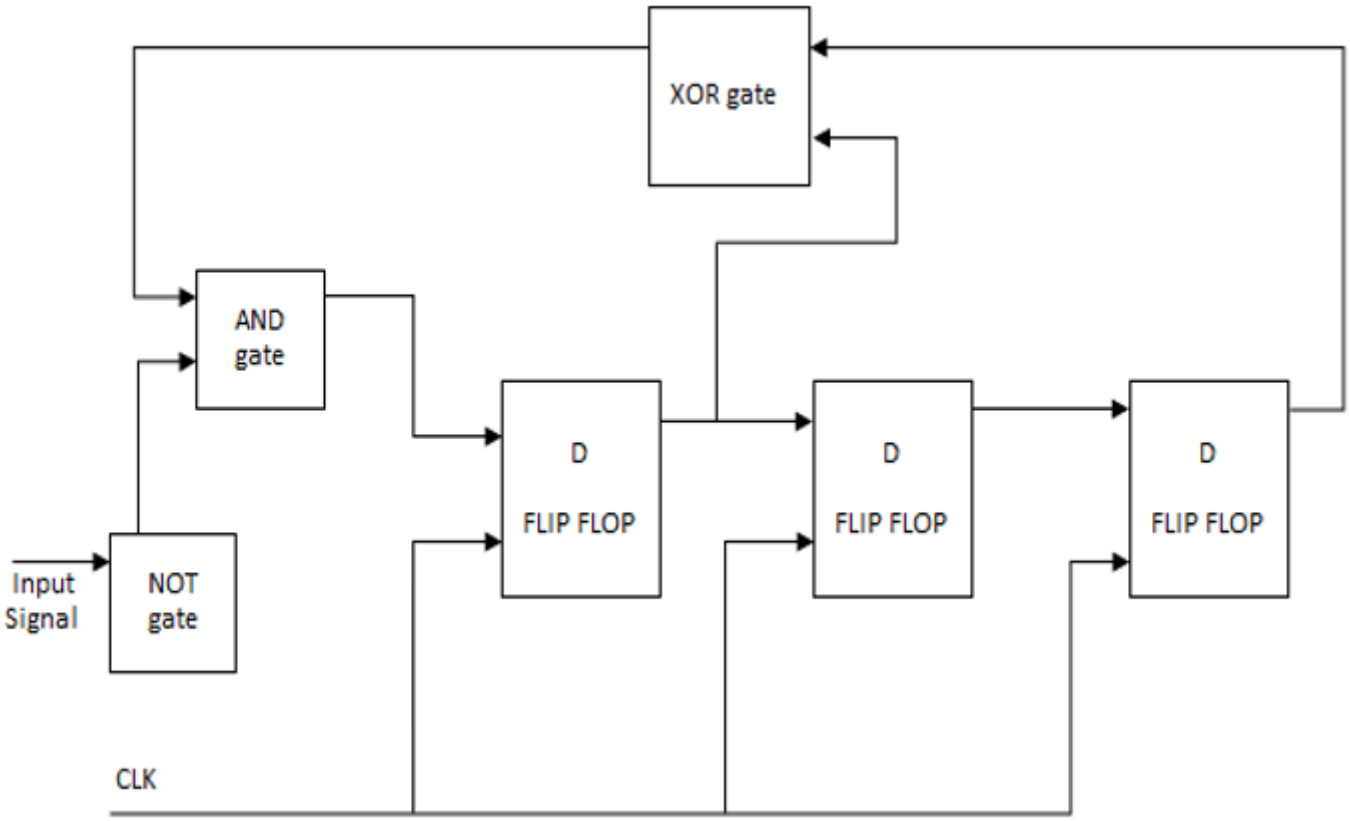


Figure 6

Schematic diagram of optical LFSR

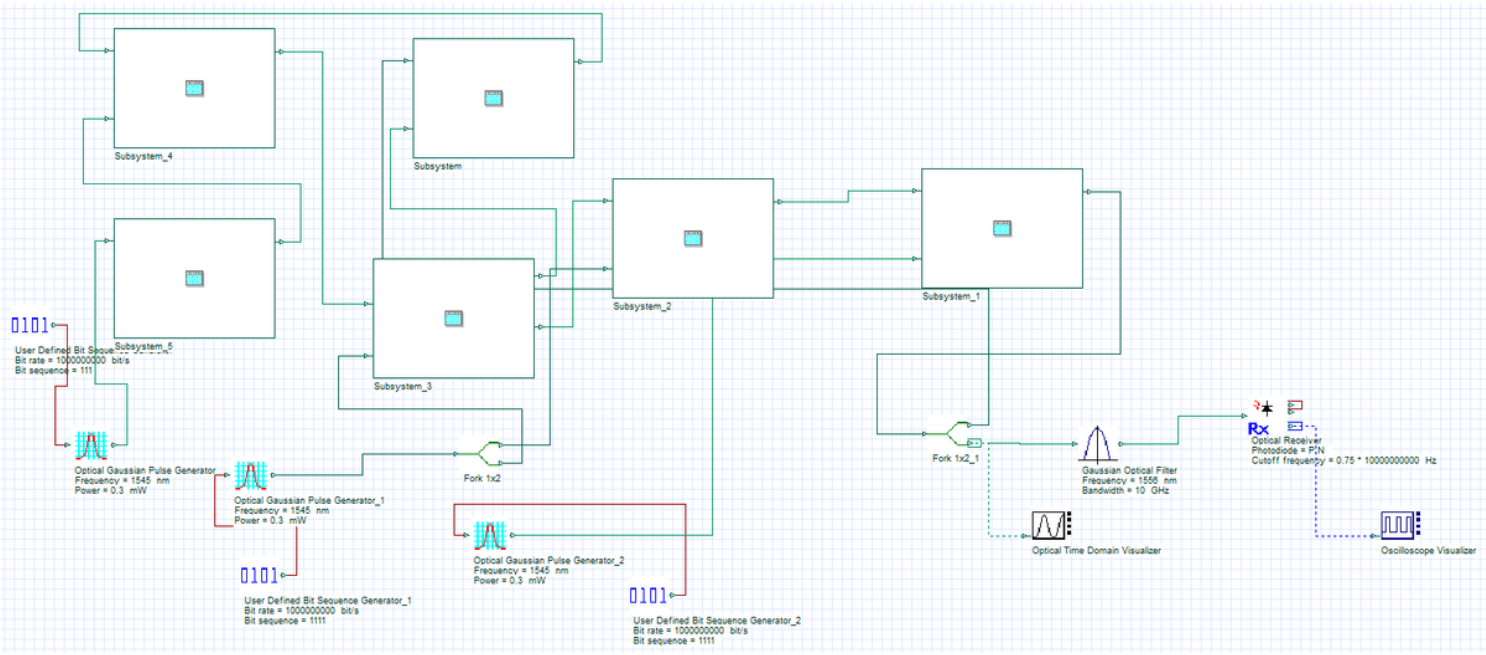


Figure 7

Simulation layout of Optical LFSR

