Security and performance evaluation of different pulse shapes in diagonal identity matrix codes

SIMARPREET KAUR[a,*], SIMRANJIT SINGH[b,*]
[a]*Department of Electronics and Communication Engineering, CEC, Landran, Mohali, 140307, Punjab, India*
[b]*Department of Electronics and Communication Engineering, Punjabi University, Patiala, 147002, Punjab, India*

A security postulate of optical code division multiplexing codes is an imminent forte to study for the elimination of the threats of eavesdropping. OCDMA system suffers from multiple access interference and cross correlation effects. In this research article, a high speed (30 Gbps) coherent spectral amplitude coding based OCDMA system is proposed by constructing a novel ZCC code termed as diagonal identity matrix code. Further, uni-phase, bi-phase and quad-phase modulations are investigated in the system and their security traits are explored. An expression is derived for the estimation of the signature code by the eavesdropper in the presence three modulations. In order to facilitate the large number of users, a mapping free code is designed. DQPSK (quad-phase) modulation is found out to be maximum secure against eavesdropper out of uni and bi-phase modulations.

(Received July 2, 2020; accepted June 11, 2021)

Keywords: Uni-phase (NRZ, RZ), Bi-phase (CSRZ, MDRZ, DPSK), Quad-phase (DQPSK), Spectral amplitude coding, Zero cross correlation codes, WDM, TDM, OCDMA

1. Introduction

Recent trends in optical communication systems are taking communication towards enormous transmission capacity with the incorporation of multiple access techniques such as wavelength, time, spatial and code division multiplexing. Optical code division multiplexing is a prominent technology in optical networks which has numerous advantages like more security, transparency, high capacity and improved spectral efficiency [1]. Threats of secret information breaching by un-authentic user in OCDMA are far more less than WDM and TDM system because of specific code chips in OCDMA [2]. High number of users increases code length and it improves the security of the system against eavesdropper due to large code combinations [3]. However, MAI and cross correlation are also prominent limitation in non-zero cross correlation codes (NZCC) [4]. Zero cross correlation codes are free from cross correlation effects but MAI exists due to presence of code wavelengths, time and polarizations [5]. Add/drop, multiplexing can be performed over single network with OCDMA [6]. Diverse code chips allow many users to communicate within same communication channel at same time without interfering with each other. Spectral amplitude coding is a type of OCDMA codes where frequency components are fixed in accordance with the signature codes and transmits or blocks with reference to this code so that specific user get accessed [7]. SAC OCDMA systems are based on incoherent sources and are employed where less cost expenditure is required on the system. However, due to incoherence of light emitting diodes, capability to cater high speed systems is less in SAC OCDMA [7]. Diverse codes are reported such as Enhanced Double weight code, Multidiagonal code, Diagonal Double weight code, Hadamard code, Modified Double weight code, etc [8] [9] [10]. In recent times, laser sources are incorporated in SAC OCDMA to support high speed, capacity and larger distances [11] [12]. Major issue across which researchers came by analyzing them is MAI. Utmost goal in ZCC codes is to reduce MAI and increase capacity of SAC systems. To eliminate the existing constraint in codes, a DIM has been presented with ZCC with flexibility to opt the desired code weight.

Pulse shaping in optical networks plays an important role and decides the overall performance of the system. Optical code division also gets effected significantly by different modulations which further influence security, intra-channel dispersion, and performance of the system. Eavesdropper's probability to detect authentic data gets reduced due to the presence of multi-level modulations. Moreover, advanced pulse shapes can also enhance spectral efficiency and saves bandwidth [13] [14]. In this work, we emphasised to provide a generation of DIM algorithm and also study effect of different pulse shapes on the security of system and further evaluate performance in terms of Q and BER.

2. Code construction

OCDMA system security is a prominent forte to study and it is performed in different research works such as [15][16]. Also, comparison of proposed code is also done in [11] with other existing codes and it was perceived that performance of proposed code is better.

The Generalized code construction algorithm is explained below. Algorithm of the proposed code is given as:

Step 1: First and foremost, users (k) need to be fixed and further, weight of the code is required such as W=2, 3, 4 …., N for every user.

