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.

Security Enhancement of 2-D DIM Codes using 4 x 1 NOR Logic based on FISO

Simarpreet Kaur (kaursimarpreet1291@gmail.com)
Chandigarh Engineering College https://orcid.org/0000-0001-5103-5455
Simranjit Singh
Punjabi University

Research Article

Keywords: CCDR, MEA, OCDMA, SNR, 2D-DIM, 1D-DIM, AND gate, NOR gate, S-OCDMA, A-OCDMA

Posted Date: May 21st, 2021

DOI: https://doi.org/10.21203/rs.3.rs-437074/v1

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

Version of Record: A version of this preprint was published at Optical and Quantum Electronics on July 22nd, 2021. See the published version at https://doi.org/10.1007/s11082-021-03081-w.

Security enhancement of 2-D DIM codes using 4 x 1 NOR Logic based on FISO

[a*]Dr. Simarpreet Kaur, [b]Dr. Simranjit Singh

[a*]Assistant Professor, Department of Electronics and Communication Engineering, Chandigarh Engineering College, Landran, Mohali, Punjab, India
[b]Assistant Professor, Department of Electronics and Communication Engineering, Punjabi University, Patiala, India

[a*] kaursimarpreet1291@gmail.com, +91-8054039858
[b] sjsingh@pbi.ac.in, +91- 9872552898

Abstract

Security enhancement and bandwidth increase are requirements of ultrafast future optical code division networks that also minimise the latency at nodes without distressing the traffic performance. In OCDMA systems, eavesdropper tries to breach the optical code, and encoded/encrypted data in order to get correct code word of legitimate user. For security enhancement, an ultra high speed 4×100 Gbps two dimensional Diagonal identity matrix (2D-DIM) code and four input single output (FISO) all optical logic gate (AOLG) with private key encryption is proposed and its performance in terms of security is analyzed. Expressions for synchronous and asynchronous transmissions are derived for proposed work and it is perceived that asynchronous transmission has better security. Further performance/security analysis is carried out for different scenarios such as with/without FISO, with 1D-DIM/2D-DIM codes, using 4×1 AND gate/NOR gate in terms of correct code detection rate (CCDR), max. eye amplitude (MEA), Received Q factor, Signal to noise ratio (SNR) at different launched power levels for legitimate user and eavesdropper. Eavesdropper attacked the proposed system but due to FISO layering, private key encryption, and 2D-DIM codes, cannot get acceptable level of CCDR. To the best of author's knowledge, proposed system is ultra high speed with enhanced security and no reported studies have investigated security enhancement at this much ultra high speed.

Keywords- CCDR, MEA, OCDMA, SNR, 2D-DIM, 1D-DIM, AND gate, NOR gate, S-OCDMA, A-OCDMA

1. Introduction

OCDMA systems have been deployed in military and commercial communication systems for data transmission [1] [2]. Network security is a prime requirement in these systems due to highly sensitive information [3]. Three different security schemes are prominent to boost the security of networks, such as (i) algorithmic cryptography (ii) quantum key distribution (QKD) (iii) physical layer cryptography [4]. Algorithm cryptography is used in upper layers or layer 3 and is constantly prone to security breaching. QKD provides high security but with a trade off between distance and data rate. Nowadays, physical layer cryptography has received attention because of enhanced security at intermediate data rates and performances. Further, different strategies which eavesdropper may use to get the signal are energy detection, code interception and differential detection. Eavesdropper can easily detect the "1" and "0" in case of non return to zero modulated transmission with simple photo-detector [5]. Multicode keying is also demonstrated in [6] [7] and differential detection is used in [8]. Multicode keying is the most widely used technique for chiphertexting to randomize data in OCDMA for security purposes. Multicode keying allows

multiple binary bits for each one and zero of authentic user bits but it wastes the bandwidth of the medium. Cryptanalysis is a method to decrypt signals when a key is not known to eavesdropper [9] and different attacks are known-plaintext attack, chosen-plaintext attack and ciphertext-only attack. In the case of a known-plaintext attack, plaintext and ciphertext are known but the key is not available. Chosen plaintext attack is freedom to select plaintext attack in which ciphertext and key are not known. In ciphertext-only attack, plaintext is not available. For security enhancement, many techniques are incorporated into the OCDMA systems, such as AOLG [10] [11], multi-code keying [12], steganography [13], virtual user scheme [14], and etc. Logic gates are prominently deployed in OCDMA systems due to simple encryption and decryption. Semiconductor optical amplifier (SOA) based XOR logic proposed at 120 Gbps [15], code swapping using XOR gate [16], quantum Logic Gate Code with NAND gate [17] and with multi diagonal coded NAND gate [18] etc. Optical logic gates with SOA deployment are studied in literature but SOA 's data rate capability is perceived to be limited [19]. Fiber nonlinearities are a popular technique for generating high speed optical logic gates, according to the picoseconds operation [20]. As researchers studied and engineered optical logic gates with highly nonlinear fibres, they came across the issue of long HNLFs that may decrease system compactness. Logic gates in OCDMA system for security enhancement have two input ports and a single output port (2 x 1 logic). Minimal power losses are desired for long reach systems, but multiple 2 x 1 logic gates introduce power degradation. As a result, more than two inputs based on all AOLG are required to reduce power losses.

In this research article, for the first time, we demonstrate a 4 x 100 Gbps OCDMA system using diagonal identity matrix codes [21] with ciphertexting using private key and four input single output (FISO) all optical DCF-MZI based NOR/AND gates. In order to breach network security, eavesdroppers have to break not only logic gates operations but also private key cipher texting.

Introduction of OCDMA systems and security enhancement are given in Section 1, code construction of 2 D DIM codes is given in Section 2. The concept of all optical gating is mentioned in Section 3. System setup and system parameters are written in Section 4 and this is followed by results and discussion. Graphical representation for different parameters is incorporated in Section 5. Conclusion/outcomes of the proposed work are given in Section 6.

2. Code construction of 2 dimensional DIM codes

For the OCDMA system implementation, DIM codes are used which are presented by us in [19] and these are upgraded to 2 dimensional DIM codes. K is users, W is weight of code and L is length of the code, λ_c cross correlation, and λ_a auto correlation. For the code sequence x=(x_1, x_2, x_3 ..... x_N) and y= (y_1, y_2, y_3 ..... y_N), auto correlation and cross correlation is given as (1) and (2) respectively

$$\text{Auto-correlation: } Ax, x = \sum_{n=0}^{n-1} \mathrm{C[x]C[x]} \quad \text{where } 0<m<N-1 \tag{1}$$

$$\text{Cross correlation: } Cx, y = \sum_{n=0}^{n-1} \mathrm{C[x]C[y]} \quad \text{where } 0<m<N-1 \tag{2}$$

λ_c=0 and λ_a=2 in DIM codes. Final code matrix size is K × L and length of code is K × W. There is freedom to select any weight ≥2. Size of base matrix (I_B) is 2 × $W_{Balance}$ and basic matrix of size Y × Z is given as

$$I_B = \begin{bmatrix} UE \\ LE \end{bmatrix} = \begin{bmatrix} \left[\frac{W}{2}\right] 1's & [W-2]0's \\ \left[\frac{W+2}{3}\right] 0's & \left[\frac{W+1}{2}\right] 1's \end{bmatrix}_{Y \times Z} \quad (3)$$

Where UE and LE are upper and lower elements respectively. Where Y is 2 and Z is equal to W For K users, a final matrix of size K x L is represented by matrix M which illustrates the final code of each user. Construction of M comprises three steps such as M1, M2 and final M can be obtained. First and foremost, in a sub matrix M_1, I_B is repeated K -1 times as depicted in equ. (4)

$$M_1 = \begin{bmatrix} UE \dots \dots \dots \dots \dots \dots \dots LE \\ LE\ UE \dots \dots \dots \dots \dots \dots \dots \\ \dots . LE\ UE \dots \dots \dots \dots \dots \\ \dots \dots \dots . LE\ UE \dots . \dots \dots . \\ \dots \dots \dots \dots \dots LE\ UE \dots . \dots \\ \dots \dots \dots \dots \dots . .\quad LE\ UE \dots \end{bmatrix} \quad (4)$$

In matrix M_2, placement of identity matrix is repeated for K × L times as shown in equ. (5)

$$M_2 = \begin{bmatrix} UE \dots \dots \dots \dots \dots \dots \dots LE \\ LE\ UE \dots \dots \dots \dots \dots \dots \dots \\ \dots . LE\ UE \dots \dots \dots \dots \dots \\ \dots \dots \dots . LE\ UE \dots . \dots \dots . \\ \dots \dots \dots \dots \dots LE\ UE \dots . \dots \\ \dots \dots \dots \dots \dots . .\quad LE\ UE \dots \end{bmatrix}_{K \times L} \quad (5)$$

Final user codes are illustrated in matrix M and it can be obtained by inserting zeros in the vacant positions of matrix M_2 as expressed in equ. (6)

$$M = \begin{bmatrix} UE0000000000000LE \\ LE\ UE000000000000 \\ 000LE\ UE000000000 \\ 000000LE\ UE000000 \\ 000000000LE\ UE000 \\ 00000000000LE\ UE0 \end{bmatrix}_{K \times L} \quad (6)$$

2 D wavelength time spreading code obtained from 1 D DIM code and advantages are

(i) Increase in users using same weight (ii) Increase the security of code (iii) Show zero cross correlation (iv) code length unchanged

For the conversion of 1 D DIM codes (6) into 2 D DIM codes, dimension of time (t) is added to (6) and then final matrix is M_T

$$M_T = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \\ \lambda_5 \\ \lambda_N \end{bmatrix} \begin{bmatrix} t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 t_9 t_{10} t_N \\ - - - - - - - - - - - \\ \text{UE0000000000000LE} \\ \text{LE UE000000000000} \\ \text{000LE UE000000000} \\ \text{000000LE UE000000} \\ \text{000000000LE UE000} \\ \text{00000000000LE UE0} \end{bmatrix}_{K \times L} \quad (7)$$

Wavelengths are representing row wise and time in column. Time t is selected as

$$t_N = j_N \times t_b \quad (8)$$

where j is number of time the slot j (1,2,3,4…..N) and t_b bit time slot, calculated as

$$t_b = \frac{1}{bit\ rate} \quad (9)$$

Performance of comparison performed in reported work [19] and 1D DIM codes emerged as an optimal code out of double diagonal weight, multi diagonal weight, enhanced diagonal weight, walsh hadamard code. Therefore, in this work we are upgrading 1D DIM code to 2D DIM codes.

3. Concept of all optical gating

Figure 1 represents the two co-propagating optical signals. Four wave mixing (FWM) occurs inside nonlinear medium and represented in Figure 2. Mixed product of N number of wavelengths is given as [22]

$$N = \frac{N^2}{2}(\mathrm{N} - 1) \quad (10)$$

Efficiency $\boldsymbol{\eta}$ for equal channel spacing, same input power, for fiber is given as

$$\eta = \frac{n_2 \mathrm{P}}{A_{eff} D (\Delta\lambda)^2} \quad (11)$$

where P is the power of the channel, n_2 is nonlinear refractive index, A_{eff} is fiber effective area, $\Delta\lambda$ is spacing between channels and D is chromatic dispersion.