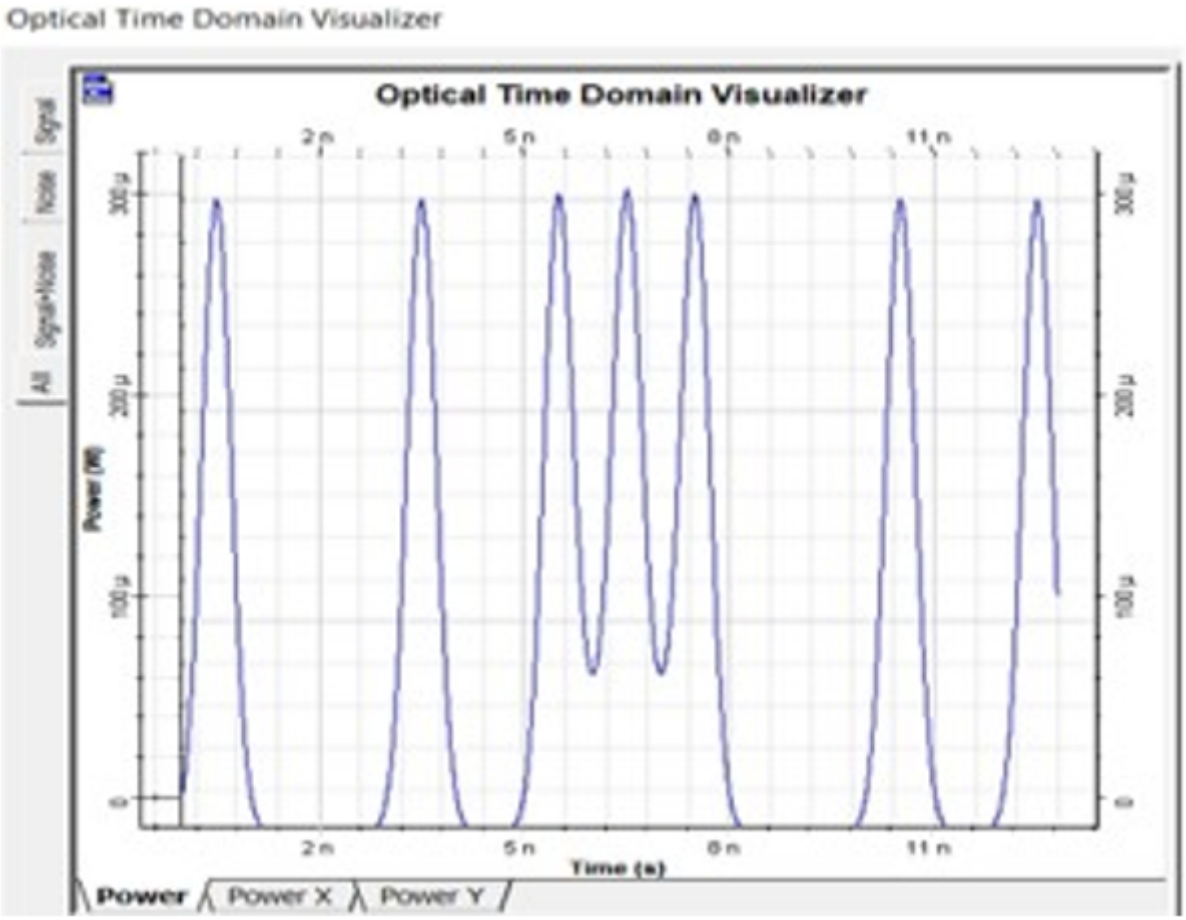


Figure 8

Output of Optical LFSR (1001011)

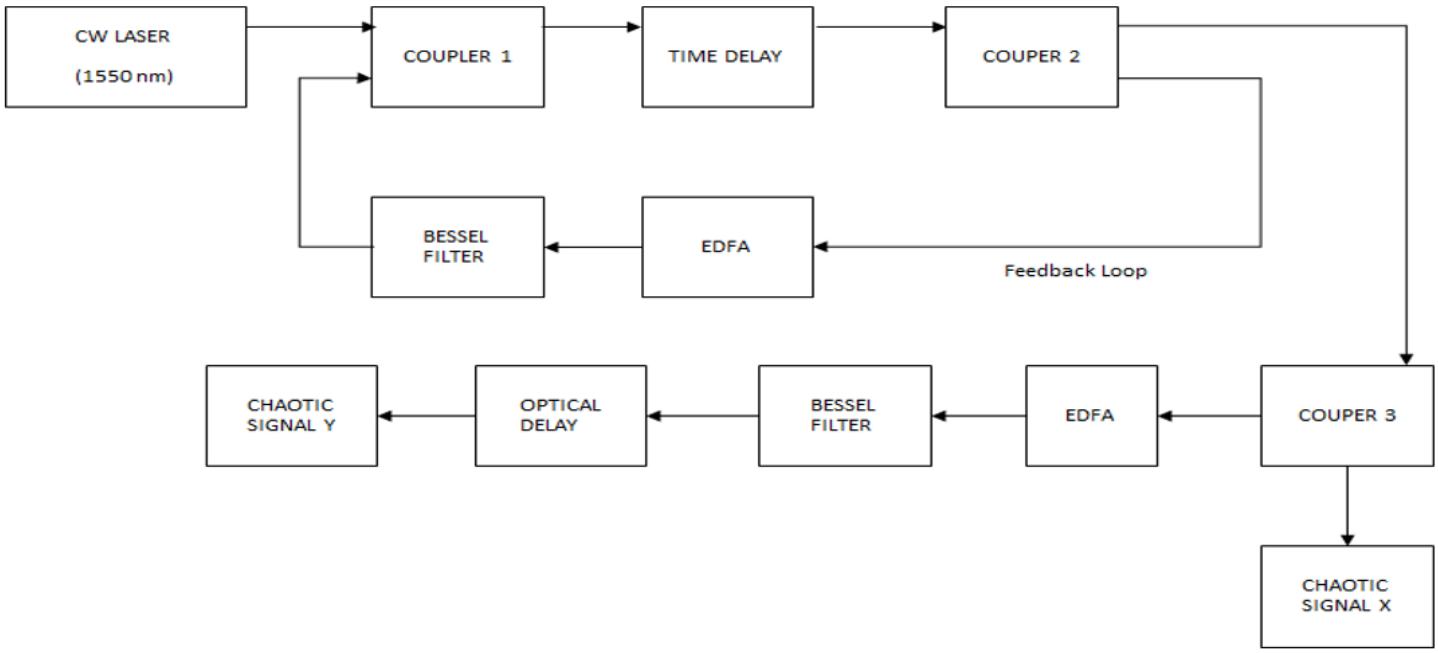
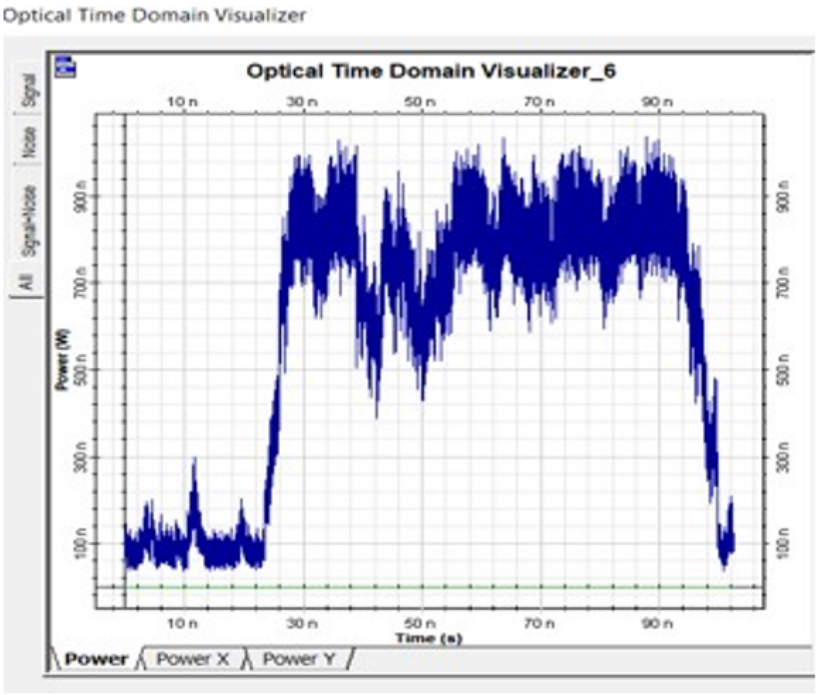
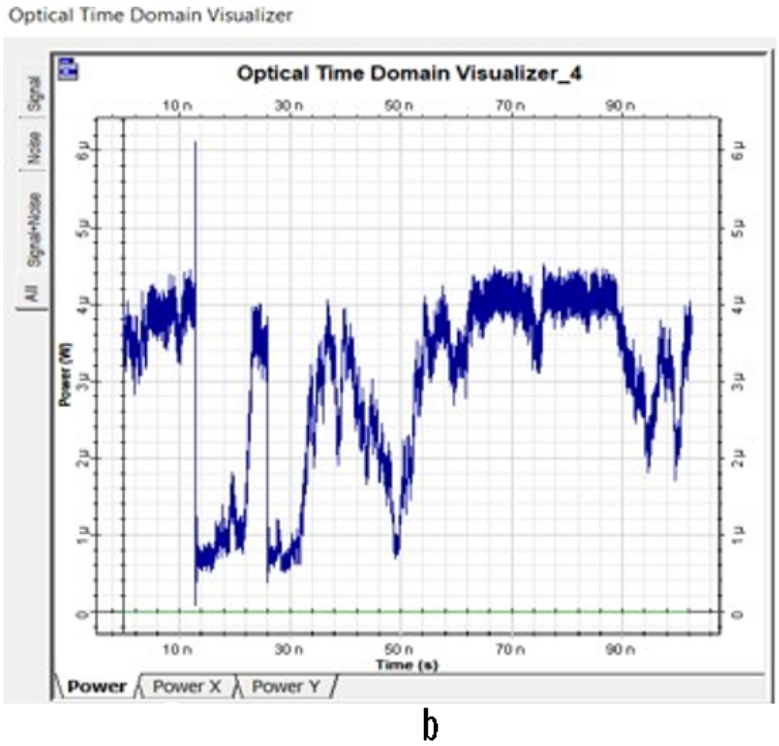


