

# Performance and security analysis of novel ZCCRW codes in lower earth orbit based MDM-OWC incorporating hybrid modulations

Rupinder Kaur<sup>1</sup>, Rajinder Singh Kaler<sup>2</sup>

Explosive data rate requirements in the satellite communication for surveillance, military services, and broadcasting have put peer pressure on the optical wireless communication (OWC) systems. Secure data transmission against eavesdropper and performance enhancement at authentic user is major concern these days. In this work, performance and security analysis of spectral amplitude codes (SAC) in mode division multiplexed (MDM) OWC have been carried out and a novel zero cross correlation resultant weight (ZCCRW) code at 100 Gbps capacity has been presented. Random diagonal (RD), Enhanced double weight (EDW), Diagonal double weight (DDW) codes have been compared through simulations and also mathematical expressions are derived under the effects of eavesdropper. Hybrid modulations have been compared to check optimal modulation with combination of Laguerre-Gaussian (LG), and HermiteGaussian (HG) modes. Results have revealed that ZCCRW code with MD-DQPSK using LG modes provide best performance and least susceptibility to eavesdropper.

**Keywords:** OWC, IsOWC, MDM, ZCCRW, OCDMA, ZCC, LG, HG

## 1 Introduction

In the present era, increasing demand for high-speed transmission systems is perceived, and to combat this demand, it has become mandatory to implement innovative techniques in data communication [1]. Optical wireless communication (OWC) links are gaining significant stature as compared to traditional radio frequency (RF) based techniques owing to its numerous benefits such as extensive bandwidth, high speed, more security, no license need, and absence of electromagnetic interference (EMI) [2]. Nowadays, for OWC, optical code division multiple access (OCDMA) based efficient coding techniques are preferred among all the existing access techniques such as WDM and TDM, as it is a promising substitute for network access [3, 4]. This technique permits flexibility and scalability for increased traffic within the aforesaid transmission link. Unfortunately, the developed/reported codes have few limitations as listed: i) Larger Code length [5] ii) Complexity in code design [6] iii) Variable cross correlation [7] iv) MAI [5] v) Less security against eavesdropper and jammer [2] vi) High Cost [8, 9]. OCDMA codes with zero cross correlation (ZCC) to eliminate MAI and variable cross correlation are reported in [5], and in [10] code design without mapping for reducing code complexity is presented. For improving the prevailing network security by protecting sensitive information from spurious users, different studies have been conducted such as using all optical logic operation [11], multi code keying [12], data scrambling [13], hybrid codes [14], code switching [15],

code shift keying and temporal phase coding [16], 2-dimensional/3-dimensional codes [17], and 2-D modulation format [15]. To achieve all these features, different codes have been developed with certain trade-offs between code length, cross correlation and security [15, 18]. However, cost of the OCDMA is also prominent concern and different past studies tried to lower it with the design of systems having lesser weights/fixed weights ( $W = 2$  in double diagonal weight codes) [19], using Light Emitting Diodes (LEDs) with Fiber Bragg Grating (FBG) filtering/spectrum slicing mode division multiplexing (MDM) serving double users with random diagonal codes (RD) reported in [14]. But aforementioned techniques either support lesser data rates/more MAI or provide limited performance/distance/less signal to noise ratio because of lower weights. The most pivotal factor among OWC based systems is to securely transmit the data without allowing any eavesdropper to access the confidential information [18, 20]. In IsOWC, security breaching is observed at different stages like within a satellite, in the communication channel [21] or at ground station [22]. Among all, maximum unauthorised access occurs at communication channel which needs to be resolved with the optimal design of transmitter [23]. MDM technology has emerged as a remarkable multi user supporting technique due to its cost effective operation [14, 24–26] owing to single laser usage with linearly polarised modes consisting of intensity profiles for transverse field shapes [27, 28]. On contrary, WDM has high cost due to  $n$  laser sources for  $n$  users and TDM has problem of time skews [29]. MDM in OWC investigated using integrated modulations

<sup>1,2</sup> Optical Fiber Communication Research Laboratory (OFCR Lab), ECE Department, Thapar Institute of Engineering and Technology University, Patiala 147004, Punjab, India, rupinderdhillon9@gmail.com, <sup>2</sup> drrajindersinghkaler@gmail.com