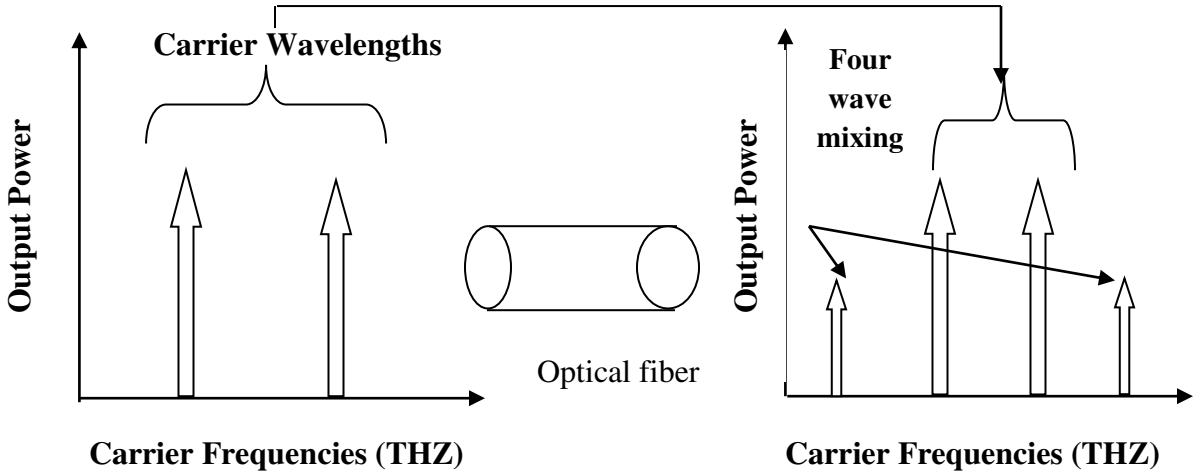
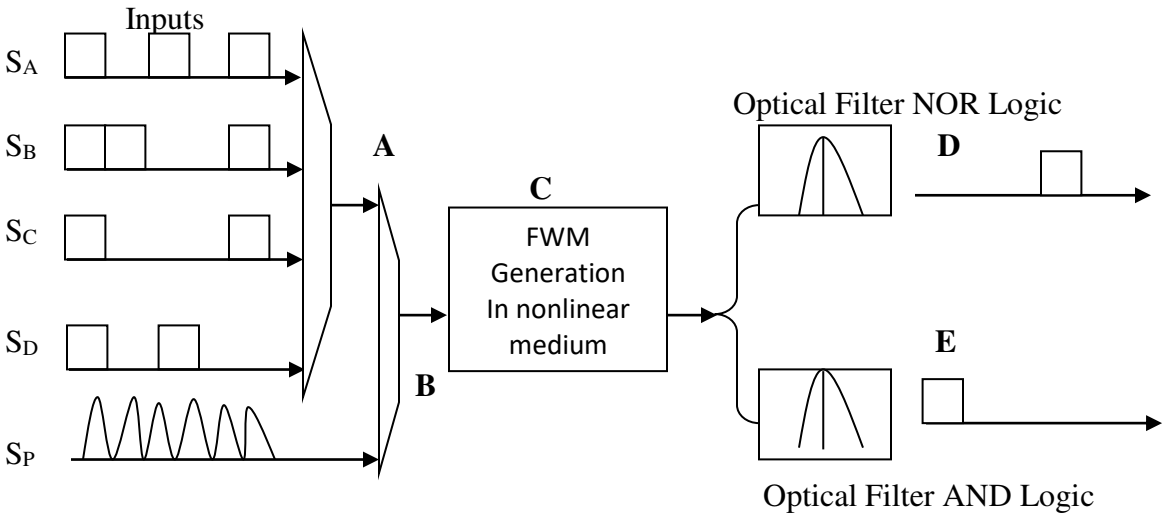


Figure 1 Carrier spectrums of (a) input signal and (b) after nonlinear medium

Dispersion compensation fiber (DCF) in Mach-Zehnder interferometric (MZI) configuration employed and Compensation of dispersion with DCFs is prominently observed in optical communication systems [23] [24] and has negative dispersion from -70 to -90 ps/nm/km. Power of signal or probe significantly affects the FWM in DCF and higher the probe power, more is the signal quality. On contrary, high pump power, suppress the power level of ones and zeros. For the better power and shape of signal pulse, optimal power levels are needed. We present four input single output AND/NOR gate for security enhancement using DCF-MZI configuration. Output at AND will be true if all the inputs are true and for NOR gate to be true, all input bits should be false. In simple works, 4 input bits having 0 on all ports provide 1 for NOR only and having 1 on all ports provide 1 for AND gate only. Concept diagram of FISO is represented in Figure 2 using DCF-MZI structure and gate logic tables are shown in Table 1 (a)(b).



S-signal, P-pump

Figure 1 Proposed FISO AND/NOR gate using DCF-MZI

Table 1(a) NOR logic for 2 inputs (Truth table)

A	B	Output
0	0	1
0	1	0
1	0	0
1	1	0

Table 1(b) AND logic for 2 inputs (Truth table)

A	B	Output
0	0	0
0	1	0
1	0	0
1	1	1

Four signals S_A, S_B, S_C, S_D generated from optical laser source, amplified with erbium doped fiber amplifier (EDFA) and for the wavelength multiplexing, send to part (A). P_k is the private key (explained in section 4) as depicted in part (B).

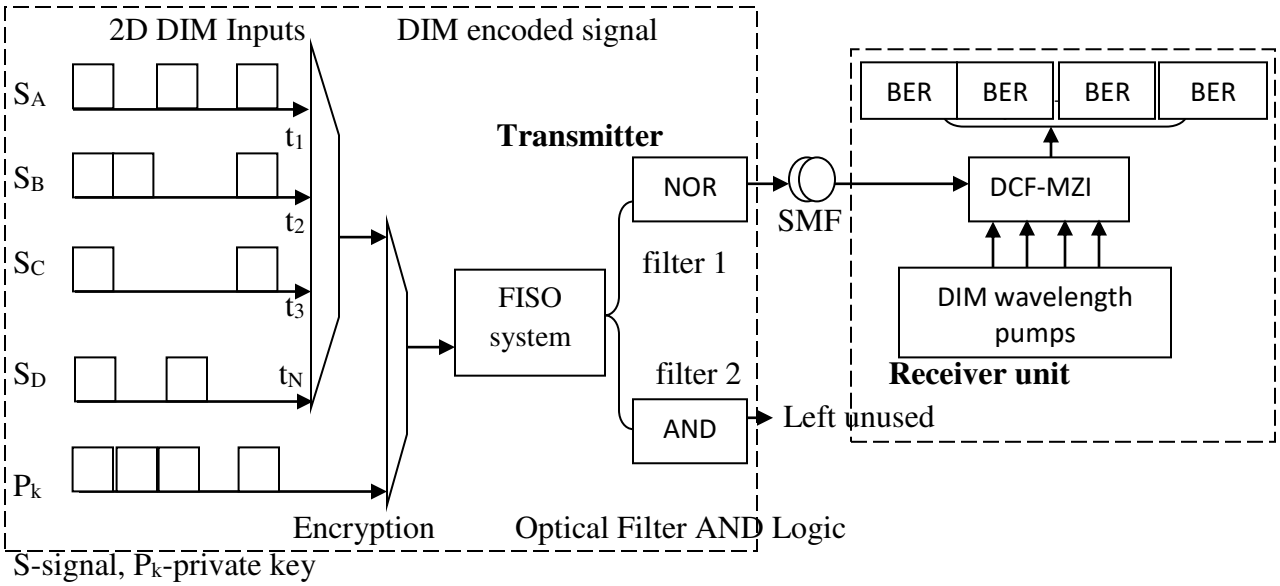


Figure 2 Proposed FISO AND/NOR gate using DCF-MZI

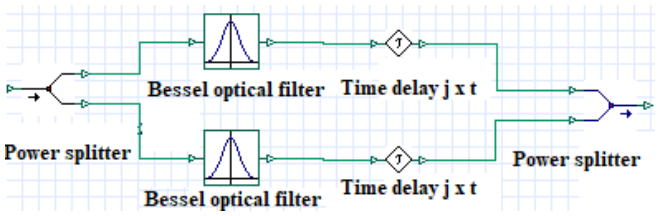
FWM nonlinear medium in part (C) consists of two DCFs in MZI configurations for destructive and constructive interference. Upper port of the FISO unit shows the carriers at the OSA while lower port show only noises. Therefore constructive interference is on upper port and further in order to analyze the output data behaviour, signal is divided into two parts and each part consists of optical Bessel filers of variable frequencies. Varied frequencies are used to check the wavelengths which will provide data according to some logic gates. It is observed that data after filter 1 act as NOR logic data and after filter 2 is acting as output data of AND gate. Part (D) shows that NOR gate is high when all the inputs are low and in case of part (E) which is acting as AND gate, will provide high output when inputs are also high. Proposed FISO system is used for security enhancement of OCDMA system and legitimate user security system is depicted in Figure 2. Four user 2D DIM data passed through FISO system and in order to baffle eavesdropper, a private key (P_k) in place of pump signal is multiplexed with DIM data and passed through DCF-MZI. AND gate output from FISO system is neglected to increase the number of cases to get legitimate data and keep eavesdropper in illusion. NOR gate output communicated through optical fiber and then passed through DCF-MZI. Pumps equal to DIM user wavelengths are combined to DCF-MZI then again NORing with P_K is performed to get legitimate user data.

4. System Model

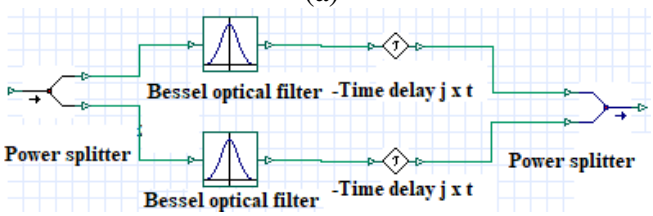
Figure 2 represents the 2D DIM code with optical layering and private key based OCDMA system. Legitimate data can be attacked in OCDMA networks and eavesdropper can use known plaintext attack to get the authentic information. In security enhanced OCDMA systems, first and foremost data layer security is performed and optical encoder then performs physical layer security. Optical decoding implemented at receiver to retrieve legitimate data and in this work, wavelength-time spreading codes are implemented. Security enhancement of 2D DIM based OCDMA system is proposed and investigated in Optiwave Optisystem^{TM}. Four users are selected from DIM code matrix having weight (W) 2, code length (L) 8 and cross correlation 0. Code matrix for 2D DIM code is given as

$$DIM = \begin{bmatrix} t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 \\ - - - - - - - - \\ 1\,0\,0\,0\,0\,0\,0\,1 \\ 0\,1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,1\,1\,0 \end{bmatrix} \quad (12)$$

Laser array with eight frequencies (193.1 to 193.8 THz) each at 100 Gbps provide continuous pulse train and spacing between channels is 100 GHz. From the power optimization, 10.877 dBm input power is selected and pseudo random bit sequence generator data is modulated with NRZ and further electrical to optical conversion is performed by Mach-zehndar modulation (MZM). In order to realize 2D DIM users, time delays (t) are added to each wavelength as shown in Figure 3 (a) and t is calculated as equation (8) (9) . Time delays are t_1 =0.1 ns, t_2= 0.2 ns, t_3= 0.3 ns, t_4= 0.4 ns, t_5= 0.5 ns, t_6= 0.6 ns, t_7= 0.7 ns, and t_8= 0.8 ns. After that data multiplexed and joined with private key P_k. Simulation parameters are given in Table 2 (a) (b). P_k has input power of -0.96 dBm and all the signals fed to FISO unit which consist of two DCFs and a MZI switch. DCFs of lengths 0.09 km are placed in two arms of MZI i.e. lower arm and upper arm. FWM occurs in both the arms and at the output of MZI, there are two ports and it is observed that lower port provide constructive interference. Constructive port output has different FWM wavelengths and outputs of these wavelengths are checked with optical filters so as to get the specific logic operation. At frequency 193.93 THz, system act as NOR gate because provide output "1" when all the input bit are "0" and act as AND when all the input bits are "1". AND gate realized through optical filter having frequency 194.18 THz. NOR gate has high output power as compared to AND gate and therefore we have used NOR gate for further transmission and left AND gate output to baffle eavesdropper.



(a)



(b)

Figure 3 General Time spreading encoder at (a) transmitter (b) receiver

In [25], code interception by eavesdropper for single user is given and probability to comprehend legitimate user data at eavesdropper is denoted as P_C and it is expressed as

$$P_C = (1 - P_M)^W (1 - P_F)^{(L \times \lambda - W)} \quad (13)$$

Where P_M is miss detection of transmitted pulse, P_F is false detection when no pulse transmitted, code length is L, code weight W and no. of wavelengths are λ.

$$P_M = 1 - Q\sqrt{\frac{2E}{N}, \sqrt{\frac{2\gamma}{N}}} \quad (14)$$

$$P_F = \exp\left(-\frac{\gamma}{N}\right) \quad (15)$$

Marcum Q function is expressed in equ. (16), detection threshold is γ, and Peak pulse energy to the noise power spectral density is E/N.

$$Q(a, b) = \int_b^\infty xI_0(ax)\exp\left(\frac{x^2+a^2}{2}\right)dx \quad (16)$$

Where first order modified Bessel function zeroth order is represented as $I_0(x)$.