Figure 9

Schematic for generation of Chaotic Signal



a



b

Figure 10

a. Chaotic Signal x. b. Chaotic Signal y

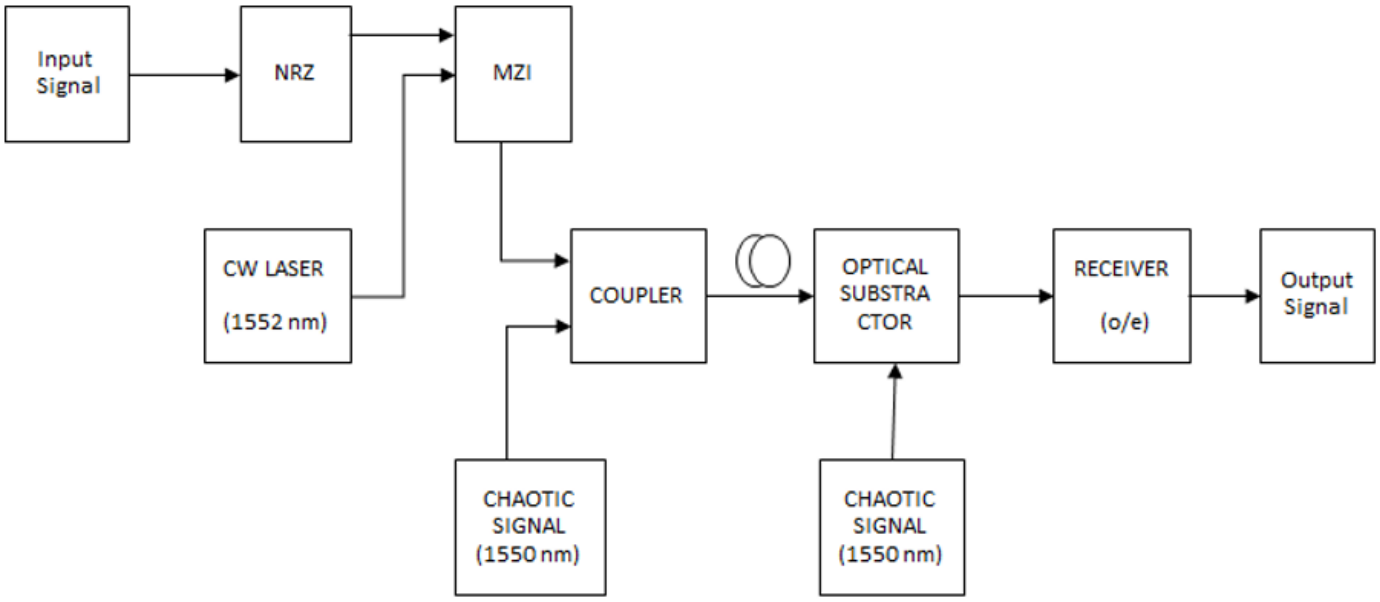


Figure 11

Schematic diagram for chaos masking-based transmission and reception

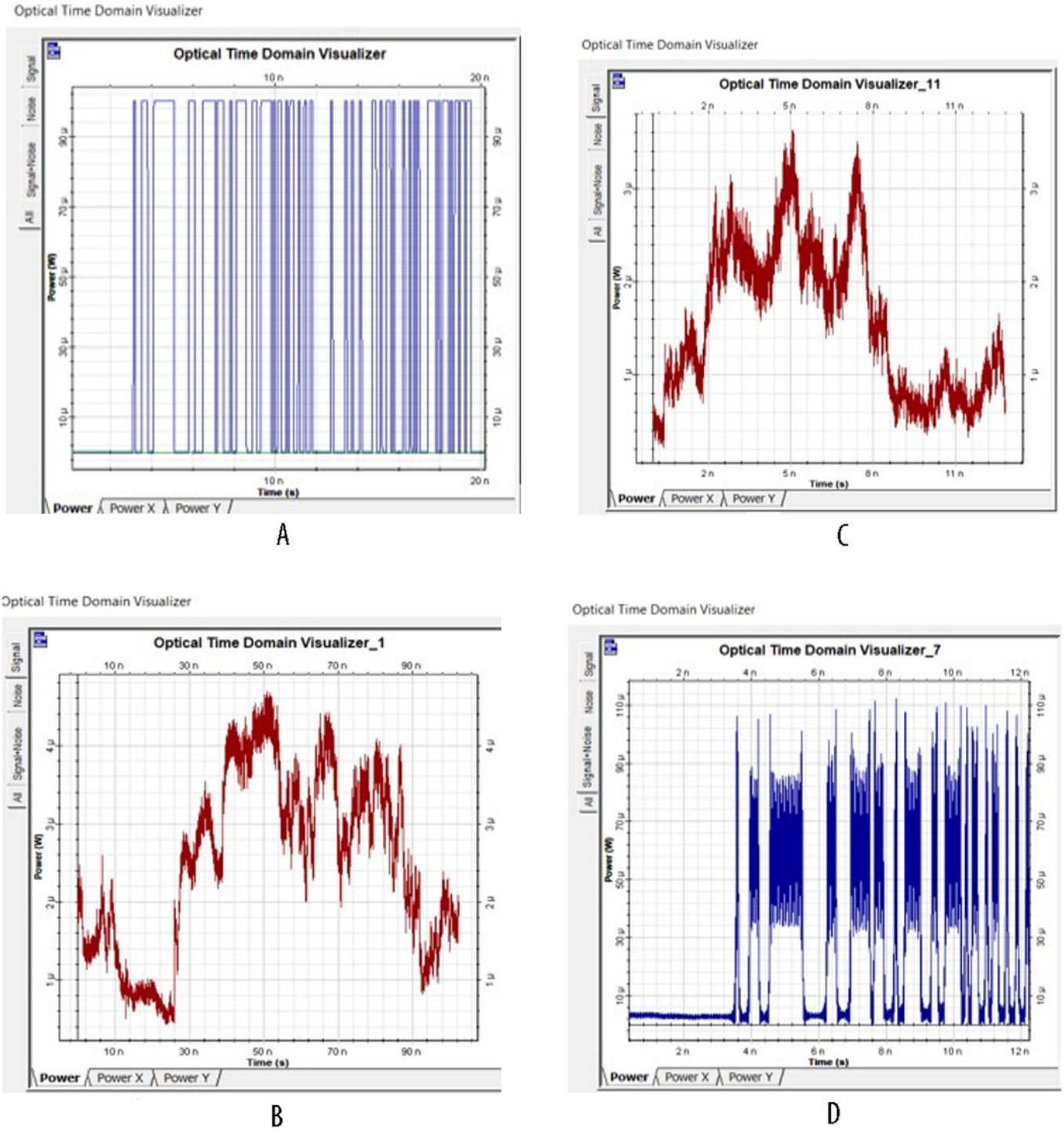


Figure 12

a. PRBS input signal. b. Chaotic Signal. c. Chaos Masked Signal. d. De-masked Signal