Step 2: Total length of the proposed code is calculated as:

$$L=K * W$$

Step 3: After code length calculation, a basic matrix construction is required as shown below:

$$I_B=2 \text{ x } W \text{ (Balanced)}$$

Step 4: For any number of selected users, Y x Z order matrix is constructed as:

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

Where Upper End is UE and Lower End is LE

Step 5: For K users, required code set is shown as M for K users. For the realization of the M, three steps are followed using an intermediary matrix M^1, M^2 and M^3. M^1 is given below and I_B is repeated K -1 times in it.

$$M^1=\begin{bmatrix} UE\cdots\cdots\cdots LE \\ LE\ UE\ \cdots\cdots\cdots \\ \cdots\cdots LE\ UE\ \cdots\cdots \\ \cdots\cdots\ LE\ UE\cdots \\ \cdots\cdots\cdots\ LE\ UE \end{bmatrix}$$

For M2, Repeat the process for K X L times as given below:

$$M^2=\begin{bmatrix} UE\cdots\cdots\cdots LE \\ LE\ UE\ \cdots\cdots\cdots \\ \cdots\cdots LE\ UE\ \cdots\cdots \\ \cdots\cdots\ LE\ UE\cdots \\ \cdots\cdots\cdots\ LE\ UE \end{bmatrix}_{Kx\ L}$$

For the final matrix, zeros are filled in the empty space to realize M

$$M=\begin{bmatrix} UE\ 00\ 00\ 00\ LE \\ LE\ UE\ 00\ 00\ 00 \\ 00\ LE\ UE\ 00\ 00 \\ 00\ 00\ LE\ UE\ 00 \\ 00\ 00\ 00\ LE\ UE \end{bmatrix}_{Kx\ L}$$

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

DIM codes have auto-correlation of 2 and cross correlation of 0. The following flow diagram i.e. Fig. 1 depicts how the Diagonal Identity Matrix code is constructed and implemented.