In linear cryptanalysis in which output ciphertexts are utilized, is termed as known plaintext attack [26]. Time required obtaining output cipher texts by eavesdropper using linear cryptanalysis is given as:

$$T = \sum_{n=1}^{\infty} n(T_{en} + T_{in})C_{dn} \quad (17)$$

Time required to perform encryption on Advanced encryption standard is denoted by T_{en}, and time needed to intercept complete code once is T_{in}. Probability of complete detection of n user codes at eavesdropper is represented as C_{dn}.

$$C_{dn} = (1 - P_C)^{n-1}PC \quad (18)$$

SMF of 50 km is deployed and output is given to logic gate decoder such as DCF-MZI unit having same DCFs lengths with eight laser wavelengths same as DIM transmitter wavelengths/frequencies. The FWM again emerges and data from 193.93 THz spread on other laser wavelengths and specific legitimate output wavelength selected with demultiplexer. Negative time delays corresponding to specific user are given to wavelengths such as $t_{1=}$ -0.1 ns, $t_{2=}$ -0.2 ns, $t_{3=}$ -0.3 ns, $t_{4=}$ -0.4 ns, $t_{5=}$ -0.5 ns, $t_{6=}$ -0.6 ns, $t_{7=}$ -0.7 ns, $t_{8=}$ -0.8 ns and general receiver is shown in Figure 3 (b). PIN photodetector, low pass filter, 3-R regerator, BER analyzer are together make receiver.

Table 2 (a) System parameters for DIM OCDMA system

Parameters	Values
DIM Users	4
Frequencies	193.1 THz-193.8 THz
Input Power	10.877 dBm
Frequency spacing	100 GHz
Data rate	100 Gbps
Total capacity	4 × 100 Gbps
L,W, λc	8, 2, 0
Modulation format	NRZ
SMF	50 km
Receiver	PIN, low pass Bessel filter, 3R-regerator

Table 2 (b) FISO system parameters

Parameters	Values
Module	DCF-MZI
Optical amplifier, Gain, noise figure	EDFA, 25 dB, 4 dB
DCF Length	0.09 km
No. of DCFs	2
Nonlinear index	2.6×10^{-20} m^2/W
Dispersion	-85 ps/nm/km
Attenuation in DCF	0.5 dB/km
A_{eff}	50 μm^2
λ_{NOR}/f_{NOR}	1545.87 nm/ 193.93 THz
λ_{AND}/f_{AND}	1543.88 nm/194.18 THz

5. Results and Discussions

Equation (17) reveals the increase and decrease in the time complexity to detect the legitimate user data at eavesdropper at different parameters i.e. for instance, signal to noise ratio (SNR) level increase at eavesdropper reduce the time complexity. At lower levels of SNR, for eavesdropper, security increase and therefore complex codes preferred. For multiple users, there are two transmission schemes such as synchronous and asynchronous transmission.

5.1 Synchronous OCDMA systems (S-OCDMA)

OCDMA encoded total N users with NRZ data linecoding travel inside fiber simultaneously operating at B bits per second. Probability of transmitting logic '1' by special user is ½ at given bit period and for same bit period, '0' is transmitted by N-1 users is $1/2^{N-1}$. Probability of transmission of '1' when other user transmits '0' assuming that there are independent data bits from each other is given as $N/2^N$. Time for which eavesdropper wait to get bit of single user is $2^N/(B\times N)$.

5.1.1 Time required for breaching S-OCDMA security

Code interception is used to detect the single legitimate user code by eavesdropper and ciphertext information can be taken. Once eavesdropper gets the ciphertext, encryption key will decipher.

Time required for breaching S-OCDMA security is given as

$$T_R = \sum_{n=1}^{\infty} n \left(T_{ea} + T_{ei} + \frac{2}{B\times N}^{N} \right) P_{en} \tag{19}$$

Where T_{ea} is eavesdropper time to attack encryption algorithm, T_{ei} is eavesdropper time to get address code after interception. P_{en} is eavesdropper probability till nth interception to get correct user's code.

$$P_{en} = \frac{(1-P_C/N)^{n-1}PC}{N} \tag{20}$$

If total users are not known by eavesdropper which are simultaneously travel, eavesdropper perform code interception on each bit period and thus probability is given as

$$P_{ens} = \frac{(1-P_C/2^N)^{n-1}PC}{2^N} \tag{21}$$

5.2 Asynchronous OCDMA systems (A-OCDMA)

In A-OCDMA, no synchronization is needed and in this case, for the duration of transmitting '1' by one user, fraction of 2 adjacent bits is transmitted for the same duration by all other users (N-1). For eavesdropper to differentiate one user, when it transmit '1' for fixed duration and all other users (N-1) for same time duration must transmit 2 adjacent '0'. Probability of transmit '1' by one user is ½ at given time period and for N-1 users, which transmit '0' on two overlapped bits, probability is $1/2^{2N-2}$. Eavesdropper time to wait one user transmission is $2^{2N-2}/(D\times N)$.

5.2.1 Time required for breaching A-OCDMA security

Time required for breaching S-OCDMA security is given as

$$T_R = \sum_{n=1}^{\infty} n \left(T_{ea} + T_{ei} + \frac{2}{B\times N}^{2N-1} \right) P_{en} \tag{22}$$

Comparison of S-OCDMA and A-OCDMA in terms of time required by eavesdropper to get the correct code is clear from equ. (20) and equ. (22) such that due to the presence of greater number of cases in A-OCDMA ($\frac{2}{B\times N}^{2N-1}$) as compared to S-OCDMA ($\frac{2}{B\times N}^{N}$), the security of former system is more i.e. time required by eavesdropper to get the correct code is more. Therefore A-OCDMA is more secure than S-OCDMA systems.

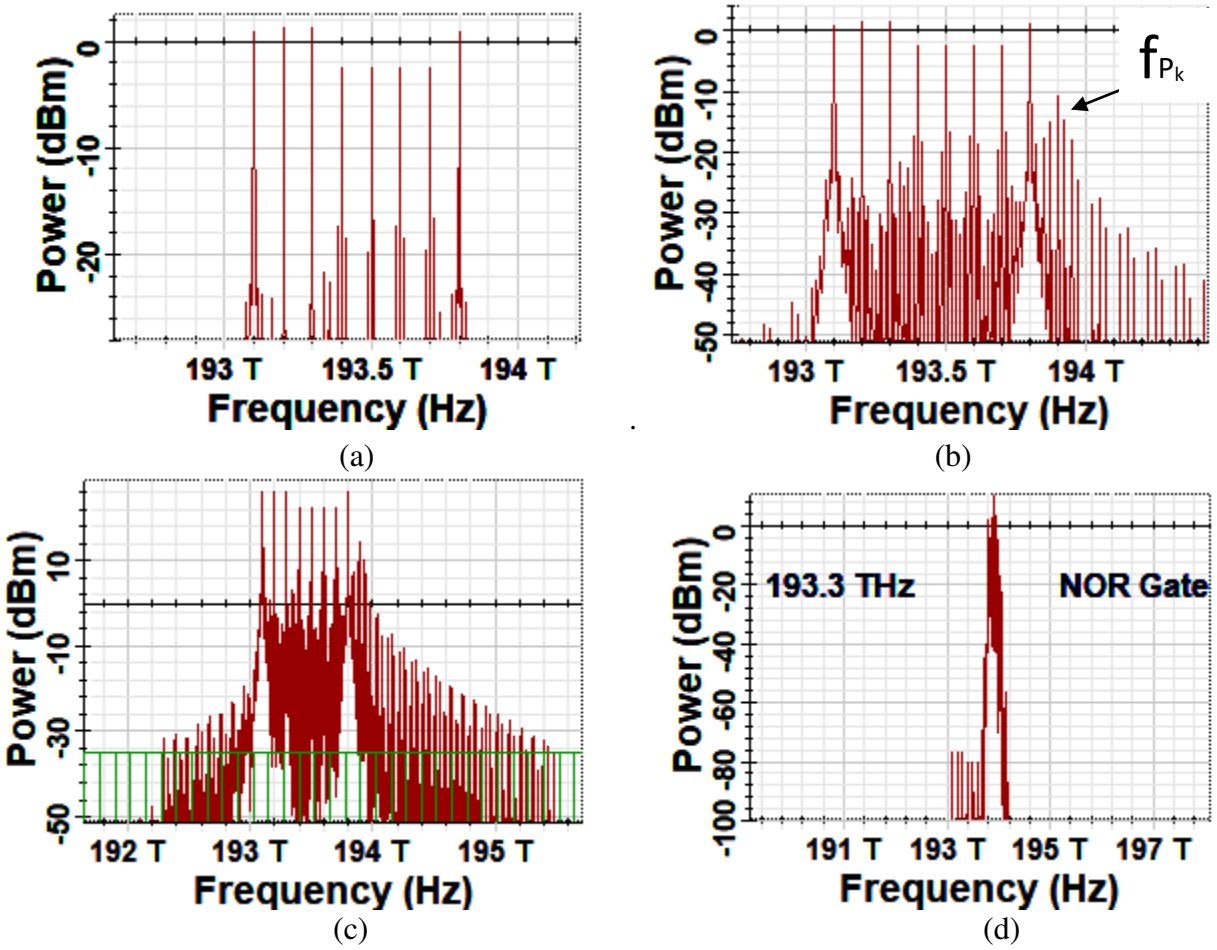
If total users are not known by eavesdropper which are asynchronously travel, eavesdropper perform code interception on each bit period and thus probability is given as

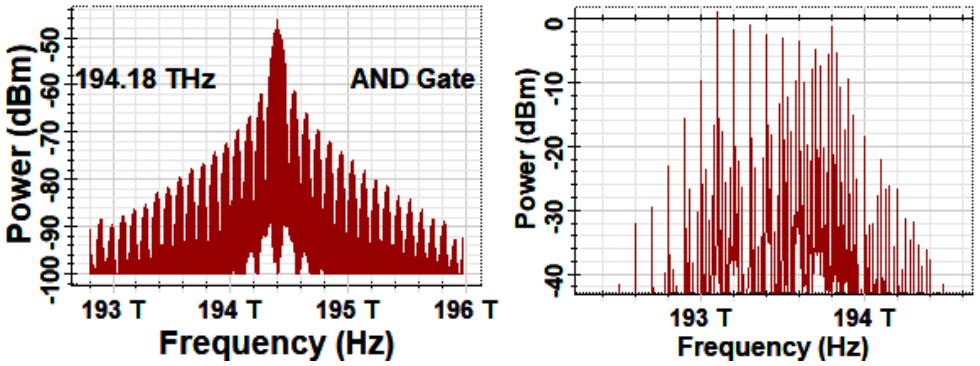
$$P_{ena} = \frac{(1-P_C/2^{2N-1})^{n-1}PC}{2^{2N-1}} \tag{23}$$

Number of users in the optical network is directly proportional to the security of the system and if eavesdropper do not know the users in the system, security improves and when it get to know total users, security reduces as clear from equ. (21) and equ. (23).

5.3 Performance and security analysis in Optisystem

2-D DIM OCDMA system having capacity 4×100 Gbps over 50 km using FISO unit is investigated in Optisystem software.