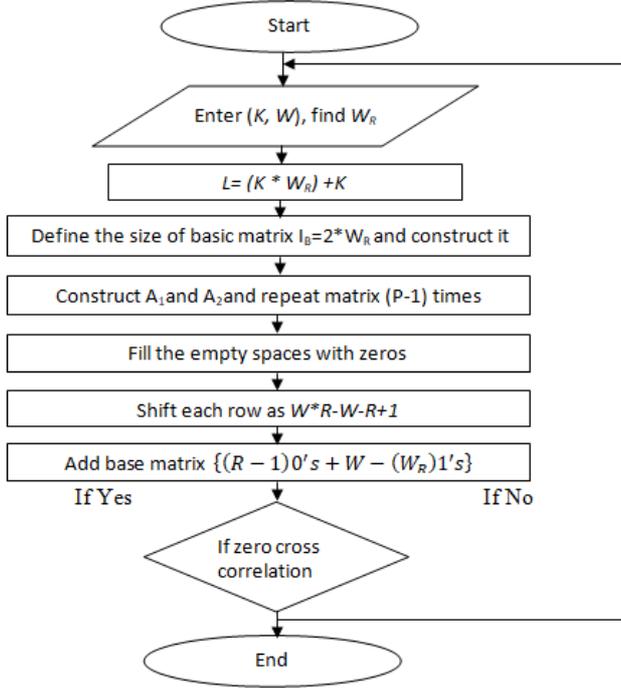


Fig. 1. Flow diagram of ZCCRW code

for capacity enhancement, employing Manchester, DPSK and DQPSK [2], and with polarization division multiplexing, hybrid modulations [14, 30] *etc.* Advantage of hybrid modulations is to introduce additional phase shifts or provide combined effects of multiple modulations to get better performance. Therefore, current generation OWC systems requires low cost, security enhanced, performance improved multi-user systems with optimal OCDMA code having medium code length, ZCC, freedom to select code weight, and mapping free code construction.

In this research article, a lower cost security and performance enhanced dense OWC system has been presented with ZCCRW code and MDM at 100 Gbps capacity. Security of OWC system has been analyzed in the presence of eavesdropper with mathematical study and simulation software. Performance of hybrid modulations with LG and HG in proposed system has been compared. To the best of authors knowledge, no work like our proposed work has been reported in the area of security of OWC systems.

## 2 Security enhancement principle and OCDMA code design

MAI due to cross correlation and multiple users in the OCDMA systems is a severe performance degrading issue which limits the data rate and overall distance. ZCC codes, without mapping, simple design, are solution to aforementioned issue. Therefore, a new code ZCCRW has been proposed in this research article and given as:

### 2.1 Resultant weight ZCC code (ZCCRW)

A one-dimensional newly constructed ZCCRW code has been described with three parameters ( $K$ ,  $W$ ,  $\lambda_c$ ) where  $K$  represents the number of supported users,  $W$  denotes weight and  $\lambda_c$  indicates the value of cross correlation present in the code. A simple relationship has been created among the number of users ( $K$ ) and resulting weight ( $W_R$ ) that is  $W_R = W - 1$  for calculating the length of the proposed code.

$$L = (K * W_R) + K. \quad (1)$$

The size of simple matrix is denoted with  $\mathbf{I}_B$  and defined as

$$\mathbf{I}_B = 2 * W_R \text{ (Balanced)} \quad (2)$$

As number of users can be chosen up to any extent, therefore a basic matrix  $K * L$  is constructed for flexible number of users.

$$\mathbf{I} = \begin{bmatrix} R_1 \\ R_2 \end{bmatrix} = \begin{bmatrix} (W/2)1_s & (W-2)0_s \\ \{(W+2)/3\}0_s & \{(W+1)/2\}1_s \end{bmatrix} \quad (3)$$

where  $R_1$  and  $R_2$  represent row number 1 and row number 2 of the  $\mathbf{I}_B$  and code weight  $W = 1, 2, \dots, W_R$ . The entire set comprises of  $K * L$  sized matrix  $A$ . Further, various steps have been followed for constructing the matrix  $A$  where initially intermediate matrix  $A_1$  has been designed. Then, repetition of  $\mathbf{I}_B$  matrix occurs  $P - 1$  times as given:

$$A_1 = \begin{bmatrix} R_1 & \dots & \dots & \dots & R_2 \\ R_2 & R_1 & \dots & \dots & \dots \\ \dots & R_2 & R_1 & \dots & \dots \\ \dots & \dots & R_2 & R_1 & \dots \\ \dots & \dots & \dots & R_2 & R_1 \end{bmatrix}$$

As presented in  $A_2$  matrix, the process has been reiterated  $K * L$  times.

$$A_2 = \begin{bmatrix} R_1 & \dots & \dots & \dots & R_2 \\ R_2 & R_1 & \dots & \dots & \dots \\ \dots & R_2 & R_1 & \dots & \dots \\ \dots & \dots & R_2 & R_1 & \dots \\ \dots & \dots & \dots & R_2 & R_1 \end{bmatrix}_{K \times L}$$

In every row of matrix  $A_2$ , zeroes are filled in empty spaces and matrix  $A_3$  is formed, as shown below.

$$A_3 = \begin{bmatrix} R_1 & 0 & 0 & 0 & R_2 \\ R_2 & R_1 & 0 & 0 & 0 \\ 0 & R_2 & R_1 & 0 & 0 \\ 0 & 0 & R_2 & R_1 & 0 \\ 0 & 0 & 0 & R_2 & R_1 \end{bmatrix}_{K \times L}$$

Further, a shifting operation is applied on rows and rows have been shifted to the right side according to the particular weight present in each row.

$$[\text{Weight} * \text{Row number} - \text{Weight} - \text{Row number} + 1]. \quad (4)$$

Addition of matrix has been done to the resulted shifted row as

$$\{(R-1)0_s + W - (W_R)1's\}_{K * K}. \quad (5)$$

After addition, matrix  $A$  will be obtained consisting of  $= (K * W_R) + K$ . The flow chart of novel ZCCRW code has been given in Fig. 1.