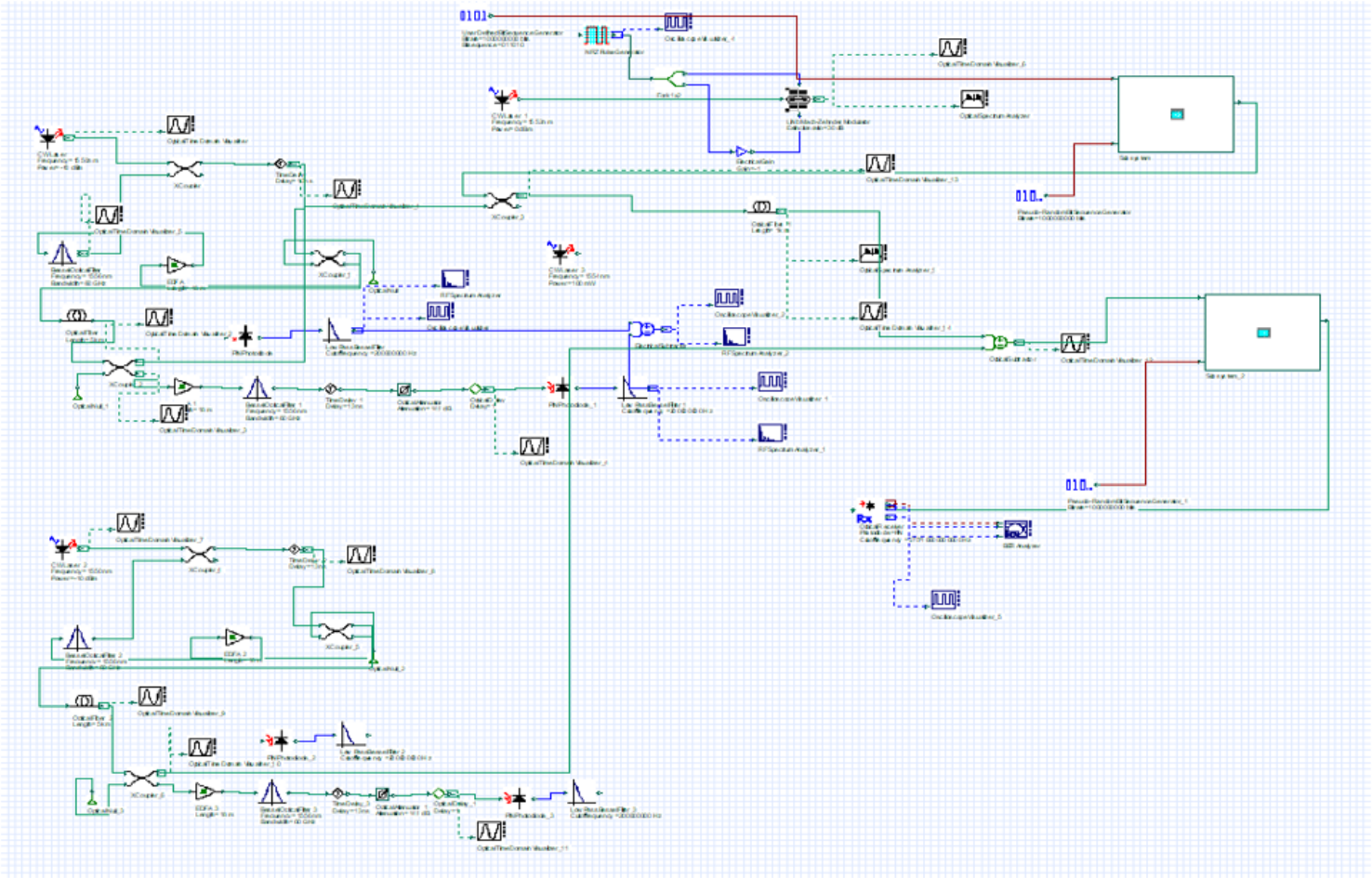
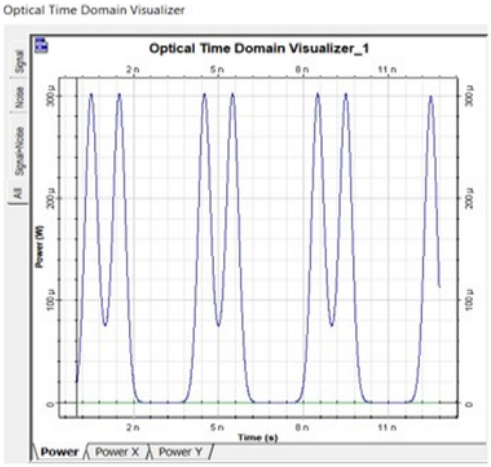
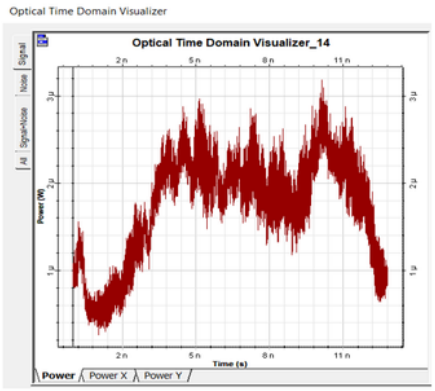


Figure 13

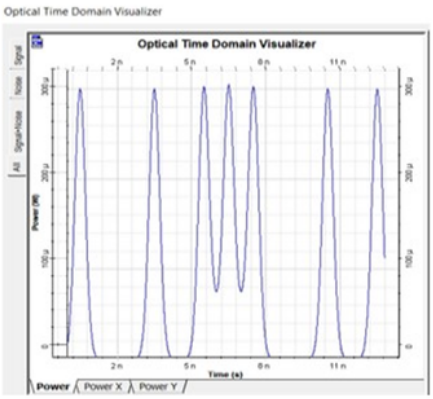
Simulation layout of Encryption and Decryption based on Chaos masking



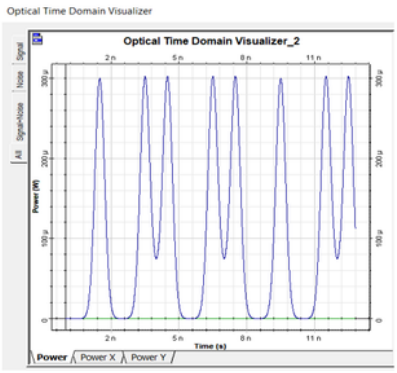
A



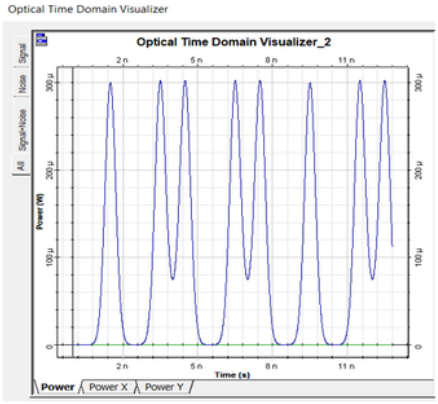
D



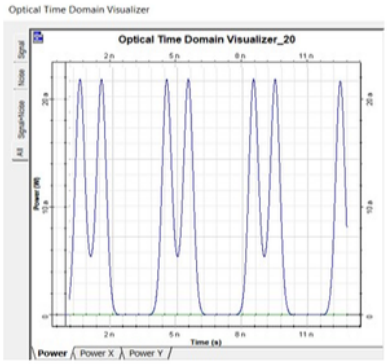
B



E



C



F

Figure 14

a. Input Signal (1100). b. Output of Optical LFSR (1001011). c. Encrypted Signal (0101101). d. Masked Signal. e. De-masked Signal (0101101). f. Decrypted Signal (1100)