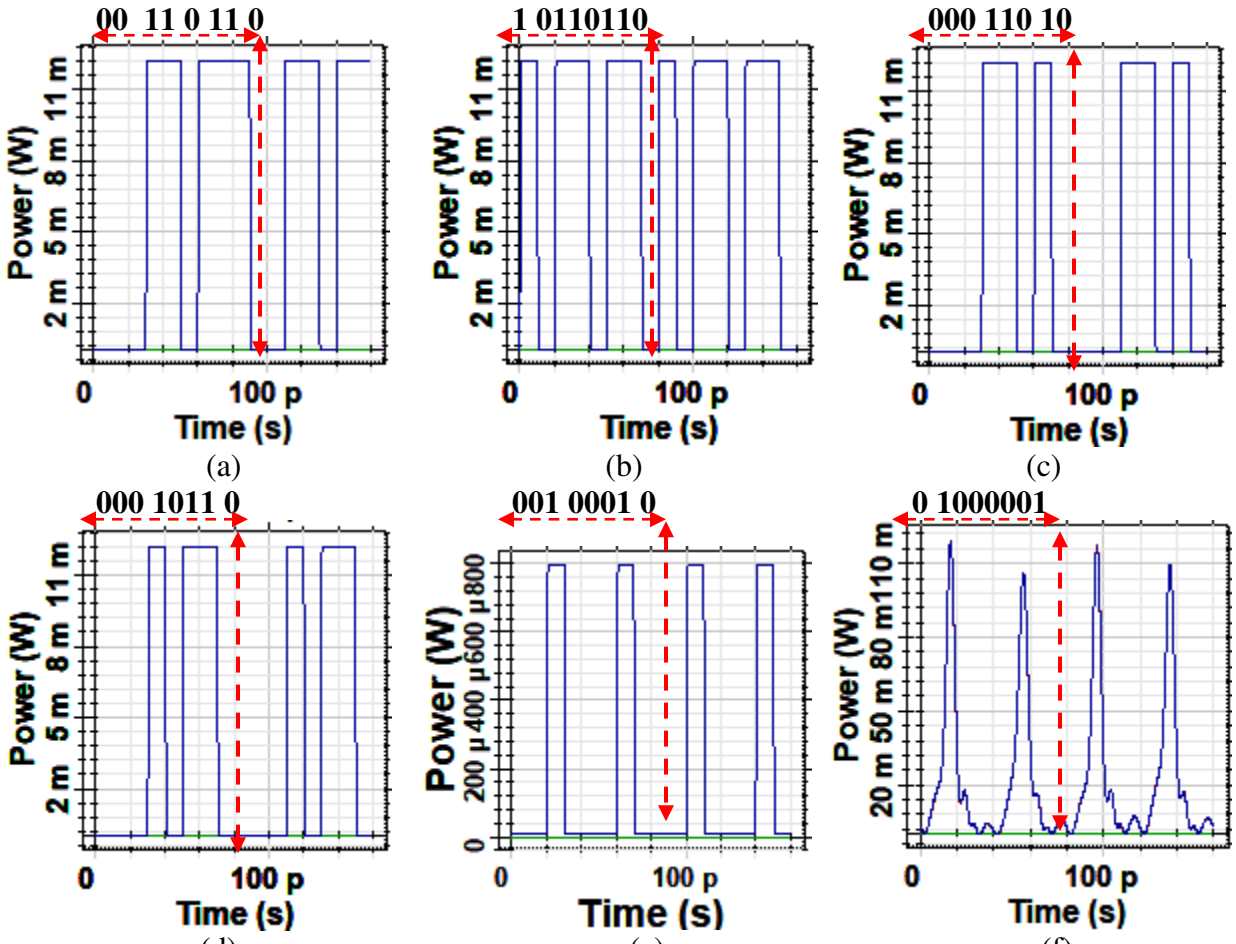




(e) (f)

Figure 4 Optical carrier spectrum after (a) Four OCDMA users (b) adding private key (c) FWM in FISO (d) filter NOR wavelength in upper arm (e) filter AND wavelength in lower arm (f) FISO decoder with reference input laser signals

Representation of four users multiplexed frequencies spectrum which is 2-D coded using DIM codes is depicted in Figure 4 (a) and carrier spectrum addition of private key is shown in Figure 4 (b). As discussed in section (4), four user data at the rate of 100 Gbps/user fed to FISO unit by adding P_k and FWM takes places inside FISO unit due to MZI-DCF configuration as shown in Figure 4 (c). Iteration is set to select the different frequencies at filter 1 and filter 2 in order to check the behaviour of filters towards data.



(a) (b) (c)

(d) (e) (f)

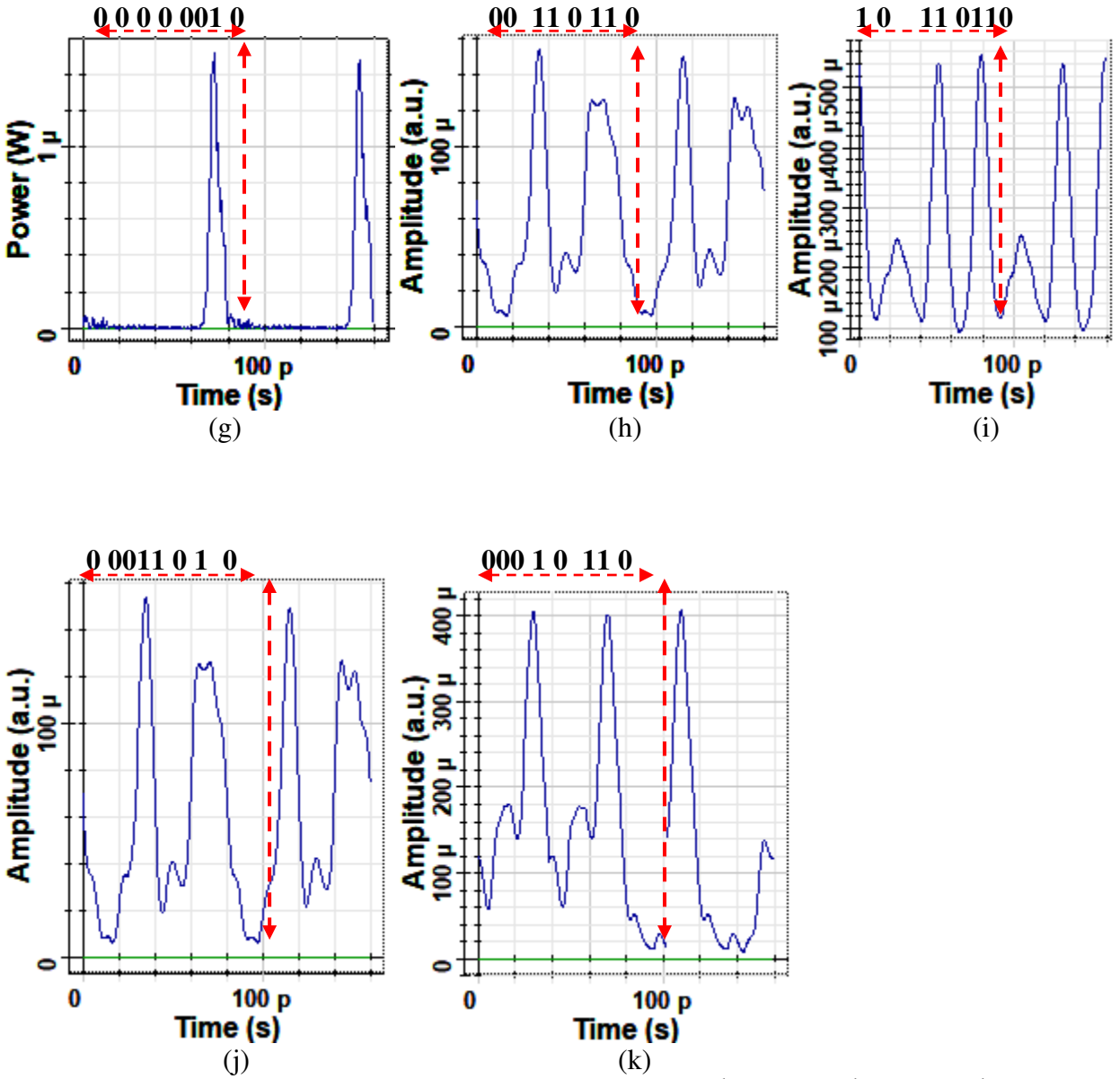


Figure 5 Optical bits with respect to time for (a) 1st user (b) 2nd user (c) 3rd user (d) 4th user (e) P_k (f) NOR gate (g) AND gate (h) received 1st user (i) received 2nd user (j) received 3rd user (k) received 4th user

It is evident that frequency 193.3 THz performs the operation of NOR gate as shown in Figure 4 (d) and 194.13 THz does the logic operation of AND gate as depicted in Figure 4 (e). Optical data bits are checked with optical time domain visualizers at diverse points in system to check the logic operations. Input sequence of 1st, 2nd, 3rd, 4th users are shown in Figure 5 (a)(b)(c)(d) and further P_k is added and it is shown in Figure 5 (e). Bit sequence at NOR gate and AND gate after respective filters is represented in Figure (f) (g). Figure 5 (h)(i)(j)(k) shows received bit patterns in proposed system after decoding of FISO data at legitimate users such as 1st, 2nd, 3rd, 4th users.

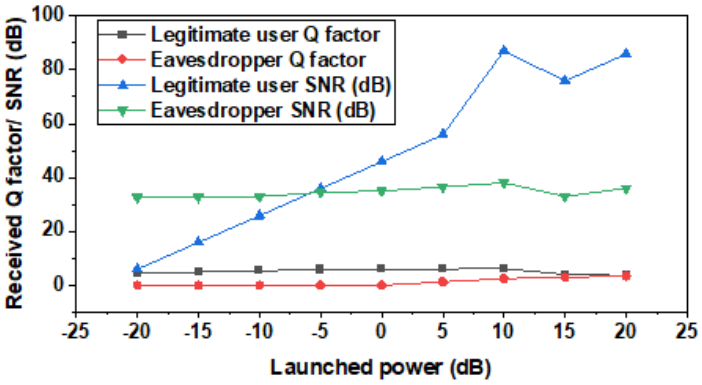


Figure 6 Sensitivity of received Q factor and SNR towards launched power

Launched power has significant effects on the Quality, and SNR of received signal at both legitimate and at eavesdropper. Performance of FISO-2D DIM system is affected by launched/ input power but due to presence of FWM in the FISO, there is nonlinear response in both legitimate and eavesdropper as illustrated in the Figure 6. Power optimization is selected by observing received Q at varied power level -20 dBm to 20 dBm. Figure 6 shows the highest Q at 10 dBm launched power for both legitimate user and eavesdropper but eavesdropper has low Q factor. SNR increase with the increase in launched power and there are approximately same values at eavesdropper for all power levels but highest SNR observed at 10 dB launched power. Investigated parameters are analyzed in terms of security and high performance also which shows that security and performance of proposed system is enhanced.

System security with and without FISO unit is investigated in terms of correct codeword detection rate (CCDR) at legitimate user and eavesdropper, at diverse launched powers. FISO system enhances security of the system but also introduce insertion losses as well as nonlinear effects in the system. Therefore it is evident from Figure 7 that performance in terms of CCDR at legitimate user without FISO is enhanced followed by legitimate user with FISO. However different in both systems, is security of the communication and results revealed that eavesdropper in absence of all optical FISO system has greater success rates to receive correct code word but in other case where FISO is deployed, CCDR of eavesdropper is negligible as compared to aforementioned system.

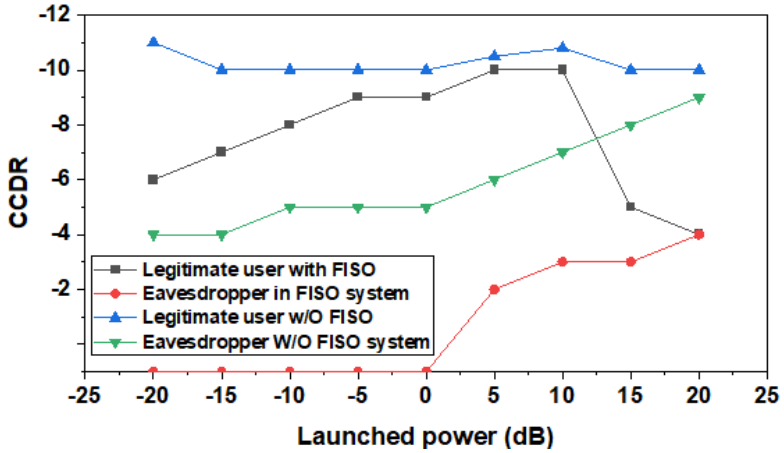


Figure 7 CCDR responses on different launched powers for with and without FISO unit

AND gate and NOR gate are obtained from the FISO system and we have taken NOR due to high output power but in terms of security, better optical logic gate is selected after analysis. Analysis is performed on different launched power levels and system with AND gate provides lesser security to legitimate user in proposed system. AND gate encoding is common these days and become easy to decode for eavesdropper in the system. However, our FISO system is more secure than conventional system but here, NOR gate is best performing because of the logic operation of NOR. Table 3 (a) and (b) shows the logic operation of NOR and AND gate respectively on input data bits and P_k.