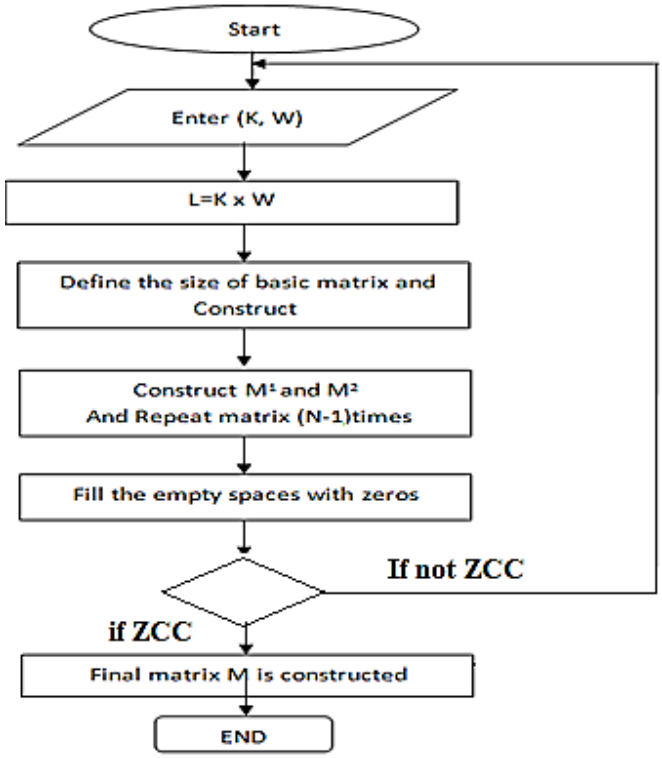

Fig. 1. DIM code based Flow diagram

3. System setup

Diagonal identity matrix codes are implemented in Optiwave's Optisystem at data speed of 30 Gbps. Use of coherent optical laser sources has been done according to the code (length, weight). For the encoding of serial data streams from binary bits generator, different pulse shapes are employed such as on-off keying (non return to zero, return to zero), differential phase shift keying (DPSK), compressed spectrum return to zero (CSRZ), modified duo-binary return to zero (MDRZ), differential quadrature phase shift keying (DQPK). Each user is passed through multiplexer and combined signal is fed to single mode fiber (SMF-28) which is having attenuation of 0.2 dB/km and pulse broadening of 17 ps/nm/km along with nonlinear effects. Decoder of each pulse shaper modulation is according to modulation such as in OOK, CSRZ, and MDRZ and single photodetector is used. For DPSK, and DQPSK, balanced photo detection is employed. Fig. 2 depicts the spectrum amplitude coding based system incorporating generalized code. For the accomplishment of the operation to select the required wavelength, a filter is placed after SMF as specified by the code matrix. This filter section is followed by decoder (respective to the phase of modulation) which does photon to electric conversion using photo detector and then low pass bessel filter eliminates the emerged noises. BER in the end of the simulation is located to find out the output parameters such as Q factor and BER. System specifications are shown in Table 1.

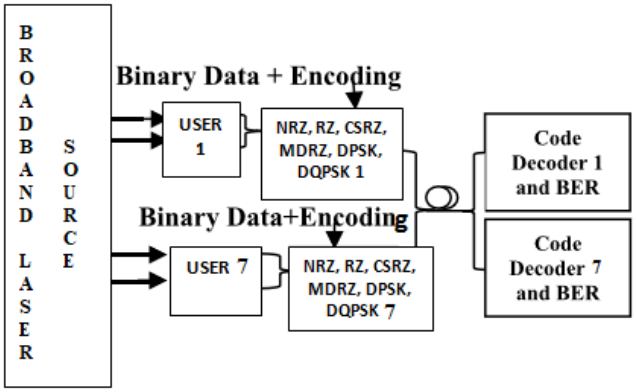

Fig. 2. Block diagram of DIM system employing different modulations

Table 1. System specifications of proposed system

Input Parameters	Values
Light source	Continuous wave Laser
Polarization Mode Dispersion	0.2 ps/nm/km
Power	0 dBm/channel
Attenuation	0.2 dB/km
Transmission Distance	10 Km
Data Rate	30 Gbps/channel
Laser Linewidth	10 MHz
Fiber	SMF 28
Dispersion	17 picosec/nm/km
Freq. Band	C Band (1530-1565 nm)
Light source	Continuous wave Laser
Polarization Mode Dispersion	0.2 ps/nm/km

3.1. Probability of estimation of correct code word for eavesdropper using different modulations

First and foremost probability of correct code word from an un-authentic user is derived from metadata information. In any OCDMA code, code length depends upon code weight and number of users. Combination of authentic code wavelengths increases with the increase in code length and it is perceived that eavesdropping becomes a bit tedious in prolonged code lengths signature codes. Total combinations are given as:

$$T_C = n_{C_W} \tag{1}$$

If there is cross-correlation in the code then it creates chaos but eavesdropper can fix interfering wavelengths which ultimately can fix the position of wavelength in code and total cross-correlation cases are given as

$$T_{\lambda c} = n_{C_{\lambda c}} \tag{2}$$

From total cases, cross correlation cases are subtracted to find out the remaining cases

$$T_{Cr} = n_{C_W} - n_{C_{\lambda c}} \tag{3}$$

Presence of the total pulses is half for the total users and total pulses are considered as

$$P(p) = (\frac{1}{2})^K \tag{4}$$

However, probability of an eavesdropper to detect the correct codeword is ½ and after combining the aforementioned equations, expression is given as

$$P(E) = \frac{1}{n_{C_W} - n_{C_{\lambda c}}} \left(\frac{1}{2}\right)^K . \left(\frac{1}{2}\right) \tag{5}$$

Further P(E) is calculated for the different pulse shapes such as NRZ, RZ, CSRZ, MDRZ, DPSK and DQPSK. In on off keying, P(E) is same as given in (5) such that eavesdropper can either detect true or false bit because there is information on 1's and no information on 0's. However, due to noise or different wavelength combination, probability of eavesdropper to get true pulse is half. Further it is important to see that if there are phase shifts in the data stream, detection of correct bit at eavesdropper further decreases. In case of CSRZ, MDRZ and DPSK, there are two phase shifts such as 0 and 180 which complicate the eavesdropping process. Probability of estimation is modified for two shifts which is given as:

$$P(E) = \left(\frac{1}{2}\right)_{phase\ shifts} \frac{1}{n_{C_W} - n_{C_{\lambda c}}} \left(\frac{1}{2}\right)^K . \left(\frac{1}{2}\right) \tag{6}$$