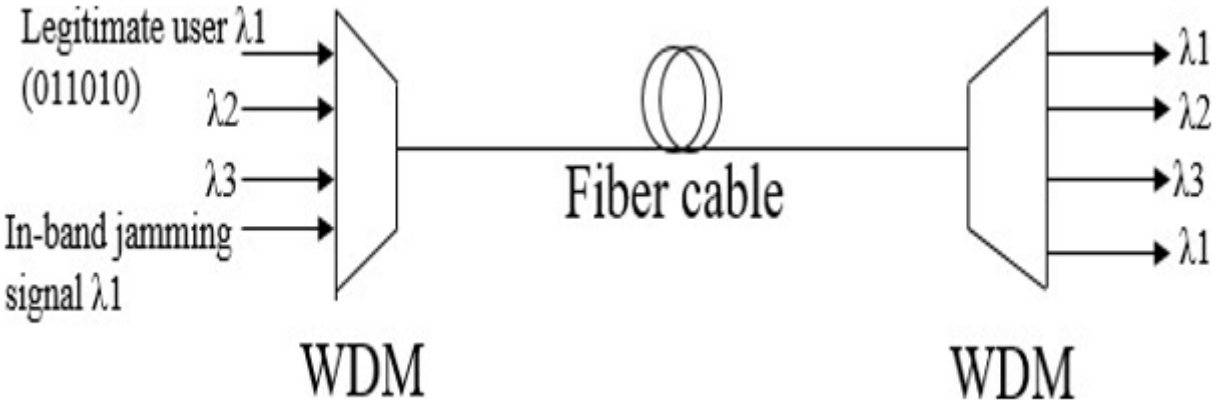


Figure 15

SD attack due to in-band jamming

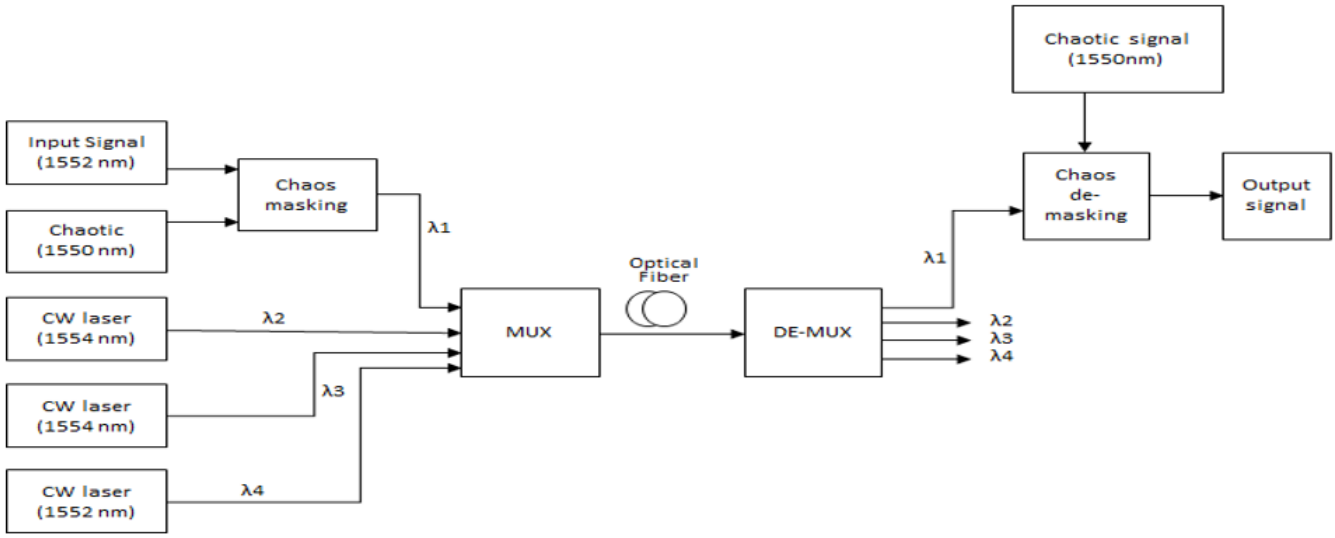
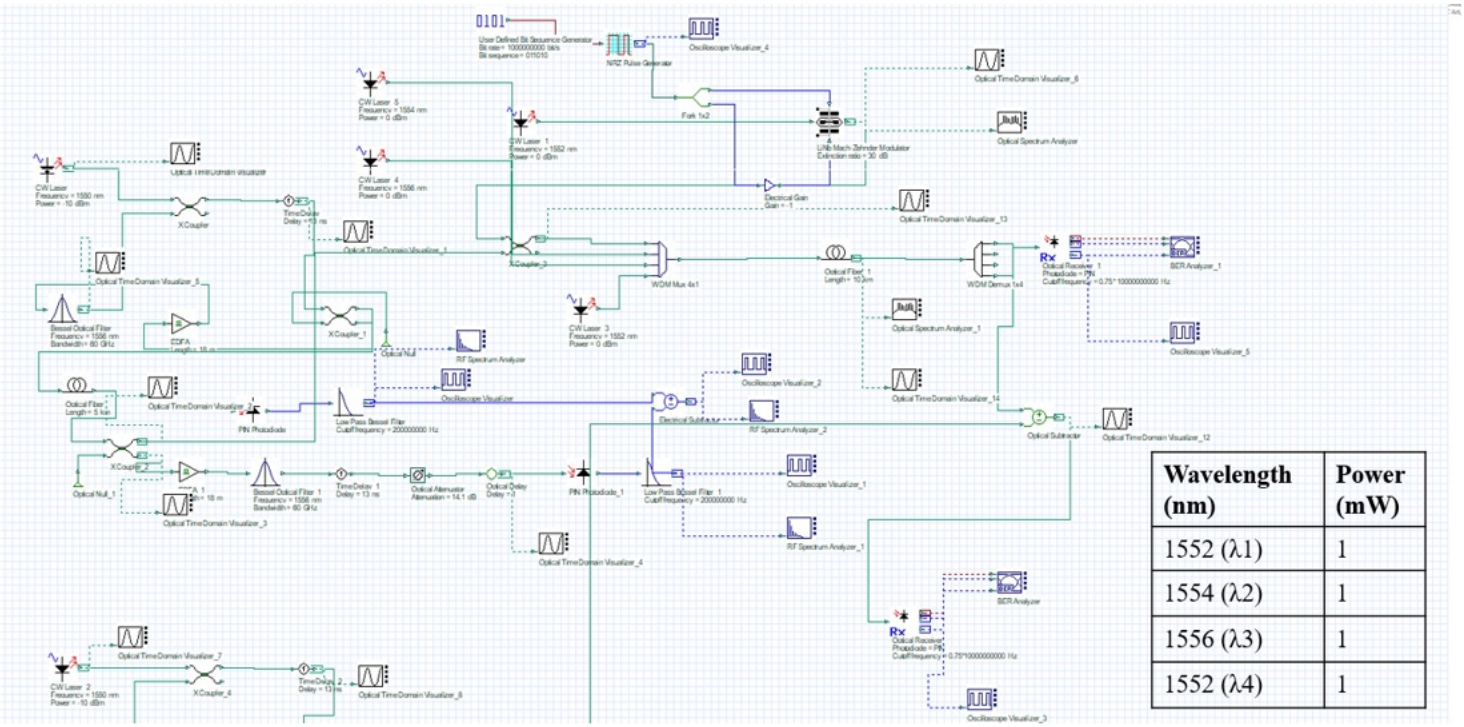