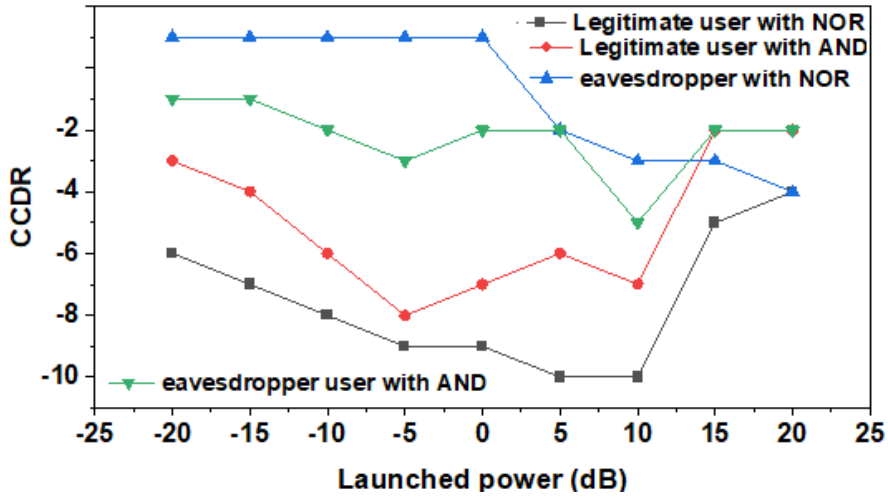


Figure 8 Performance of 2-D DIM codes with and without AND gate/NOR gate

Table 3 (a) NOR logic for all inputs and P_k

Input 1st	Input 2nd	Input 3rd	Input 4th	P_k	NOR output
0	1	0	0	0	0
0	0	0	0	0	1
1	1	0	0	1	0
1	1	1	1	0	0
0	0	1	0	0	0
1	1	0	1	0	0
1	1	1	1	1	0
0	0	0	0	0	1

Table 3 (b) NOR logic gate for inputs and P_k

Input 1st	Input 2nd	Input 3rd	Input 4th	P_k	NOR output
0	1	0	0	0	0
0	0	0	0	0	0
1	1	0	0	1	0
1	1	1	1	0	0
0	0	1	0	0	0
1	1	0	1	0	0
1	1	1	1	1	1
0	0	0	0	0	0

1-D DIM codes are ZCC codes with improved performance because of lesser multiple access interference as investigated in [21] as compared to enhanced double weight codes (EDW), multi-diagonal codes (MD), Walsh Hadamard (WH) codes, Double diagonal weight codes (DDW) etc. In this work, 2D-DIM codes are investigated with FISO and comparison is carried out in Figure 9 with 1D-DIM codes with FISO in terms of maximum eye amplitude (MEA). MEA is least in case of eavesdropper with 2D-DIM codes and performance in MEA of 1D-DIM is highest because 2D-DIM code has some time skews limitations but eavesdropping MEA is highest in 1D-DIM, therefore it is lesser secure than 2D-DIM. Figure 10 shows the eye diagram at 50 km SMF distance for legitimate user and eavesdropper. Eye opening at legitimate user is wide because of encryption key and FISO system. Eavesdropper attack the proposed system but get

insignificant information and therefore error are more and eye opening is very less. Encrypted legitimate user data reaches to the optical network unit with improved quality, better CCDR and high SNR. Therefore proposed 2D-DIM FISO system is suggested for the very high speed OCDMA systems in services where data protection is utmost concern.

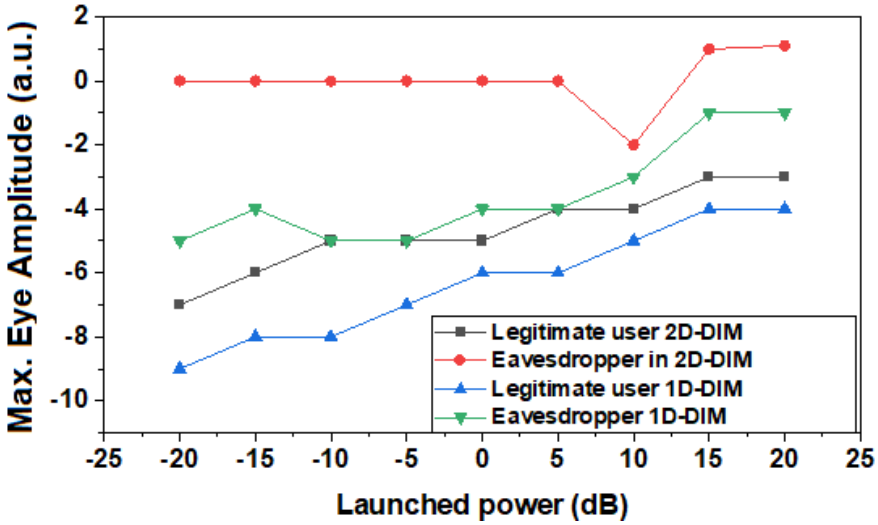
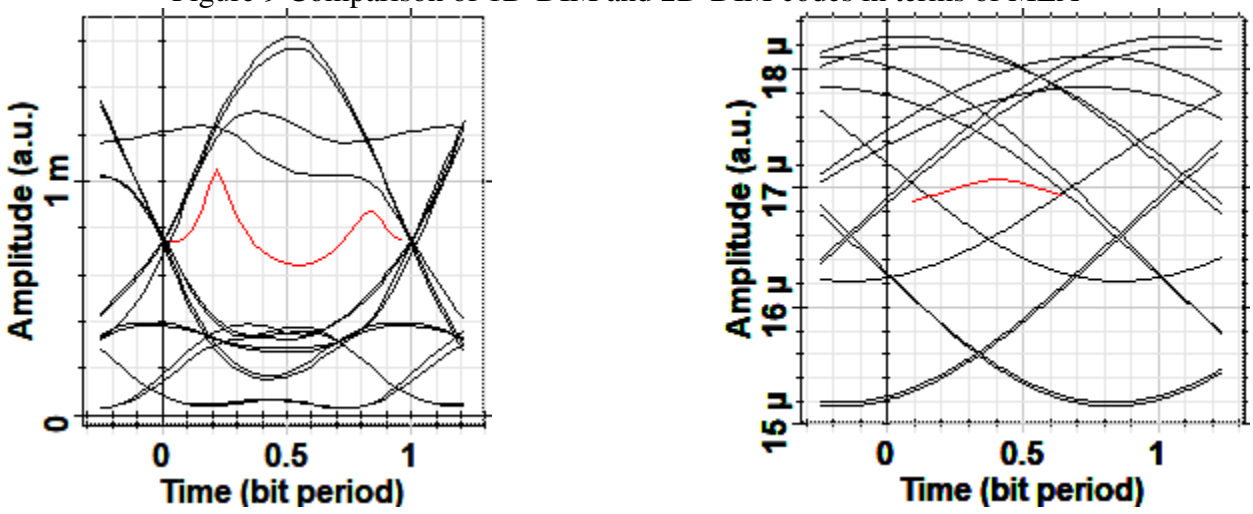


Figure 9 Comparison of 1D-DIM and 2D-DIM codes in terms of MEA



(a) (b)

Figure 10 Eye diagram of proposed system for (a) legitimate user (b) eavesdropper at 50 km

6. Conclusion

Confidentiality enhanced ultra high speed OCDMA system is proposed in this work with all optical FISO gating and private key encryption using 2D codes. Security enhancement is performed such that eavesdropper has to breach the physical layer based optical code, FISO operation and also the encryption key in order to get correct code word of legitimate user. Large number of users in the A-OCDMA provides far better security than S-OCDMA. Optisystem simulation tool is considered for the realization of proposed work and system is analyzed at different launched powers in terms of CCDR, MEA, Received Q factor, SNR for legitimate user and eavesdropper when different scenarios are used such as system with/without FISO, with 1D-DIM/2D-DIM codes, using 4×1 AND gate/NOR gate. For the successful legitimate user data detection, eavesdropper need matched decoder/encryption at the same time. Results reveal that

proposed system with FISO at 10 dBm launched power provide CCDR of 10^{-10} at legitimate user, CCDR of 10^{-3} at eavesdropper, without FISO show CCDR of 10^{-10} at legitimate user but system is very much prone to eavesdropper and provide CCDR 10^{-7}. FISO system improve the security of proposed system and analysis is also performed for 1D-DIM and 2D-DIM, it is seen that eavesdropping is easier in 1D-DIM system. NOR gate due to its logic operation and high output power from FISO offers improved security than AND gate. Therefore, proposed system is good candidate for secure transmission and in near future, effect of uni-phase, bi-phase and quad-phase modulation can be studied.

Declaration: No funding was received for the research work presented in this manuscript.

References

[1] W. Sahraoui, H. Aoudia, A. Amphawan, B. Smail, Y. Belkhier, R. Shaw," Enhanced Performances of SAC-OCDMA System Operating with Different Codes", International Conference on Electrical and Electronics Engineering (ICEEE), pp. 1-11, 2021.
[2] A. L. Filatov, "Experimental Study of Multiband Acousto-Optic Filtering by Decoding of Spectrally Encoded Signals in Noncoherent OCDMA Systems", Technical Physics Letters, vol. 47, pp. 16-18, 2021.
[3] W. Sahraoui, A. Amphawan, S. Berraha, R. Matem, "A novel 2D polarization-spatial encoding approach for OCDMA system based on multi-core fiber", Optik, vol. 228, no. 166164 pp. 1-19, 2021.
[4] R.Alléaume et. al., "Using quantum key distribution for cryptographic purposes: A survey", Theoretical Computer Science, vol. 560, part I, pp. 62-81, 2014.
[5] B. Dai, Z. Gao, X. Wang, N. Kataoka and N. Wada, "Demonstration of Differential Detection on Attacking Code-Shift-Keying OCDMA System," IET Electronics Letters, Vol. 46, No. 25, pp. 1680–1682, 2010.
[6] K. Chen, "Multiple-Code Technique for Multi-Rate Transmissions in Optical Packet Switching Networks Based on OCDMA Labels", photonics, vol. 6, no. 2, 2019.
[7] U. Kaur, H. Singh, "Security enhancement in OCDMA system using multicode keying and data randomisers", 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 2016.
[8] Z. Wang, Y.-K. Huang, Y. Deng, J. Chang, and P. R. Prucnal, "Optical encryption with OCDMA code swapping using all-optical XOR logic gate," IEEE Photon. Technol. Lett., vol. 21, no. 7, pp. 411-413, Apr. 1, 2009.
[9] X. Liu et. al., "Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding", Optics Express, vol. 23, no. 15, 2015.
[10] T. Sharma, R. Maddila, "Optical Code Construction Based on Enhanced Quantum Logic Gate (EQLG) Technique for Spectral Amplitude Coding Optical CDMA Systems", Wireless Personal Communications, vol. 113, pp. 2587–2609, 2020.
[11]] T. Sharma, R. Maddila, S. Aljunid, "Simulative Investigation of Spectral Amplitude Coding Based OCDMA System Using Quantum Logic Gate Code with NAND and Direct Detection Techniques", Current Optics and Photonics, vol. 3, no. 6, pp. 531-540, 2019.
[12] J. Lin, G. Yang, C. Chang, and W. Kwong, "Study of Multicode-Keying Incoherent Optical CDMA Without the Conventional Symbol-Synchronous Assumption", Journal of Lightwave Technology, vol. 34, no. 16, pp. 3663-3674, 2016.