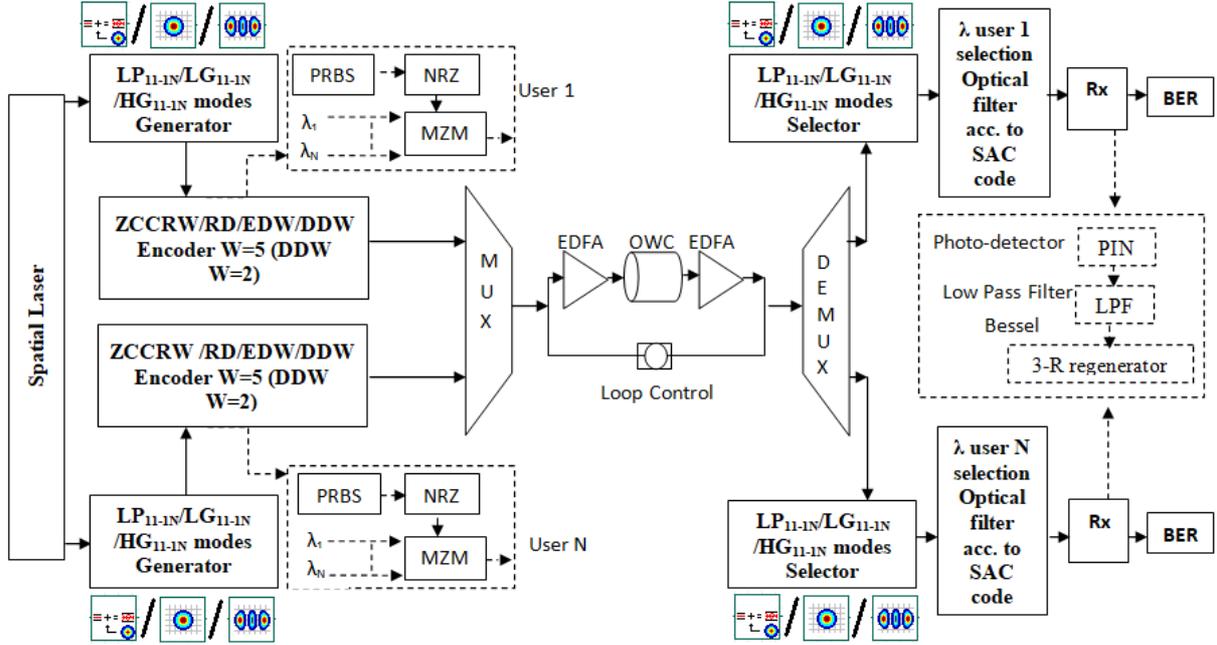


Fig. 2. Proposed MDM-IsOWC system using different SAC codes

On the basis of characteristics of the proposed ZCCRW code, the numerical equation of SNR has been discussed in [31] as

$$\text{SNR} = \left( \frac{RWP_{ST}}{N} \right)^2 / \left( \frac{\epsilon BRP_{ST}W^2}{N} + \frac{4K_bT_nB}{R_L} \right). \quad (6)$$

The bit error rate (BER) or the probability of error ( $P_e$ ) of the pulse sent through wireless channel can be evaluated as [32]

$$P_e - \text{BER} = \frac{1}{2} \text{erfc} \left( \frac{Q}{\sqrt{2}} \right) \quad (7)$$

where erfc denotes the error complimentary function.

Eye height has been calculated as [33]

$$E_H = (\mu_1 - 3\sigma_1) - (\mu_0 - 3\sigma_0), \quad (8)$$

$\sigma_0$  is the standard value of sample 0,  $\sigma_1$  is the standard value of sample 1,  $\mu_0$  is the average value of sample 0, and  $\mu_1$  is the average value of sample 1.

## 2.2 Principle

The basic principle of optical MDM technique is enhancing the security by transmitting distinct polarised signals simultaneously using the same wavelength over different mode multiplexed divisions. The proposed system can be an attractive out way for cost efficient and zero cross correlation approach.