Further, differential quadrature phase shift is discussed and probability of estimation for eavesdropper is calculated and it is observed that due to four phase shits, eavesdropping gets difficult because data is in chaos more than double phase shift modulations and P(E) is given as

$$P(E) = \left(\frac{1}{4}\right)_{phase\ shifts} \frac{1}{n_{C_W} - n_{C_{\lambda c}}} \left(\frac{1}{2}\right)^K . \left(\frac{1}{2}\right) \tag{7}$$

Probability of authentic user to detect the intended signal is simply as

$$P(A) = 1 - P(E), \tag{8}$$

where $P(A)$ is probability of authentic user.

3.2. Results and discussion

For the analysis of security of the different pulse shapes in the proposed OCDMA system incorporating DIM codes, probability of estimation of eavesdropper is calculated when different users are accommodated in the system. It is evident that despite the secured nature of OCDMA, information can be taken by the un-authorized user and in case of OOK pulse format, energy is only present at one's and therefore continuous exposure of data

to photon counter can make eavesdropping easy. Also, there is another trait of OCDMA that if larger code lengths are send to the fiber, then it leads to the wastage of bandwidth to some extent but it has prominent advantage that longer code lengths bring eavesdropping down due to more required combinations to identify authorized bits or it may take several years if code length is extremely very large. Fig. 3 represents the probability of estimation of eavesdropper versus number of users for different modulation and in the following graphical representation, we have categorized modulation under three categories such as uni-phase (NRZ, RZ), bi-phase (CSRZ, MDRZ, DPSK) and quad-phase (DQPSK). P(E) decreases as the users in the system increase because code length enhances. From equation (5) (6) (7), it is evident that probability of estimation becomes less if denominator is large and cross correlation is minimum or we can say approaches to 0. In case of DQPSK, P(E) is least because of larger denominator of the equation. Security of quad-phase is maximum followed by bi-phase and least security is in the case of uni-phase. Quad phase modulation has very high dispersion tolerance and bandwidth efficiency is too high due to due to 0, 90, 180, or 270 degrees phase shifts. In case of bi-phase, dispersion tolerance is lower than quad phase modulation because of only two phase shifts (0 and 180).

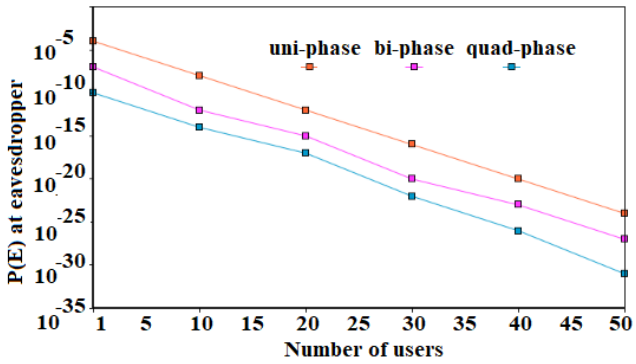

Fig. 3. Effect of users and modulations on probability of estimation of eavesdropper (color online)

Authentic user's correct word detection is shown in Fig. 4 with the variation of signal to noise ratio. Major performance deteriorating factor of the signature codes performance is the cross correlation that interferes with the data of consecutive user. However due to ZCC code, only MAI exists due to wavelengths of multiple users in optical fiber.

It is evident that greater signal power and less noise power leads to a high signal to noise ratio in case of quad phase modulation and therefore with increase in SNR, more and more correct words are comprehended by the receiver for DQPSK and in general for all modulations. Least correct detection is observed in uni-phase modulation because of maximum intra-channel dispersion. Pulse exceeds its intended time slot in case of uni-phase modulation however these effects are less in case of bi and quad phase modulations.