[13] C. Yen, J. Huang and W. Zhang, “Hiding Stealth Optical CDMA Signals in Public BPSK Channels for Optical Wireless Communication”, applied sciences, vol. 8, pp. 1-18, 2018.
[14] V. Jyoti, R. S. Kaler, “Novel virtual user scheme to increase data confidentiality against eavesdropping in OCDMA network”, Chinese Optics Letters, vol. 9, no. 12, 2011.
[15] Agarwal, Vipul, M. Agarwal, P. Pareek, V. Chaurasia, and SK Pandey. “Ultrafast Optical Message Encryption–Decryption System Using Semiconductor Optical Amplifier Based XOR Logic Gate.” Optical and Quantum Electronics 51, no. 7, 2019.
[16] Z. Wang et al., “Optical encryption with OCDMA code swapping using all-optical xor logic gate,” IEEE Photonics Technol. Lett., vol. 21, no. 7, pp. 411–413, 2019. https://doi.org/10.1109/LPT.2008.2012131 IPTLEL 1041-1135
[17] T. Sharma, R. K. Maddila, and S. A. Aljunid, “Simulative Investigation of Spectral Amplitude Coding Based OCDMA System Using Quantum Logic Gate Code with NAND and Direct Detection Techniques”, vol. 3, no. 6, pp. 531-540, 2019.
[18] N. Ahmed, S.A. Aljunid, A. Fadil, “Performance enhancement of OCDMA system using NAND detection with modified double weight (MDW) code for optical access network”, Optik, vol. 124, pp. 1402–1407, 2013.
[19] J. Wang, Q. Sun, J. Sun, “Simultaneous demonstration on FWM-based all-optical 40 Gpbs multicasting CSRZ-DPSK logic XOR gate and CSRZ-DPSK to RZ-DPSK format conversion”, In: Proceeding of Asia Conference on Communications and Photonics, Shanghai, pp. 1–6, 2009.
[20] A. Bogis, P. Velanas, D. Syvridis, “Numerical investigation of a 160-Gbps reconfigurable photonic logic gate based on cross-phase modulation in fibers”, IEEE Photon. Technol. Lett., vol. 19, no. 6, pp. 402–404, 2007.
[21] S. Kaur, S. Singh, “Review on developments in all-optical spectral amplitude coding techniques”, Optical Engineering, vol. 57, no. 11, 2018.
[22] N. A. Mohammed, M. M. Ragab, M. H. Aly, “Four-wave mixing based wavelength conversion using different types of fibers”, Int. J. Eng. Sci. Technol., vol. 4, no. 1, pp. 324–330, 2012.
[23] A. J. Agrawal, M. Kumar, R. Saxena, “Comparison of different techniques of dispersion compensation”, Int. J. Electron. Comput. Sci. Eng., vol. 2, no. 3, pp. 912–918, 2013.
[24] M. Ajmani, P. Singh, P. Kaur, “Hybrid Dispersion Compensating Modules: A Better Solution for Mitigating Four-Wave Mixing Effects”, Wireless Pers. Commun., vol. 107, pp. 959–971, 2019. https://doi.org/10.1007/s11277-019-06311-3
[25] T. H. Shake, “Confidentiality performance of spectral-phase-encoded optical CDMA," J. Lightw. Technol., vol. 23, no. 4, pp. 1652-1663, 2005.