Figure 16

Schematic diagram for in-band jamming



Wavelength (nm)	Power (mW)
1552 (λ1)	1
1554 (λ2)	1
1556 (λ3)	1
1552 (λ4)	1

Figure 17

Simulation layout for In-band jamming

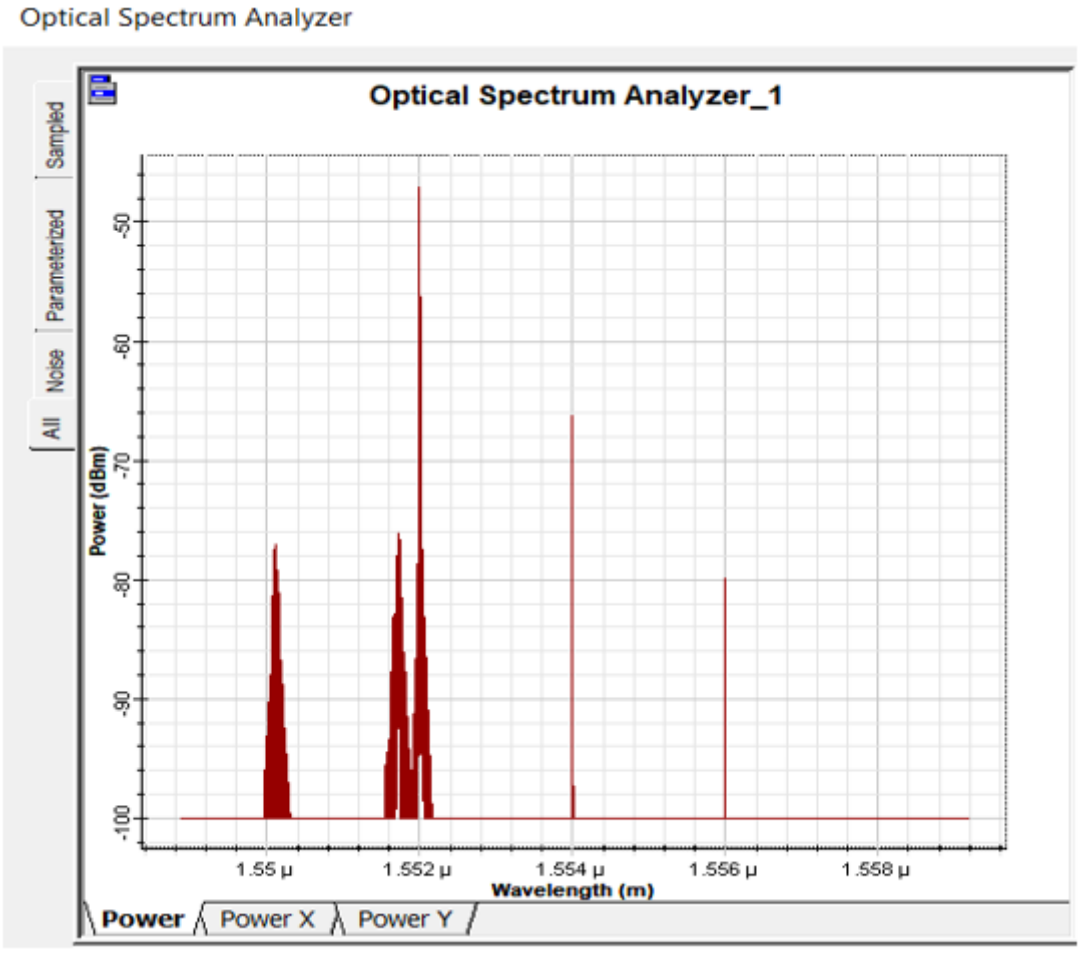


Figure 18

Optical Spectrum at transmitter side

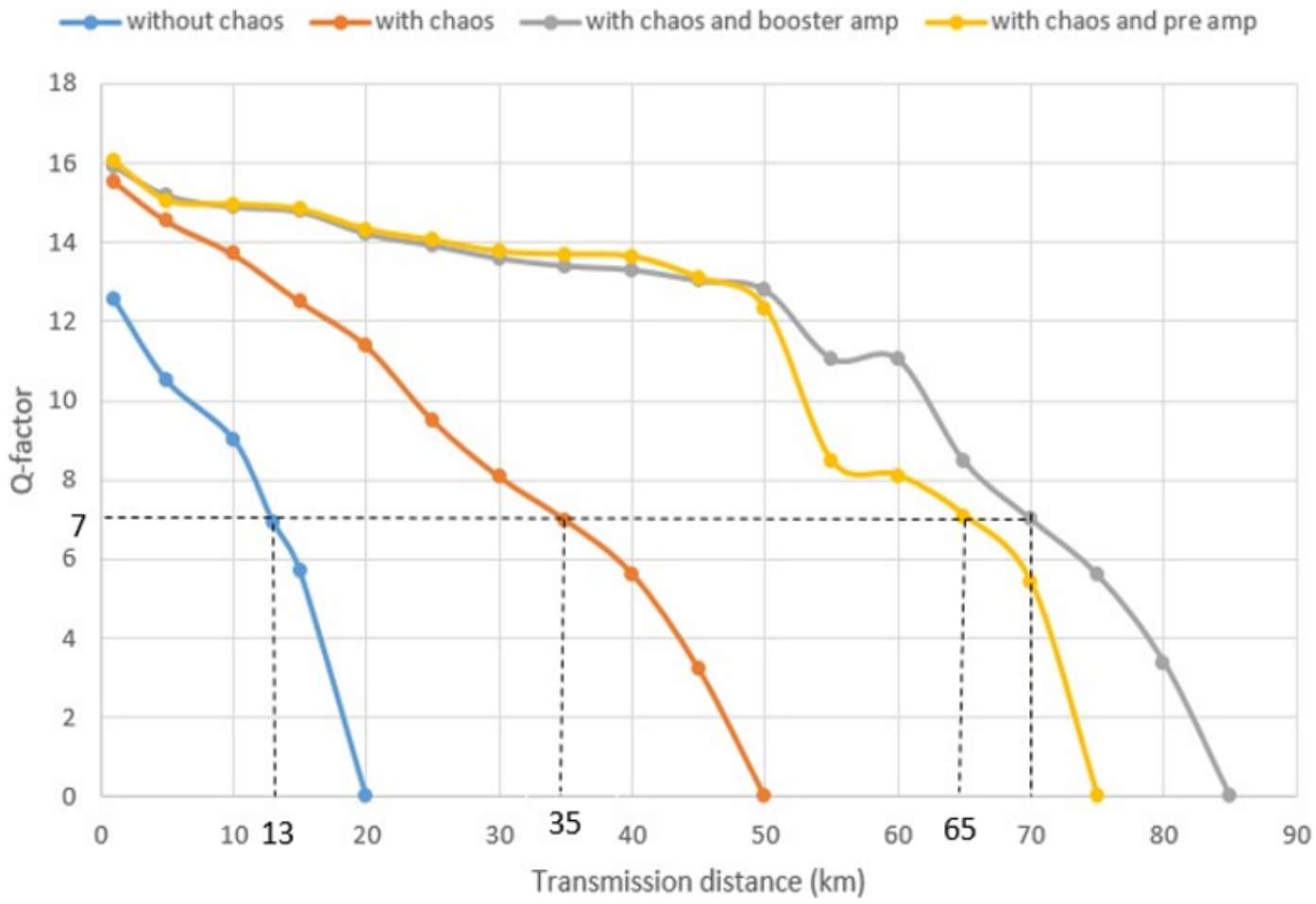


Figure 19