A simple and feasible approach incorporating MDM technique is described against eavesdropping by an expression for estimation of Eavesdroppers Probability of Correct Bit Interception. Taking the effect of code length

into consideration that enhances security, the total combinations of actual code wavelengths that need to be chosen by the eavesdropper for correct codeword detection are calculated in [33] as

$$T_C = n_{C_W}. \quad (9)$$

The presence of cross correlation fixes the position of wavelength and further decreases the total combinations.

$$T_{\lambda_c} = n_{C_{\lambda_c}}. \quad (10)$$

But in case of ZCCRW, absence of cross correlation results in  $\lambda_c = 0$ . Thus, the resultant cases are given as

$$T_{C_r} = n_{C_W} - n_{C_{\lambda_c}}. \quad (11)$$

The total pulses are 50% for the total present users considered as

$$P(p) = \left( \frac{1}{2} \right)^K. \quad (12)$$

But the probability of correct codeword detection is half

$$P(E) = \frac{1}{2} \frac{1}{n_{C_W} - n_{C_{\lambda_c}}} \left( \frac{1}{2} \right)^K. \quad (13)$$

The proposed ZCCRW code has been compared with reported codes-DDW, EDW, and RD in terms of security features. It has been perceived that ZCCRW code has less probability of estimation as compared to existing codes because larger code lengths result in requirement of large number of combinations for the intruder to detect the information. It is analyzed that due to  $\lambda_c = 0$ , the denominator value in (13) becomes larger, hence making the correct detection difficult for the intruder, whereas due to presence of cross correlation in other codes, the

**Table 1.** Simulation parameters of the proposed work

Parameter	Values
Data rate	10 Gbps/User
Total capacity	100 Gbps
Users	10
Input Power	0 dBm
MDM modes	LG11-15/HG <sub>11-15</sub>
Linecoder	CSRZ-DQPSK/MDRZ-DQPSK, DRZ-DQPSK
SAC codes compared	ZCCRW, DDW, RD, EDW
Weight of the codes	W=5 (ZCCRW, RD, EDW), W=2 (DDW)
Cross-correlation	$\lambda_c = 0$ (ZCCRW), $\lambda_c = 1$ (RD, EDW, DDW)
Distance of OWC	500 km–3000 km
OWC transmission module (each loop)	EDFA(gain 20 dB, NF 4 dB)+250 km OWC+ EDFA(gain 20 dB, NF 4 dB)
Number of Loops	2, 4, 6, 8, 10, 12

denominator value is lesser which means total combination required for getting correct data at eavesdropper also reduces, hence resulting in increasing chances of eavesdropping.

Further, due to presence of different polarized modes of laser, correct codeword detection becomes more tedious for the intruder as investigation of LP modes require more combinations. An expression for different polarized modes is derived for security enhancement using (13):

$$P(E) = \frac{1}{2^r} \frac{1}{n_{C_W} - n_{C_{\lambda_c}}} \left(\frac{1}{2}\right)^K. \quad (14)$$

where  $r$  is the number of polarized modes.

Integration of the polarized modes in the system further increases the combinations in the denominator of (13) and it is noteworthy that combination of ZCCRW and polarized modes increase the security against eavesdropper.

### 3 System setup

Figure 2 illustrates the synchronous coherent OCDMA model based on newly constructed ZCCRW code, where other existing SAC codes are also incorporated such as RD, DDW, and EDW for performance and security comparison with proposed code. The analysed system comprises three main sections: transmitter, channel, receiver section and to configure the simulation, OptiSystem<sup>TM</sup> V-13 is used. The transmitter section consists of spatial laser operating at 193.1 THz for generating signal output with a repetition rate equal to the bit rate of the setup with the frequency spacing of 50 GHz between the adjacent channels. For all compared SAC codes, Laser outputs are selected (half of the total users) based on the code construction matrix. Here MDM is prominent technology which has been used to save the overall cost (approx. 1/2) by taking half code matrix of the total users. In order to serve 10 users, mode HG/LG 11 to 15 have been used to carry first 5 users and same code of

5 users have been transmitted over mode HG/LG 21 to 25. In case of ZCCRW, total laser outputs required are 25 ( $L = (K * W_R) + K$ ), for DDW 6 ( $L = k + 1$ ), for EDW 20 ( $L = K * (W - 1)$ ) and for RD are 12 ( $L = K + 2W - 3$ ). Selected frequencies (wavelengths) from the laser have been passed through respective mode and then modulated with legitimate informative data at 10 Gbps consisting of pseudo random bit sequence generator (PRBS), Compressed spectrum return to zero-differential quadrature phase shift keying (CSRZ-DQPSK)/Modified duo-binary return to zero-DQPSK (MDRZ-DQPSK)/Duobinary return to zero-DQPSK (DRZ-DQPSK) hybrid modulations and mach-zehndar modulator (MZM). Further, data has been multiplexed and sent via the OWC transmission module in which single loop comprises of pre EDFA amplifier with 20 dB gain and 4 dB noise figures, OWC channel of 250 km, and post EDFA amplifier with 20 dB gain and 4 dB noise figure. Table 1 shows the simulation parameters of the proposed work for all investigated codes in this work. A De-MUX after the OWC transmission medium has been placed to differentiate the frequencies according to the respective user followed by HG/LG mode selector. Photo detector PIN for the optical to electrical conversion is incorporated followed by a Bessel optical filter to remove the undesired content. Eventually, the filtered data has been fed to 3-R regenerator and the eye diagram analyzer, which compares the input and output signal to generate BER value and to calculate Q-factor.