Figures

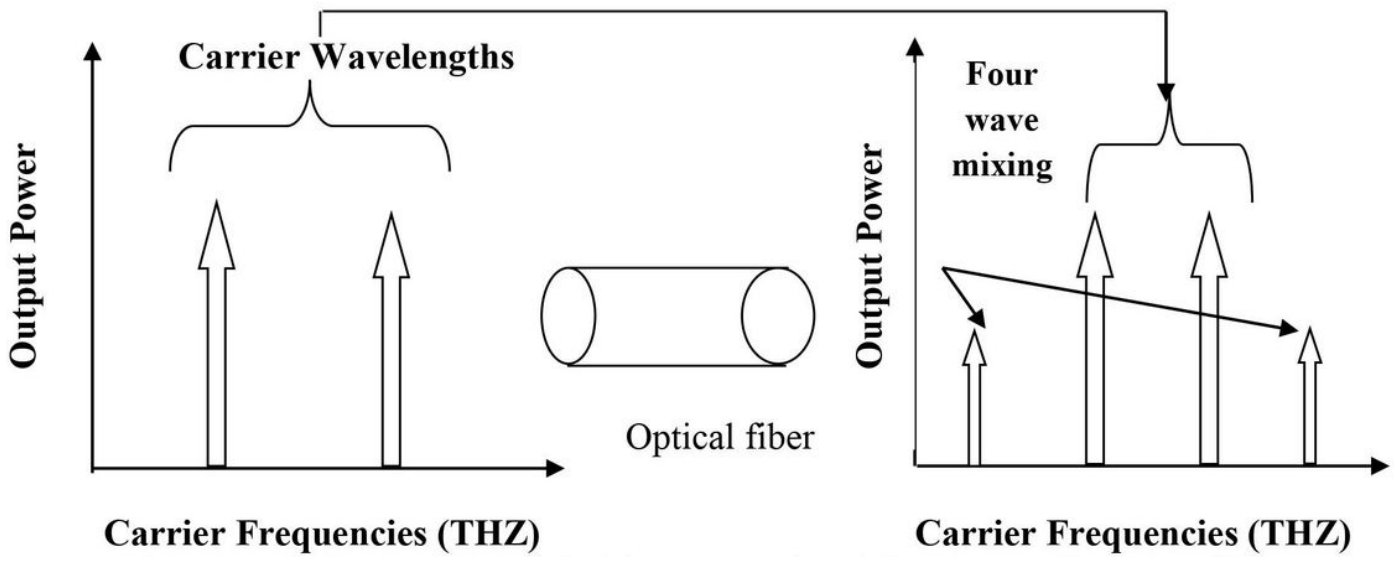


Figure 1

Carrier spectrums of (a) input signal and (b) after nonlinear medium

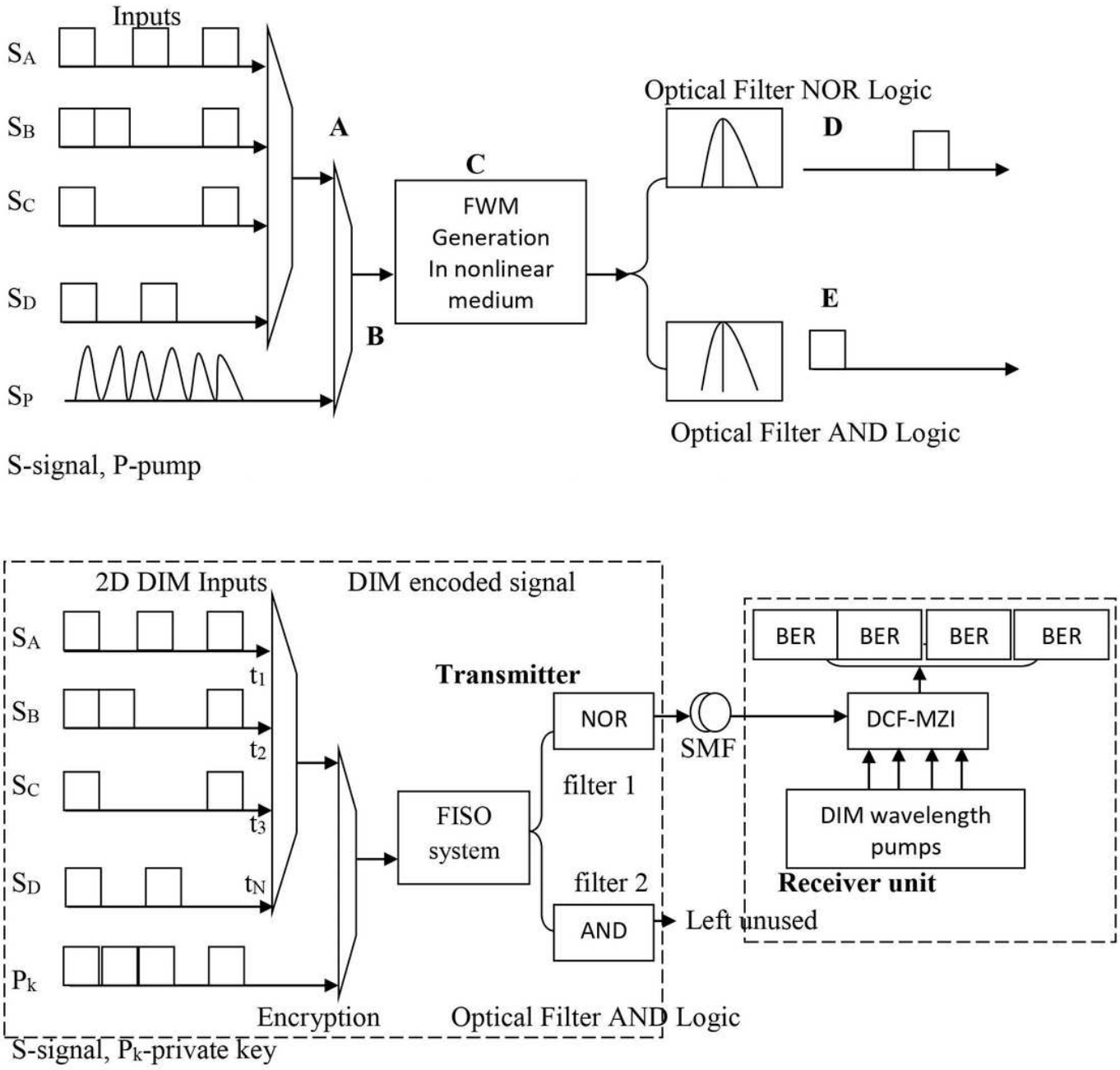


Figure 2

Proposed FISO AND/NOR gate using DCF-MZI

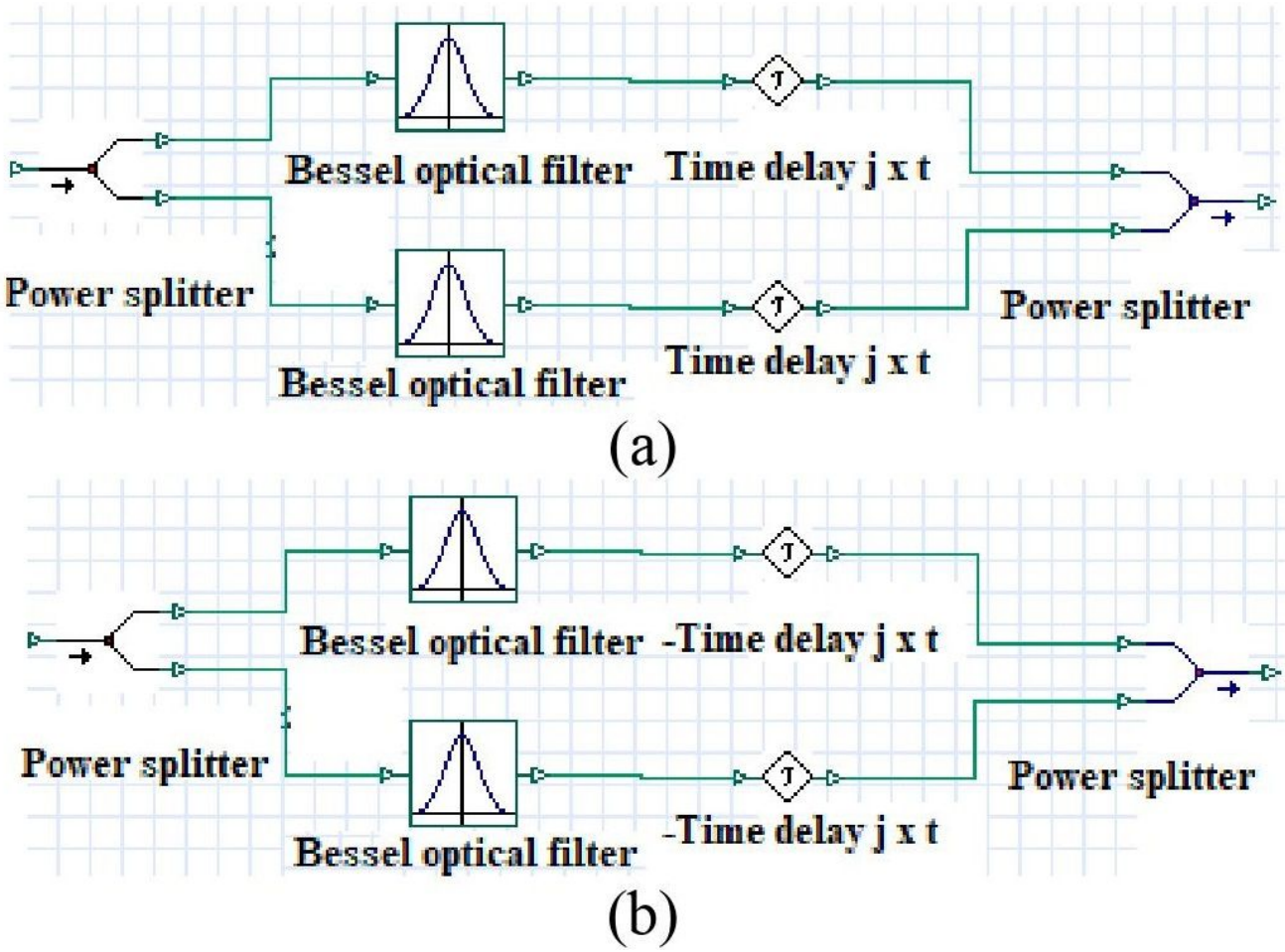


Figure 3

General Time spreading encoder at (a) transmitter (b) receiver

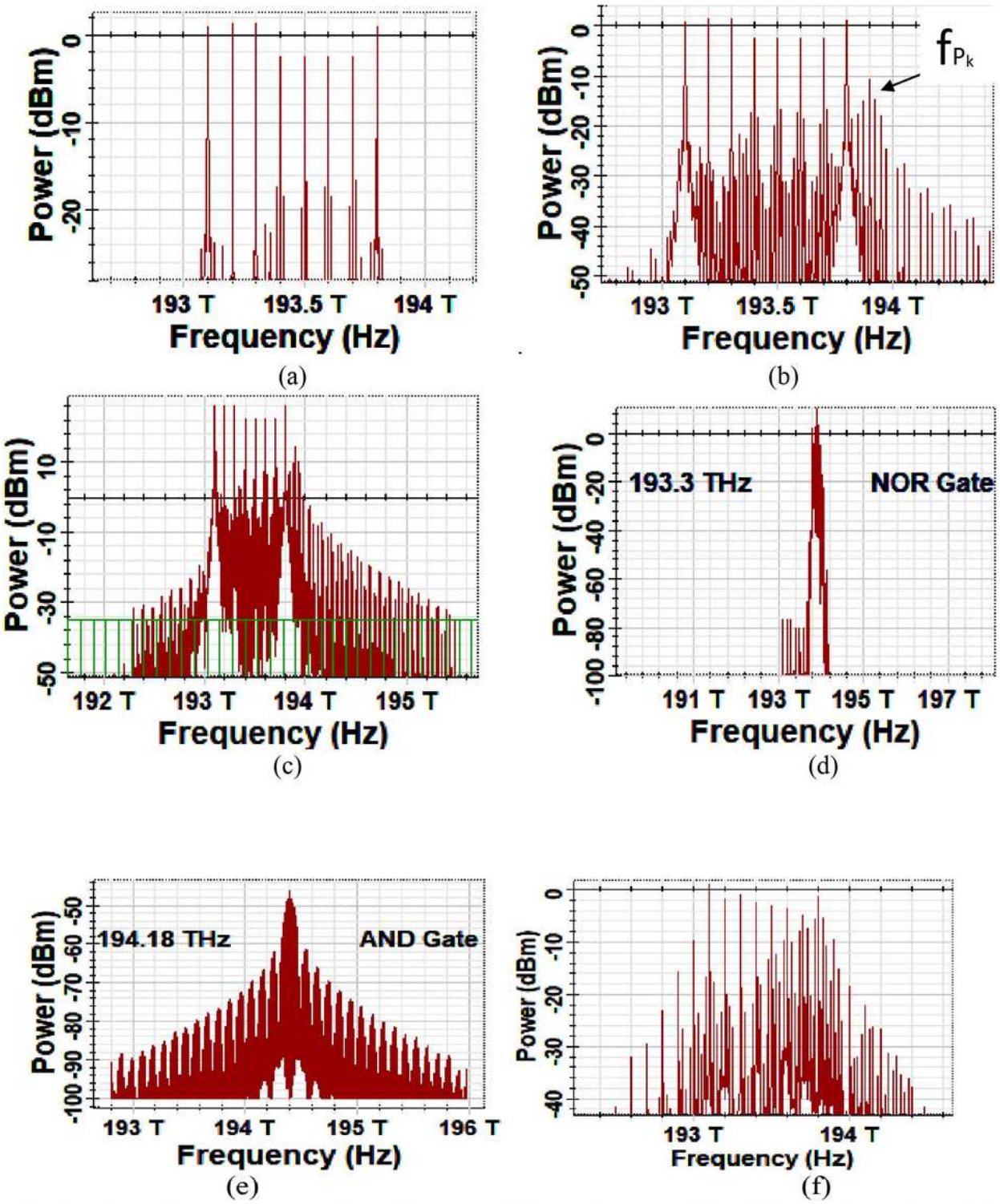


Figure 4

Optical carrier spectrum after (a) Four OCDMA users (b) adding private key (c) FWM in FISO (d) filter NOR wavelength in upper arm (e) filter AND wavelength in lower arm (f) FISO decoder with reference input laser signals

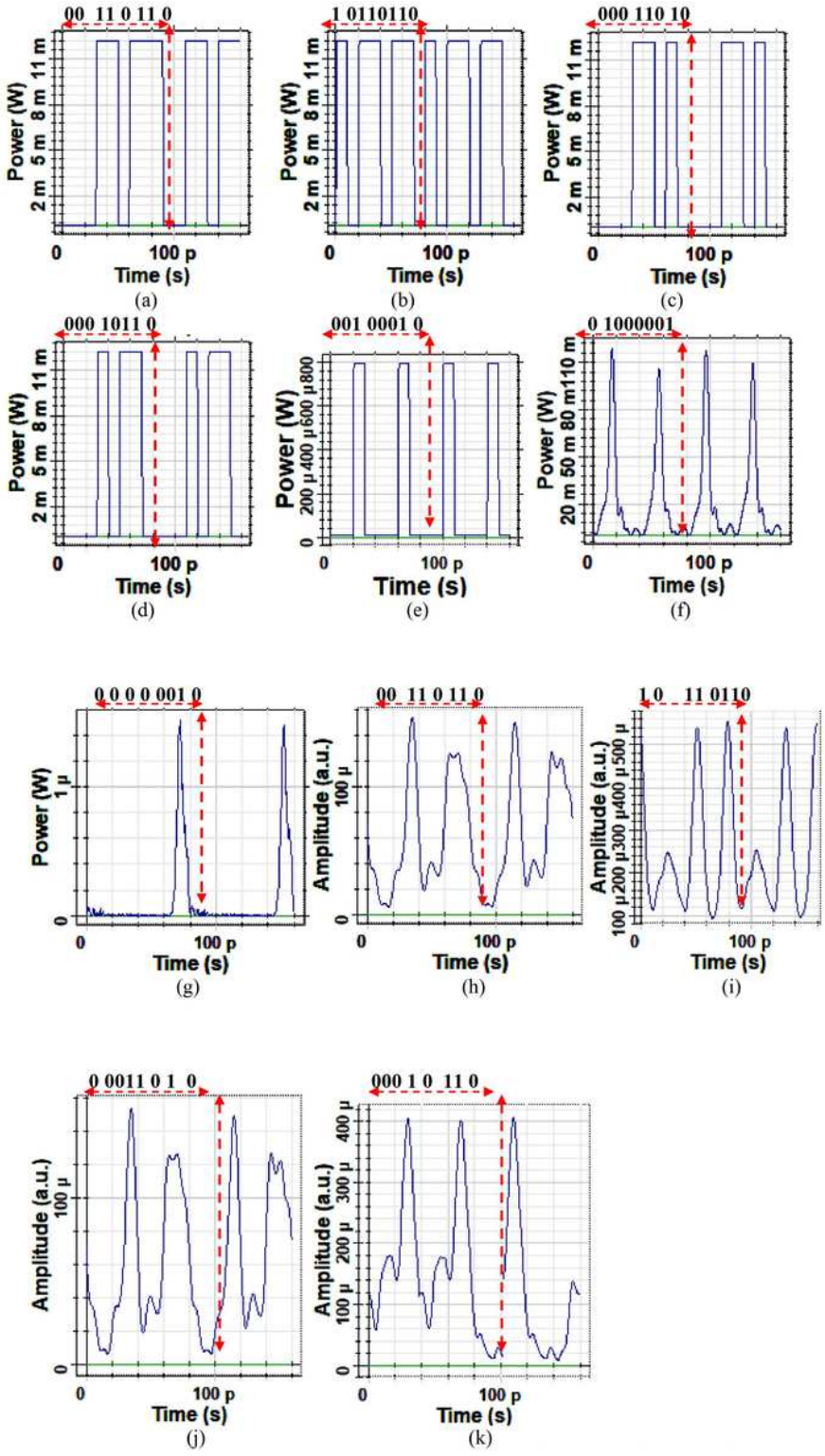


Figure 5

Optical bits with respect to time for (a) 1st user (b) 2nd user (c) 3rd user (d) 4th user (e) Pk (f) NOR gate (g) AND gate (h) received 1st user (i) received 2nd user (j) received 3rd user (k) received 4th user