Analysis of security attack in-band jamming

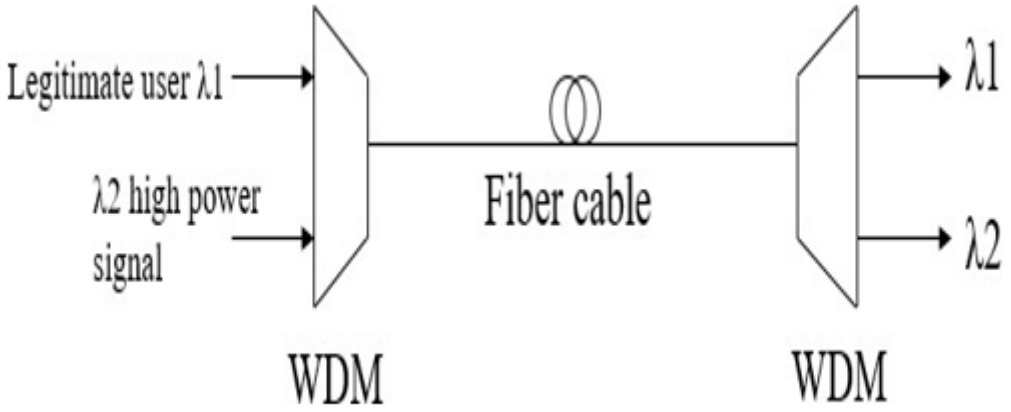


Figure 20

SD in out-band jamming

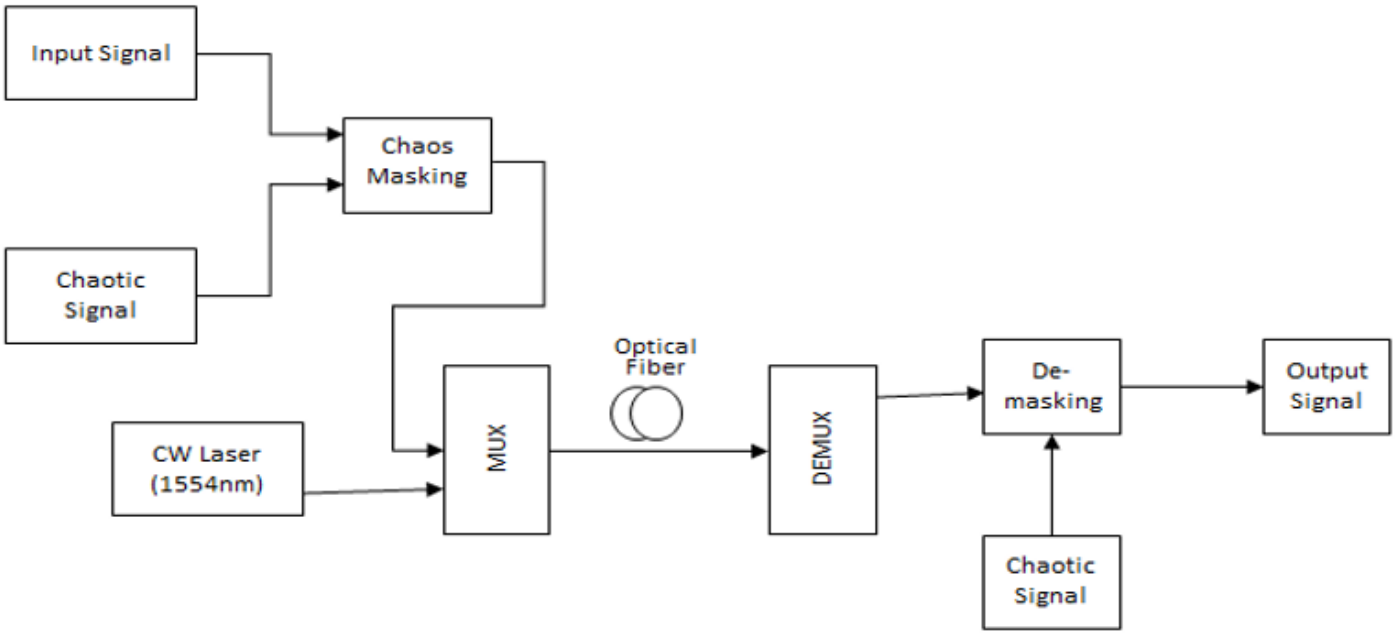


Figure 21

Schematic diagram for out-band jamming

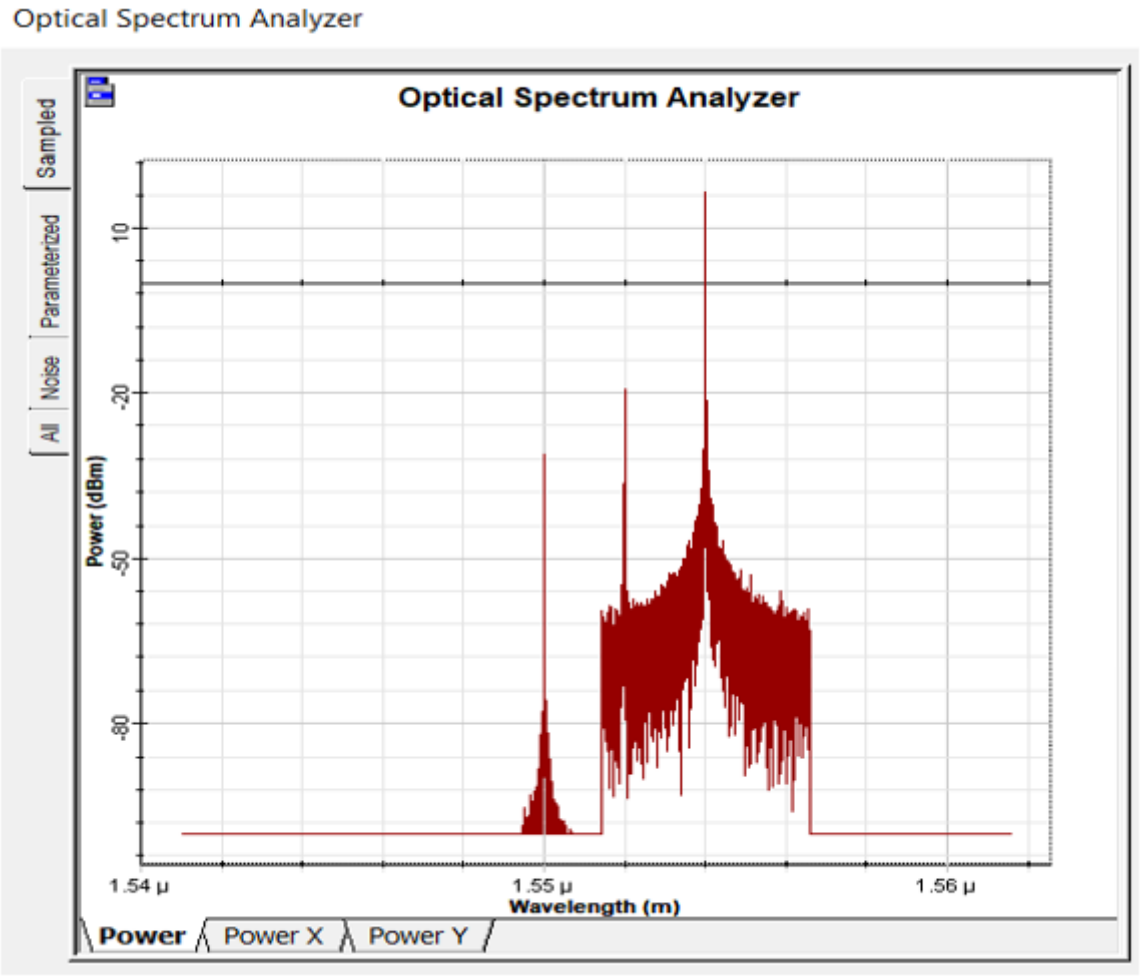


Figure 22

Optical spectrum at transmitter side

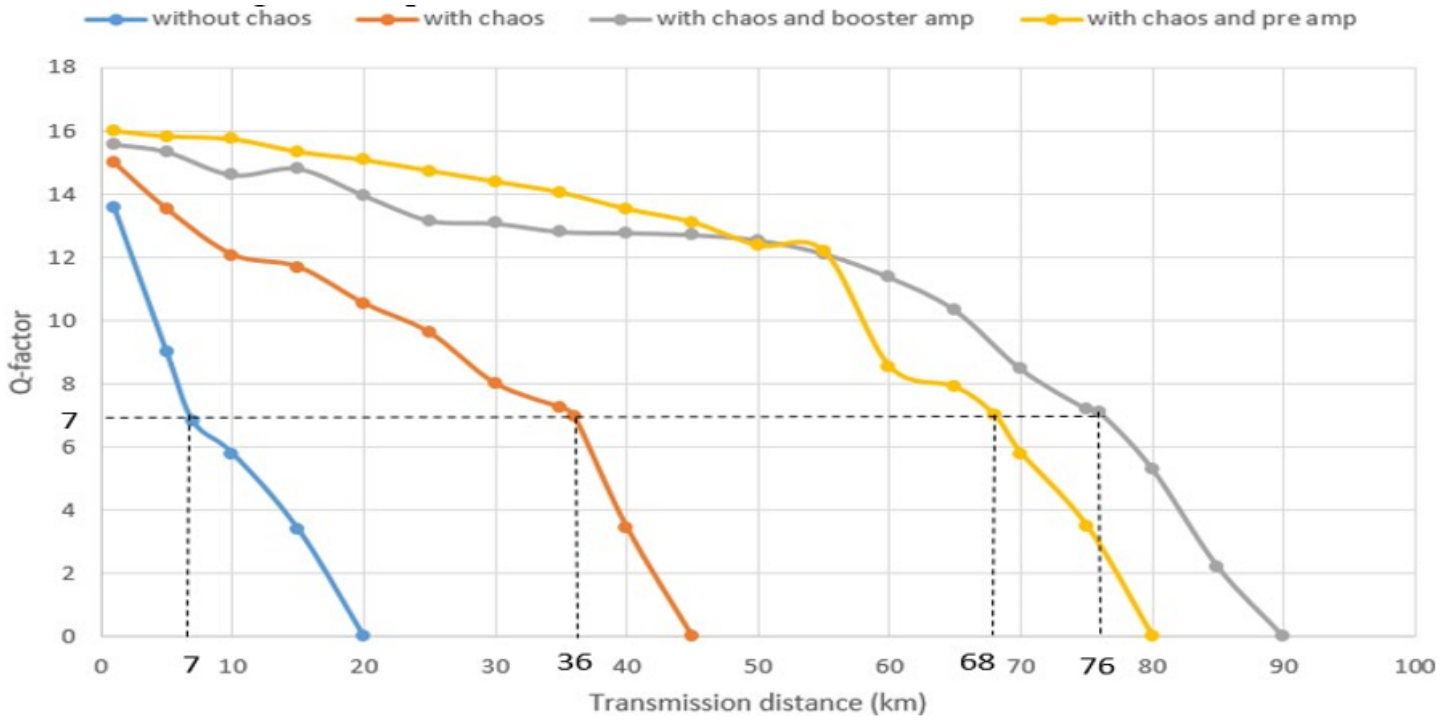