### 4 Results and discussions

Satellites are increasing in the space with the passage of each day and security of the information is essential in case of military satellites, surveillance satellites and broadcasting satellites. Therefore, in this research article, we have emphasised on the communication security of the satellites using MDM, and newly constructed ZCCRW SAC code. For the validation of the proposed work, a comparison between different SAC codes has been done

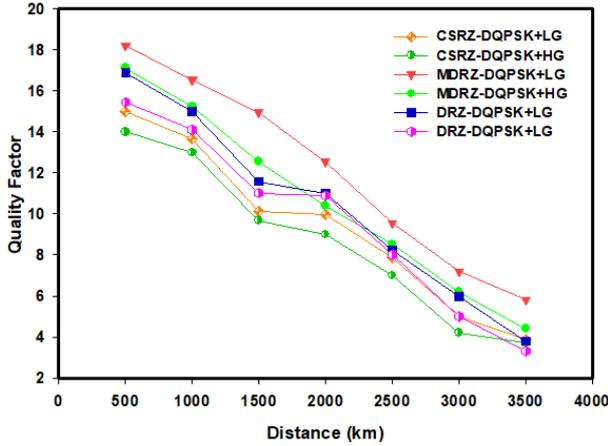


Fig. 3. Q factors of different hybrid modulations with LG and HG modes at different OWC link lengths

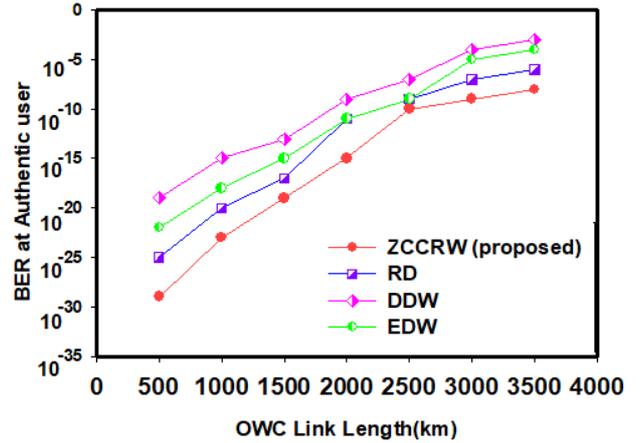


Fig. 4. BER at Authentic user versus OWC link length in LEO orbit for different SAC codes

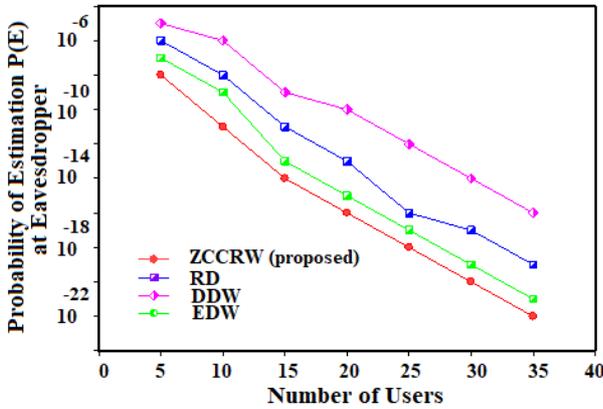


Fig. 5. Probability of Estimation P(E) at eavesdropper versus number of users

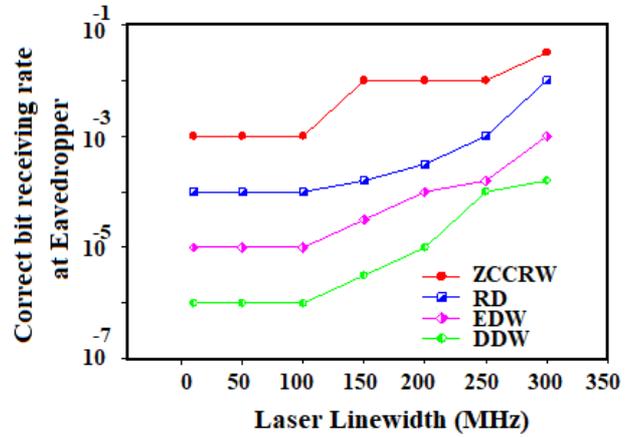


Fig. 6. Correct bit receiving rate at eavesdropper versus laser linewidth

with the same input parameters such as modes, input power, distance, and line coding *etc.*

Polarization modes play important role in the performance of the optical communication systems and finally in this work, different modes such as Laguerre-Gaussian, and Hermite Gaussian have been investigated in the proposed system with the incorporation of different hybrid modulations such as CSRZ-DQPSK, MDRZ-DQPSK, DRZ-DQPSK to select optimal mode with hybrid modulation in terms of Q factor at authentic user with respect to OWC distance as shown in Fig. 3. Advantage of hybrid modulation is to reduce interference *ie* intrachannel and interchannel and provide better performance than single (without hybridization) modulation due to additional phase shift (in this work). Results revealed that MDRZ-DQPSK with the LG modes comes out to be optimal because of better spectral efficiency and improved tolerance against interferences due to hybrid phase shifting. CSRZ-DQPSK provides least results with HG modes because of lesser spectrum efficiency.