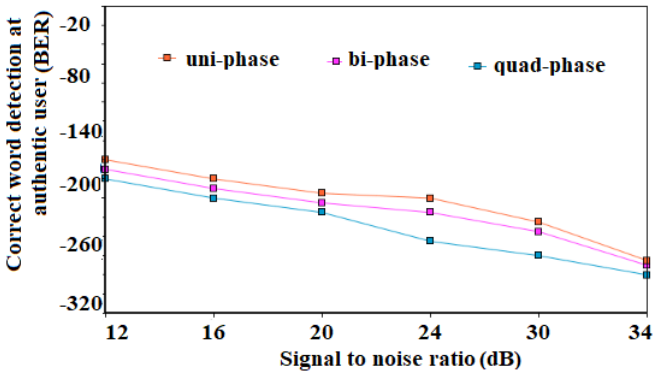

Fig. 4. Correct code word variations with SNR (dB) in case of uni, bi and quad phase modulations (color online)

Further probability of eavesdropper to detect pure authentic signal is calculated and how it is changed with SNR in case of uni-phase, bi-phase and quad-phase modulations is observed. Direct chip decoding of the received signal is done by the eavesdropper with bandpass filter. Spectral matching is performed at this bandpass filter to decode authorized signal. Decoder consists of photo detectors and received photons are converted into electrical signals and further processed by the decision signal. Determination of eavesdropper's receiver is done form signal detection theory. Decisions of the outputs are shown in Table 2 and the eavesdropper will wish to identify encoded pulses at the time of their presence and when pulse is not present, eavesdropper intend to ignore it. For P_F to be zero, eavesdropper choose threshold according to this so that he may have least false alarms and also highest probability of detection P_D=1. Optimal threshold can be fixed by checking parameters like code length, weight and SNR. Also, detection by the eavesdropper depends upon the time for which original signal gets exposed to it and type of detection used.

Probability can be calculated from detection analysis with probability of missing a transmitted pulse in a given time (P_M) and false detection of pulse ($P_{F)}$. Probability of error-free code word detection for the code inceptor depending on the encoded data bit interval:

$$P_{correct} = (1-P_M)^W (1-P_F)^{(N-W)} \quad (9)$$

$$P_F = \exp\left(\frac{-\gamma}{No}\right) \quad (10)$$

where γ and N_o are detection threshold and noise power spectral density respectively, $P_{M,}$ P_F is the probability of missing a transmitted pulse in a given time and falsely detecting a pulse where none was transmitted.

Table 2. Decision possibilities corresponding to detection threshold

Event	Threshold	decisions
Signal pulse noise	≥	detection
Signal pulse noise	<	miss direction
Noise	≥	false alarm
Noise	<	no false alarm

Fig. 5 depicts that the increase in signal to noise ratio increases the threshold and decreases the spectral noise which means at higher values of SNR, P_F is less and therefore $P_{correct}$ at eavesdropper increases. Values of $P_{correct}$ are more for uni-phase modulations because of lower threshold and more noise and therefore an eavesdropper can detect the original signal. However, in case of quad-phase modulation, due to less intra channel interference, more signal amplitude is received and spectral noise is low resulting in high spectral efficiency. Probability of false signal at eavesdropper is more and therefore $P_{correct}$ is least in this case.

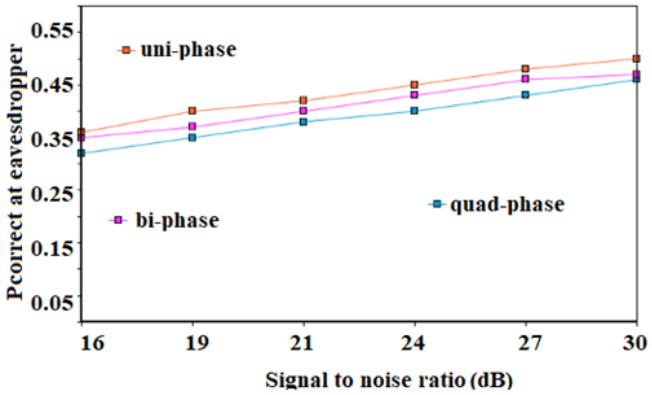

Fig. 5. Probability of correct words at eavesdropper in case of different modulations (color online)

Exact time of the coded pulse without any pulse broadening or with pulse width reduction give user better results. Therefore, confinement of pulses has significant effects on communication systems. Here, in Fig. 6, an emphasis was made to evaluate the effects of different chip sizes of the encoded pulses in terms of correct detection rate at authentic user's receiver. Chip size was oscillated to vary from 0.10 ns to 0.025 ns with the difference of 0.20 ns. Analysis revealed that shorter time chips cause more errors and provide reduced correct detection rate at receiver of authentic user. This is because of the performance deteriorating effects of the pulse broadening inside fiber optic (0.17 ps/nm/km). Prominence of intra-code interference is more at larger distances as well as at short timing chips. In case of quad-phase modulations, dispersion effects are least so, the correct code word detection at the authentic user increases and in case of uni-phase, pulse broadening is more and thus, when time slot decreases due to higher chip rates, more error occurs.