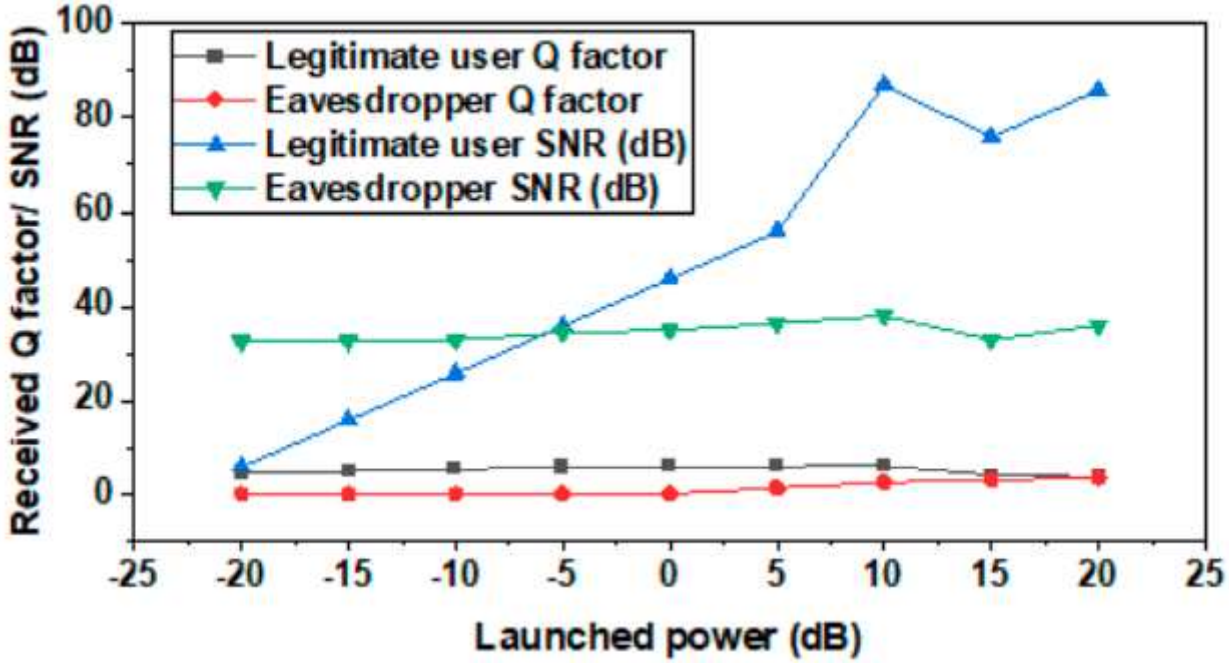


Figure 6

Sensitivity of received Q factor and SNR towards launched power

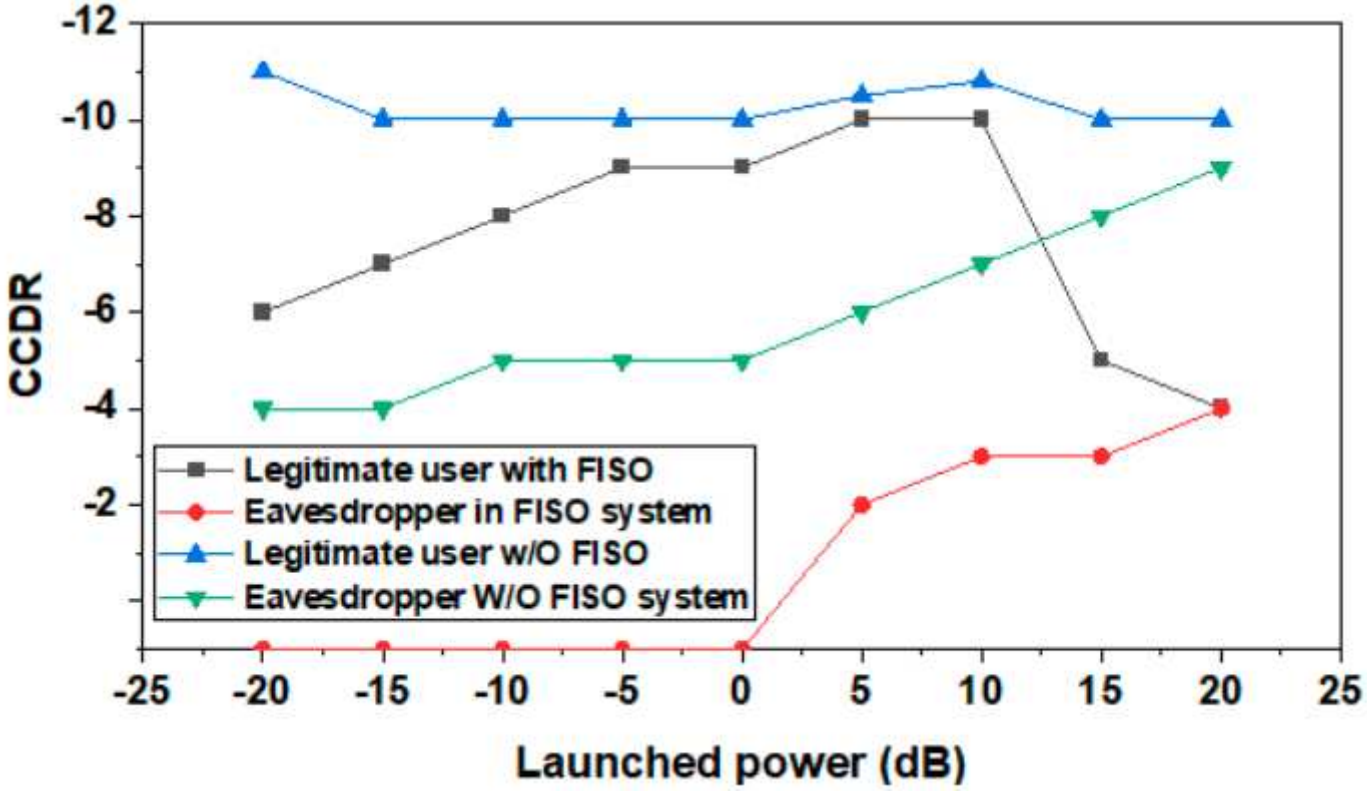


Figure 7

CCDR responses on different launched powers for with and without FISO unit

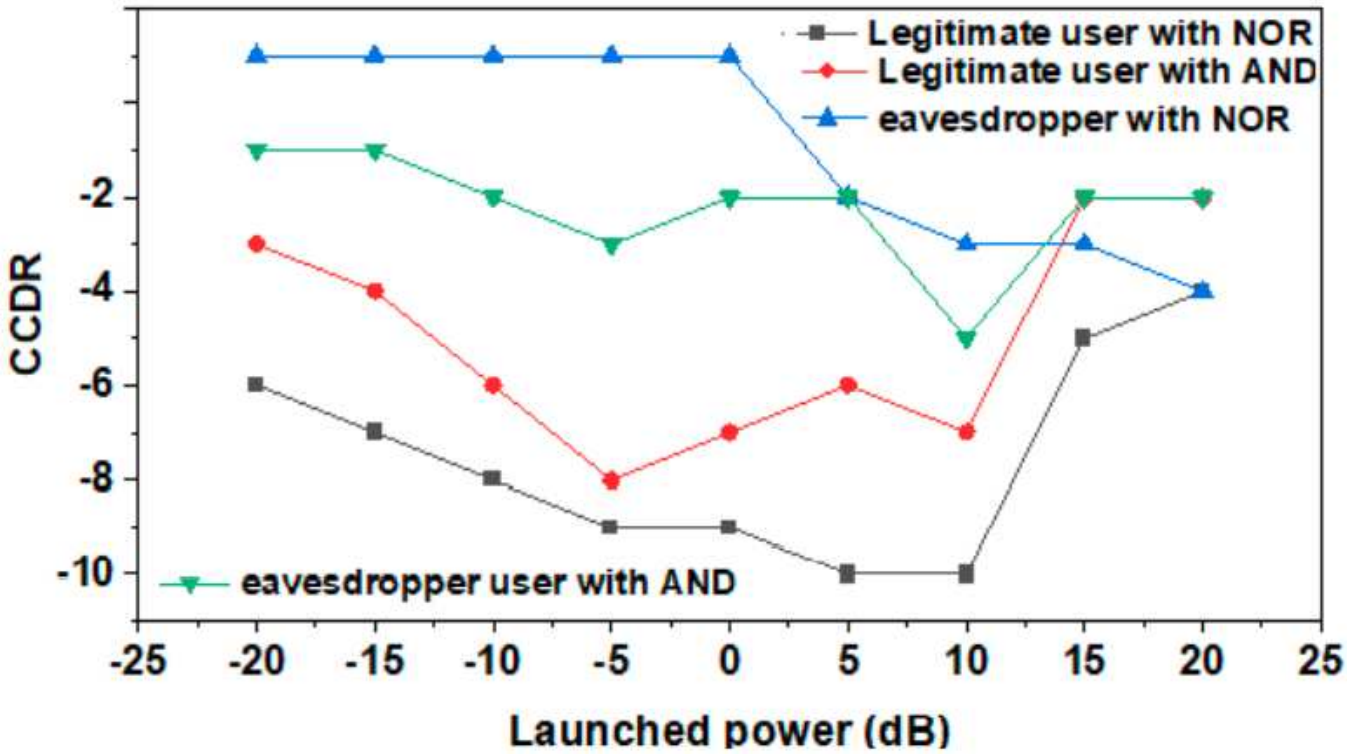


Figure 8

Performance of 2-D DIM codes with and without AND gate/NOR gate

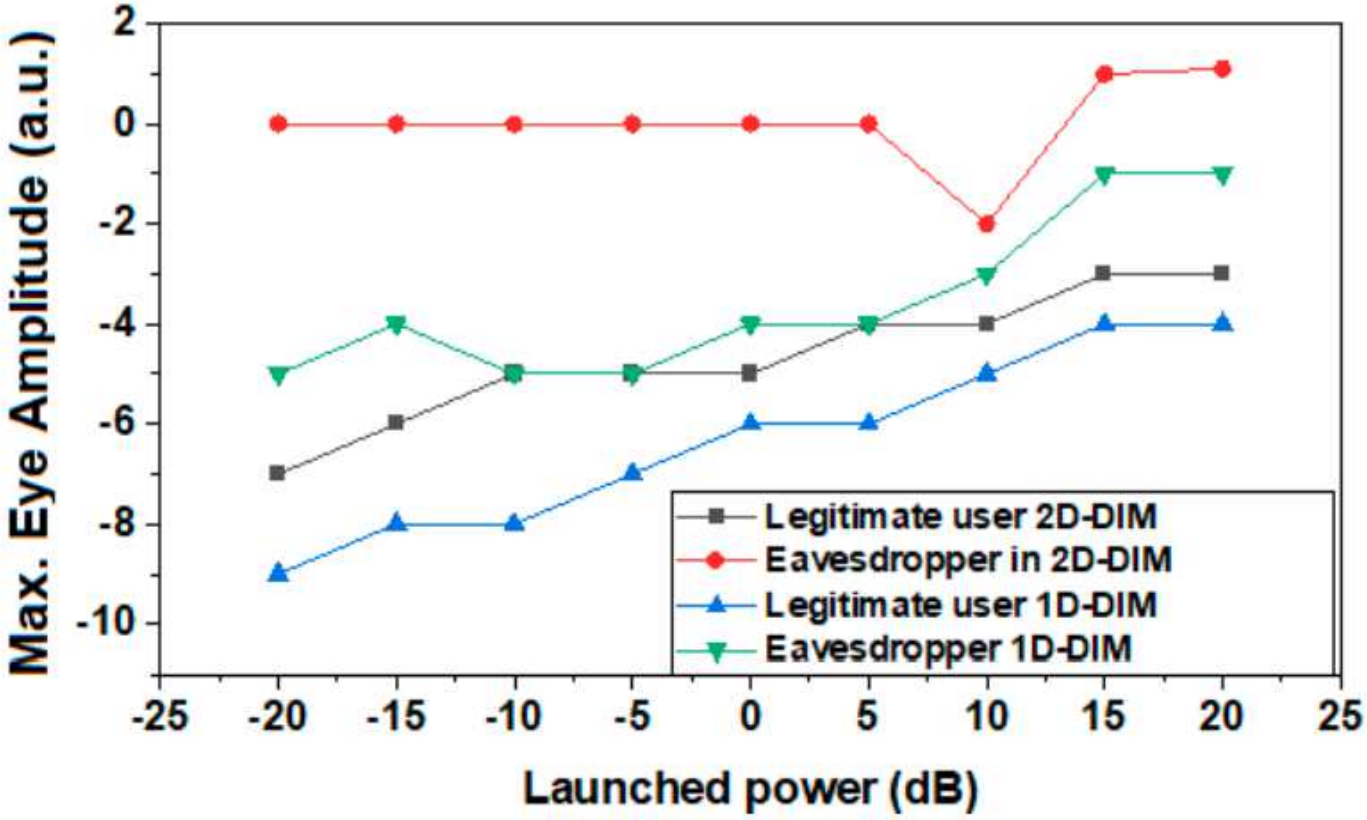


Figure 9

Comparison of 1D-DIM and 2D-DIM codes in terms of MEA

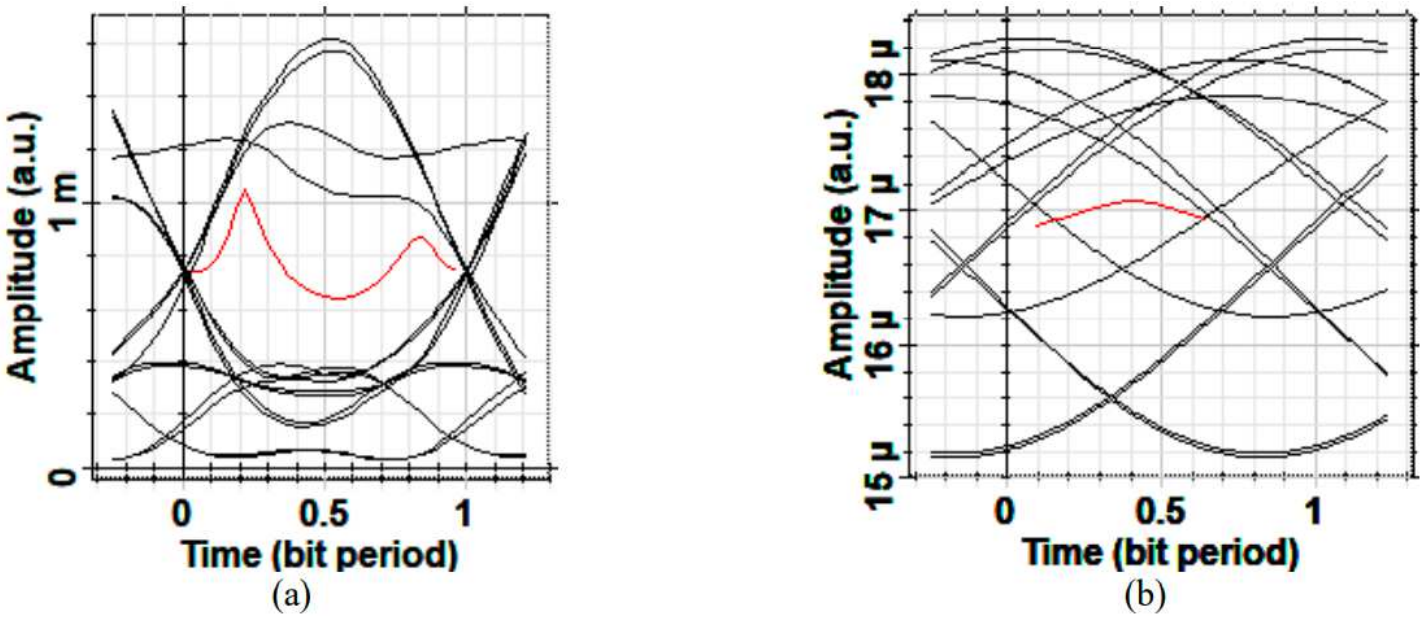


Figure 10

Eye diagram of proposed system for (a) legitimate user (b) eavesdropper at 50 km