Further, effect of distance from 500 km to 3000 km in LEO orbit has been checked on the BER at authentic user for ZCCRW (proposed), DDW, RD, and EDW SAC codes

as shown in Fig. 4. Increase in OWC link distance cause increase in the BER at authentic user because of the environment factors such as scattering, attenuation and physical factors like pointing errors of satellite antennas, noises (thermal, shot noise) in PIN. BER at authentic user is minimum in case of proposed code *ie* ZCCRW (covered 3000 km at  $10^{-9}$  BER) due to least MAI, and ZCC. It is evident that proposed code has wavelengths/frequencies at distant locations inside code matrix row unlike DDW, EDW codes due to which MAI is least. On the other side, DDW code provides most errors reception of data at authentic user (covered only 2000 km) due to DDW has  $W=2$  and cross correlation 1. It is reported that less  $W$  provide less SNR which in turn give more errors at received data. RD and EDW code have cross correlation 1 also, however performance of RD (covered 2500 km) is slightly better to EDW (covered 2500 km) because wavelengths are at distant locations in code matrix row which leads to lesser MAI.

Eavesdropper is unauthorized user which intrudes the communication and tries to get away the sensitive information. For the decoding/reception of information/data, eavesdropper performs calculations (per-

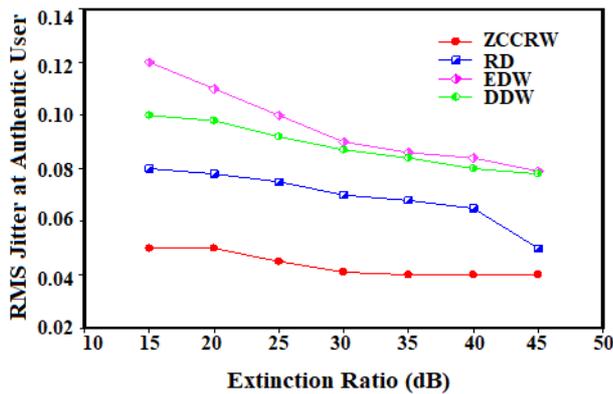


Fig. 7. RMS jitter at authentic user versus extinction ratio

mutation/combinations) in order to get the specific user code wavelengths. Estimation of getting correct codeword at eavesdropper decreases with the increase in the code length of users and user itself because more time required for eavesdropper to find specific combination of user. In this proposed work, as shown in (10), we have derived an expression for  $P(E)$  at eavesdropper where a new parameter  $r$  has been introduced and this represents number of HG/LG modes. This factor, further increase the combinations for eavesdropper and leads to better security of the OWC system.

Figure 5 represent the  $P(E)$  at eavesdropper with respect to the number of users. Results revealed that presence of more users reduce the  $P(E)$  at eavesdropper and it is also important to note that ZCC code such as ZCCRW has greater code length which results into the requirement of more combinations at the eavesdropper and provide enhanced security. Further, SAC codes having lesser code lengths and cross correlation 1 are more prone to eavesdropping. Therefore, EDW and RD codes can be estimated by eavesdropper with ease as compared to ZCCRW.  $W$  present in EDW are consecutive and thus susceptible to  $P(E)$  easier than RD and in case of DDW,  $P(E)$  is easiest because of  $W = 2$  and minimum code length.

Figure 6 shows correct bit receiving rate versus laser linewidth based on proposed system for different MDM-SAC codes. Laser linewidth is defined as the spectrum consisting of sidebands or spectrum divergence along the desired signal. As the linewidth increases, the spectrum divergence multiplies with carrier signal and further affecting the correct bit rate with errors at eavesdropper. Therefore, on comparing the output results, analysis are made that optimal results are found at 300 MHz linewidth where minimum correct bit rate is achieved at eavesdropper that is system security is highest. Out of the four codes, ZCCRW code shows least detection at eavesdropper that is  $10^{-2}$  followed by RD, EDW and DDW codes.

A comparative analysis of proposed ZCCRW code has been done with the other existing SAC-OCDMA codes

in Fig. 7. For checking the least jitter value, extinction ratio values are varied from 15 to 45 from MZM, and it is depicted that in case of all investigated codes, RMS jitter value decrease as the ER value increase however jitter value is highest for DDW code due to presence of low weight ( $W=2$ ) and unity cross correlation. Absence of cross correlation, managed ones in the code matrix rows makes ZCCRW optimal.