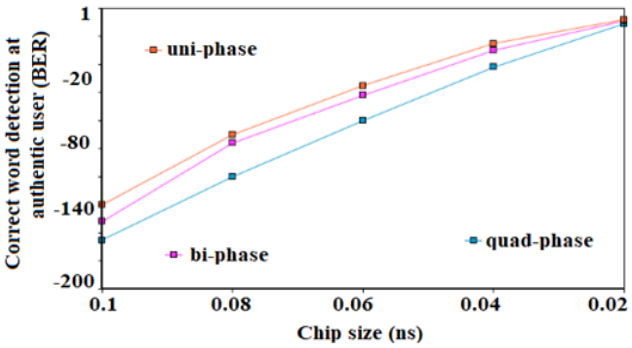

Fig. 6. Effect of chip size on the performance of different modulations in terms of correct detection at authentic user (color online)

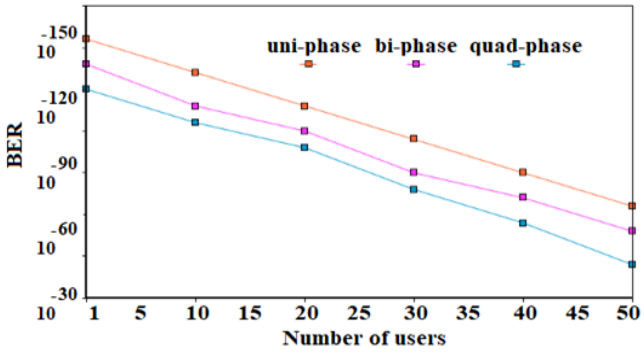

Fig. 7. Variation of BER with the number of users at authentic user (color online)

Variation of Bit error rate at the authentic user with the number of users is plotted in Fig. 7. It is perceived that the performance of all the three modulations deteriorate with the increase in the users. Decreasing trend in BER is more incase of the quad phase modulation because of high security and more dispersion tolerance along with higher bandwidth efficiency. Eye diagram of quad-phase (DQPSK in this study), bi-phase (DPSK) and uni-phase (NRZ) is shown in Fig. 8 (a), 8 (b) and 8 (c). It is observed that eye opening of quad-phase modulation is maximum because of high Q factor of received signal, least jitter and minimum eye closer. Eye diagram of uni-phase is worst because of bandwidth inefficiency and high dispersion effects.