Figure 23

Analysis of security attack out-band jamming

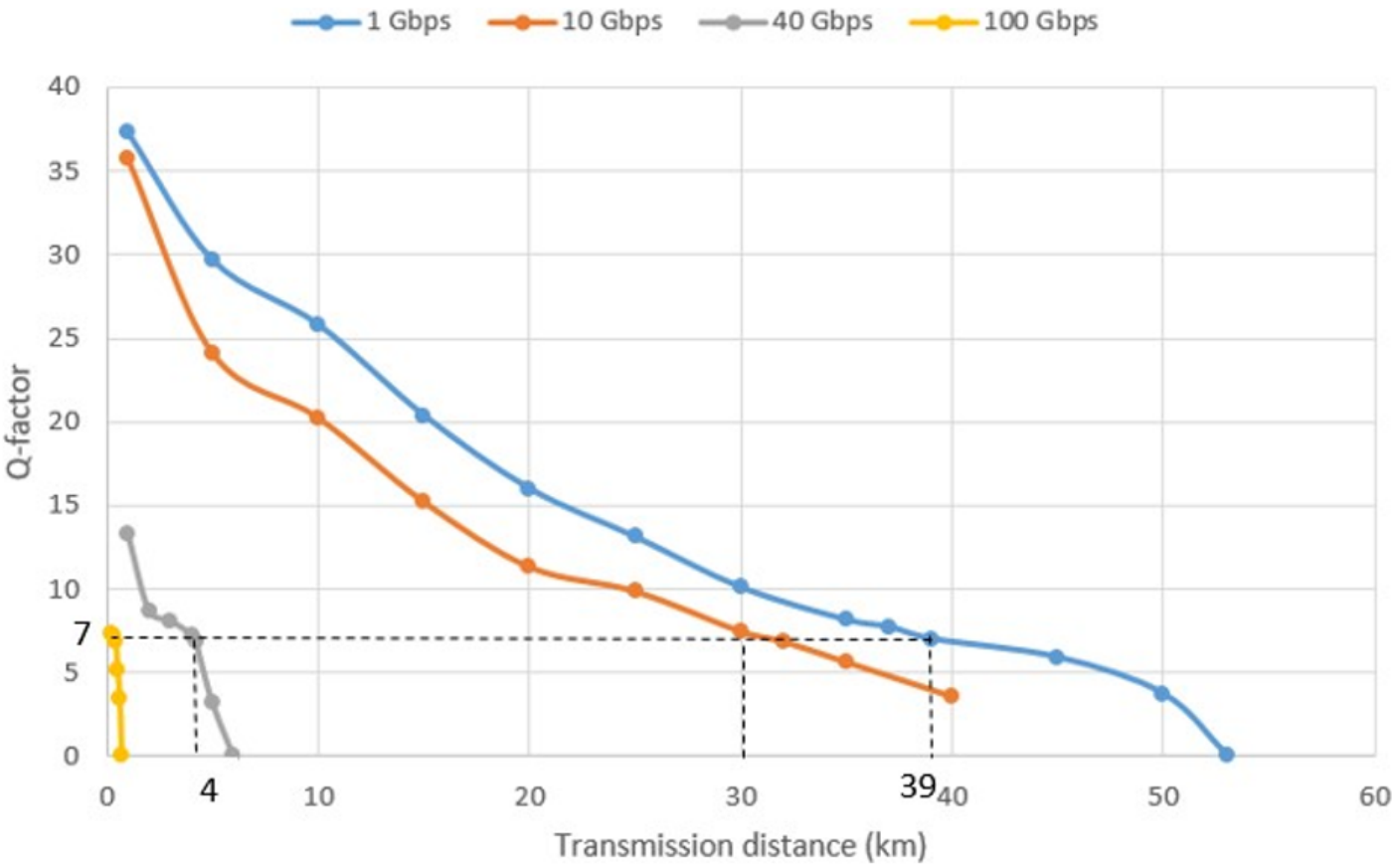


Figure 24

Performance analysis at power 1mW

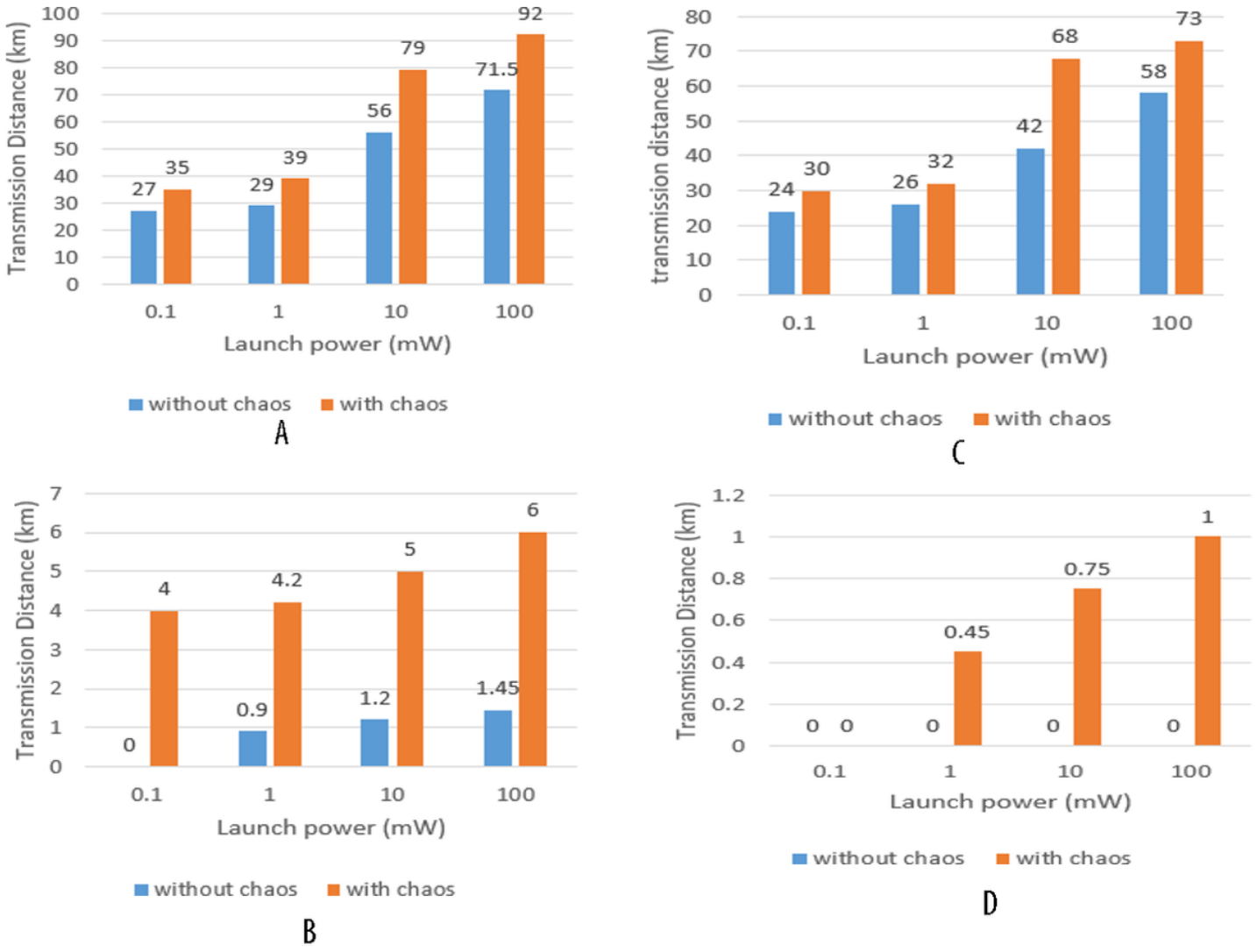


Figure 25

a. Performance analysis at 1 Gbps. b. Performance analysis at 10 Gbps. c. Performance analysis at 40 Gbps. d. Performance analysis at 100 Gbps