## 5 Conclusion

This article presented a LEO based MDM-OWC system with mode generators to enhance the security and performance. The results revealed least susceptibility to eavesdropper by employing newly developed ZCCRW code along with mathematical study and simulation. A comparison is done with the existing codes in terms of BER at authentic user,  $P(E)$  at eavesdropper, RMS jitter, and correct receiving bit rate when laser line width, users, distance and encoded SNR is varied. Performance of HG, LP mode with the combination of hybrid modulations is also explored and it is observed that MDRZ-DQPSK with LG modes provide optimal performance. Therefore, in order to realise security enhanced, better performance IsOWC system, proposed ZCCRW codes are suggested using MDRZ-DQPSK and LG modes. The security feature *ie* probability of estimation by an eavesdropper is minimum in the suggested code in comparison with the other existing SAC codes.

## REFERENCES

- [1] S. Panda, G. Palai, "Design and Performance Analysis of Data Encrypted Two Dimensional Coding Techniques for Wavelength Hopping Time Spreading Optical CDMA", *Optik*, pp. 163864, 2019.
- [2] H. K. Gill, G. K. Walia, N. S. Grewal, "Performance Analysis of Mode Division Multiplexing IS-OWC System using Manchester, DPSK and DQPSK Modulation Techniques", *Optik*, vol. 177, pp. 93–101, 2019.
- [3] P. L. Bertarini, A. L. Sanches and B. H. V. Borges, "Optimal Code Set Selection and Security Issues in Spectral Phase-Encoded Time Spreading (SPECTS) OCDMA Systems", *Journal of lightwave technology*, vol. 30, no. 12, pp. 1882–1890, 2012.
- [4] V. J. Hernandez, W. Cong, J. Hu, C. Yang, N. K. Fontaine, R. P. Scott, Z. Ding, B. H. Kolner, J. P. Heritage and S. B. Yoo, "A 320 Gb/s Capacity (32 user  $\times$  10 Gb/s) SPECTS O-CDMA Network Testbed with Enhanced Spectral Efficiency through Forward Error Correction", *Journal of Lightwave Technology*, vol. 25, no. 1, pp. 79–86, 2007.
- [5] S. Mostafa, A. E. N. A. Mohamed, F. E. A. El-Samie, and A. N. Z. Rashed, "Performance Evaluation of SAC-OCDMA System in Free Space Optics and Optical Fiber System Based on Different Types of Codes", *Wireless Personal Communications*, vol. 96, no. 2, pp. 2843–2861, 2017.
- [6] H. M. Al-Khafaji, S. A. Aljunid and H. A. Fadhil, "Improved BER Based on Intensity Noise Alleviation using Developed Detection Technique for Incoherent SAC-OCDMA Systems", *Journal of Modern Optics*, vol. 59, no. 10, pp. 878–886, 2012.