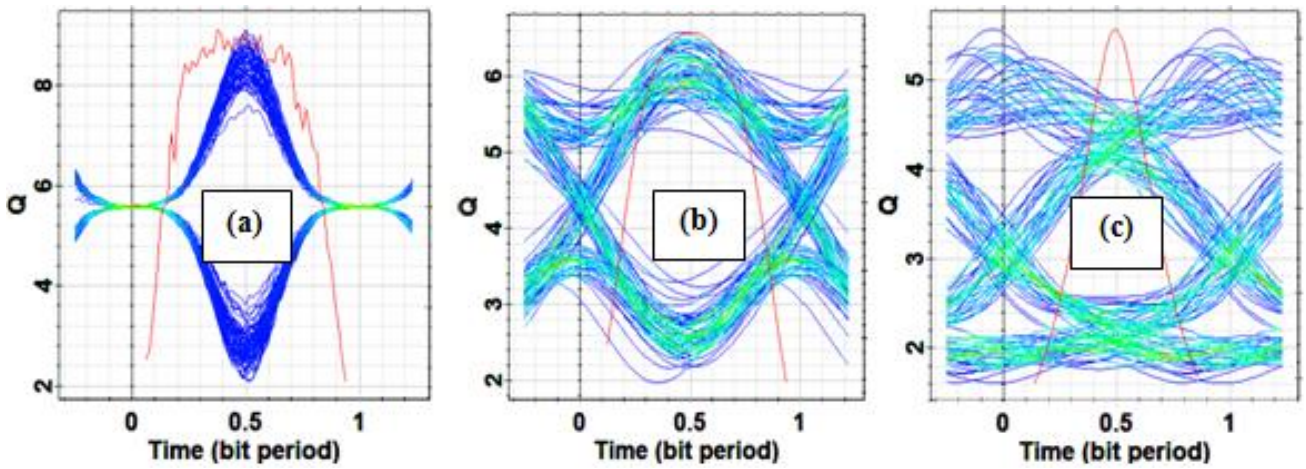

Fig. 8. Eye diagrams at 10 Gbps for 100 km in case of (a) Quad phase (DQPSK) (b) Bi phase (DPSK) (c) Uni phase (NRZ) (color online)

4. Conclusion

In this work, performance and security analysis of different pulse modulations are accomplished in spectral amplitude coded 30 Gbps diagonal identity matrix OCDMA system. Three different modulations such as uni-phase (NRZ, RZ), bi-phase (CSRZ, MDRZ, DPSK) and quad-phase (DQPSK) are compared in terms of probability of estimation of original signal at eavesdropper, correct code word detection at authentic user, $P_{correct}$ at eavesdropper when SNR, chip size and number of users are varied. Mathematical derivation for the probability of estimation at eavesdropper in case of three modulations has been done and results revealed that due to the four phase shifts in case of DQPSK, P(E) at eavesdropper is less, correct codeword detection at authentic user is more and due to least intra channel dispersion effects, performance is the best. On the other hand, performance and security traits of bi-phase modulations are followed by uni-phase modulation. Therefore, for performance enhanced and highly secured SAC-OCDMA system, combination of DQPSK and diagonal identity matrix codes is an optimal choice and proposed code construction is cross correlation free, simple and support high speeds.

References

[1] P. R. Prucnal, "Optical code division multiple access: fundamentals and application", Taylor & Francis Group, 2006.
[2] D. Schilling, L. Milstein, R. Pickholtz, IEEE Trans. Commun. **25**(8), 748 (1997).
[3] P. C. Teh, "Applications of superstructure fibre Bragg gratings for optical code division multiple access and packet switched networks", in Doctoral Thesis. University of Southampton: Optoelectronic Research Centre, pp. 230, 2003.
[4] M. Brandt-Pearce, B. Aazhang, IEEE Trans Commun. **42**, 2 (1994).
[5] I. Sanz, M. A. Muriel, Opt. Engineering **32**(3), 481 (1993).
[6] Michel E. Marhic, Lightwave Tech. **11**(5), 854 (1993).
[7] M. Santoro, T. Fan, P. Prucnal, IEEE Lightwave Tech. **4**(5), 307 (1986).
[8] J. Hui, IEEE Journal on Selected Areas in Communications **3**(6), 916 (1985).
[9] H. Ishio, J. Minowa, K. Nosu, Journal of Lightwave Technology **2**(4), 448 (1984).
[10] Z. Jiang, D. S. Seo, S. D. Yang, D. E. Leaird, R. V. Roussev, C. Langrock, M. M. Fejer, A. M. Weiner, Journal of Lightwave Technology **23**(1), 143 (2005).
[11] S. Kaur, S. Singh, Optical Engineering **57**(11), 116102 (2018).
[12] M. Moghaddasi, G. Mamdoohi, A. S. M. Noor, S. B. A. Anas, Optics Communications **356**, 282 (2015).
[13] S. Singh, R. Kaur, A. Singh, R. S. Kaler, Optical Fiber Technology **22**, 84 (2015).
[14] K. Singh, M. Singh, K. S. Bhatia, H. S. Ryait, Journal of Optical Communications **37**(2), 227 (2015).
[15] T. Sharma, M. Ravi Kumar, Optical and Wireless Technologies **546**, 477 (2019).
[16] H. A. Bakarman, S. Shaari, M. Ismail, Journal of Optical Communications **30**(4), 242 (2009).

*Corresponding author: kaursimarpreet1291@gmail.com
simrankatron@gmail.com