- [7] U. Bhanja, and S. Panda, "Comparison of Novel Coding Techniques for a Fixed Wavelength Hopping SAC-OCDMA", *Photonic Network Communications*, vol. 33, no. 2, pp. 179–193, 2017.
- [8] N. Ahmed, S. A. Aljunid, A. Fadil, R. B. Ahmad, and M. A. Rashid, "Performance Enhancement of OCDMA System using NAND Detection with Modified Double Weight (MDW) Code for Optical Access Network", *Optik*, vol. 124, no. 13, pp. 1402–1407, 2013.
- [9] H. Y. Ahmed, and K. S. Nisar, "Diagonal Eigen Value Unity (DEU) Code for Spectral Amplitude Coding-Optical Code Division Multiple Access", *Optical Fiber Technology*, vol. 19, no. 4, pp. 335–347, 2013.
- [10] K. S. Nisar, A. Djebbari, and C. Kandouci, "Development and Performance Analysis Zero Cross Correlation Code using a Type of Pascals Triangle Matrix for Spectral Amplitude Coding Optical Code Division Multiple Access Networks", *Optik*, vol. 159, pp. 14–20, 2018.
- [11] S. C. Xavier, B. E. Carolin, A. P. Kabilan, and W. Johnson, "Compact Photonic Crystal Integrated Circuit for All-Optical Logic Operation", *IET Optoelectronics*, vol. 10, no. 4, pp. 142–147, 2016.
- [12] C. C Yang, "Performance Analysis of Multi-Code Keying Scheme for Spectral-Amplitude-Coding Optical CDMA Network", *Int. J. Inf. Commun. Sci.*, vol. 2, no. 6, pp. 100–103, 2017.
- [13] K. W. A. K. Yongjun, A. Sengupta, D. W. Lee, A. Davydov, S. Han, G. Morozov, and S. Pawar, U. S. Patent Application No. 16/127, pp. 829, 2019.
- [14] H. Sarangal, A. Singh, J. Malhotra, and S. Chaudhary, "A Cost Effective 100 Gbps hybrid MDMOCDMAFSO Transmission System under Atmospheric Turbulences", *Optical and Quantum Electronics*, vol. 49, no. 5, pp. 184, 2017.
- [15] S. Singh, R. Kaur, A. Singh, and R. S. Kaler, "Novel Security Enhancement Technique Against Eavesdropper for OCDMA System using 2-D Modulation Format with Code Switching Scheme", *Optical Fiber Technology*, vol. 22, pp. 84–89, 2015.
- [16] S. Mostafa, A. E. N. A. Mohamed, F. E. A. El-Samie, and A. N. Z. Rashed, "Cyclic Shift Code for SAC-OCDMA Using Fiber Bragg-Grating", arXiv preprint arXiv:1904.00373, 2019.
- [17] A. Kumar, M. Bharti, and T. Kumar, "Performance Investigation of 2-D Optical Orthogonal Codes for OCDMA", *Journal of Optical Communications*, vol. 40, no. 4, pp. 455–462, 2019.
- [18] V. Jyoti, and R. S. Kaler, "Security Enhancement of OCDMA System Against Eavesdropping using Code-Switching Scheme", *Optik*, vol. 122, no. 9, pp. 787–791, 2011.
- [19] S. Kaur, and S. Singh, "A Novel Zero Cross-Correlation Diagonal Identity Matrix Code", In 2018 6th Edition of International Conference on Wireless Networks & Embedded Systems (WECON) pp. 1–5. IEEE, (2018, November).
- [20] T. M. Bazan, D. Harle, and L. Andonovic, "Performance Analysis of 2-D Time-Wavelength OCDMA Systems with Coherent Light Sources: Code Design Considerations", *Journal of lightwave technology*, vol. 24, no. 10, pp. 3583–3589, 2006.
- [21] S. M. J. Shah, A. Nasir, and H. Ahmed, "A Survey Paper on Security Issues in Satellite Communication Network Infrastructure", *International Journal of Engineering Research and General Science*, vol. 2, no. 6, pp. 887–900, 2014.
- [22] D. He, X. Li, S. Chan, J. Gao and M. Guizani, "Security Analysis of a Space-Based Wireless Network", *IEEE Network*, vol. 33, no. 1, pp. 36–43, 2019.
- [23] R. Canetti, and H. Krawczyk, "Analysis of Key-Exchange Protocols and their Use for Building Secure Channels", In International Conference on the Theory and Applications of Cryptographic Techniques, pp. 453–474. Springer, Berlin, Heidelberg, (2001, May).
- [24] R. Gupta, and R. S. Kaler, "Performance Comparison of Pre-, Boost-, and Inline-Multimode Erbium-Doped Fiber Amplifier Configurations to Boost Mode-Division Multiplexed Multimode Fiber Link", *Optical Engineering*, vol. 55, no. 5, pp. 056102, 2016.
- [25] P. K. Teotia, and R. S. Kaler, "1-D Grating Based SPR Biosensor for the Detection of Lung Cancer Biomarkers using Vroman Effect", *Optics Communications*, vol. 406, pp. 188–191, 2018.
- [26] S. Singh, R. S. Kaler and S. Sharma, "FEM Simulation Analysis of Fiber Optic Surface Plasmon Resonance Sensor Based on Array of Circular Gold Nanorod", *Optik*, vol. 183, pp. 508–512, 2019.
- [27] H. K. Gill, N. S. Grewal, and G. K. Walia, "Comparative Investigation of CSRZ-DQPSK, DRZ-DQPSK and MDRZ-DQPSK Modulation Techniques in MDM IS-OWC System", *Microwave and Optical Technology Letters*, vol. 61, no. 7, pp. 1802–1809, 2019.
- [28] A. Amphawan, S. Chaudhary, T. Elfouly, and K. Abualsaud, "Optical Mode Division Multiplexing for Secure Ro-FSO WLANs", *Advanced Science Letters*, vol. 21, no. 10, pp. 3046–3049, 2015.
- [29] K. Fouli and M. Maier, "Ocdma and Optical Coding: Principles, Applications, and Challenges", *IEEE Communications Magazine*, vol. 45, no. 8, pp. 27–34, 2007.
- [30] S. Singh R.S. Kaler and S. Sharma, "Resonance Effect of Bimetallic Diffraction Grating on the Sensing Characteristics of Surface Plasmon Resonance Sensor with COMSOL Multiphysics", *Journal of Nanoelectronics and Optoelectronics*, vol. 14, no. 5, pp. 669–674, 2019.
- [31] T. Sharma, and R. K. Maddila, "Performance Characteristics of the Spectral-Amplitude-Coding Optical CDMA System Based on One-Dimensional Optical Codes and a Multi-Array Laser", *Ukr. J. Phys. Opt.*, vol. 20, no. 2, pp. 81, 2019.
- [32] J. C. Cartledge, G. S. Burley, "The Effect of Laser Chirping on Lightwave System Performance", *Journal of Lightwave Technology*, vol. 7, no. 3, pp. 568–573, 1989.
- [33] S. Kaur, and S. Singh, "Review on Developments in All-Optical Spectral Amplitude Coding Techniques", *Optical Engineering*, vol. 57, no. 11, pp. 116102, 2018.

Received 30 October 2020