Оптический журнал

Оптическое приборостроение

УДК 091

Повышение безопасности путем обмена битов, принадлежащих различным каналам передачи данных

© 2021 г. Simranjit Singh

Предложена простая схема кодирования для повышения безопасности в полностью оптических сетях. Схема основана на обмене битов между потоками данных в двух различных каналах, что создает два искаженных потока битов. Используемые шифратор и дешифратор могут быть созданы на основе коммерчески доступных компонентов. Проведена оценка эффективности предложенной технологии на системном уровне для нескольких диапазонов в волоконных линиях связи с встроенными оптическими усилителями. Численное моделирование показало, что потоки данных могут быть успешно декодированы с приемлемым уровнем частоты ошибок по битам на дистанции 500 км.

Ключевые слова: *полностью оптическая обработка данных, информационная безопасность, оптическая связь*

Security enhancement by swapping bits belonging to different data channels

© 2021 Simranjit Singh, PhD

Advanced Photonics and Optical Networking Research Lab, Department of Electronics and Communication Engineering, Punjabi University, Patiala, India

E-mail: sjsingh@pbi.ac.in

Submitted 24.08.2020

DOI:10.17586/1023-5086-2021-88-09-63-68

A simple coding scheme is proposed to enhance the information security in all-optical networks. It is based on swapping of data bits belonging to two different channels to form two garbled bit streams. The encryptor and decryptor designs used here can be implemented by using commercially available components. The performance of the proposed technique is evaluated at the system level by considering multiple spans of optical fibers with in-line optical amplifiers. Numerical simulations show that the decoded bit streams can be recovered with acceptable bit error rates after 500 km.

Keywords: *all-optical processing, information security, optical communication.*

OCIS codes: *060.2330, 060.4510, 060.4785*

1. INTRODUCTION

Unlike the traditional optical communication networks, where each data channel undergoes optical-electrical-optical conversions, an all-optical network maintains all channels in an optical form over long distances [1, 2]. For many

applications secure transmission of the data is essential. This is accomplished through data encryption at the transmitter together with a suitable decryption scheme at the receiver. An all-optical encryption/decryption operating with ultrafast rates and does not emanate an electromagnetic signature as does in electronic counterpart [3].

Several optical security techniques have been proposed in recent years to ensure the privacy of the data over an optical network. Kotb *et al.* have proposed all-optical gates [1–2]. These gates can be used to encrypt the data with encryption key. An all-optical pseudorandom bit sequence was used to generate a complex key for one-time-padding. The use of multiple delay lines to construct an all-optical pseudorandom bit sequence generator makes such a scheme complex and expensive. A one-time-pad scheme can provide unconditional transmission confidentiality, but it requires unpredictable keys distributed via quantum communication, which limits the speed. Kostinski *et al.* have found that an optical code division multiple access technique with two-code keying (bits are represented by one of the two codes) enhances the security when compared to on-off-keying, since an eavesdropper cannot rely on simple energy detection to differentiate bits [4]. A variable two-code scheme based on XOR operation was proposed to produce random code to represent each data bit.

Chang *et al.* introduced multi-code-keying for enhancing physical-layer confidentiality in optical networks [5]. In this paper, we propose a novel technique to enhance the security that mixes the data streams of two or more users onto one channel frequency. The key idea behind the proposed technique is to swap the data bits of one user with the data bits of other users in a predefined manner. Apart its cost-effectiveness, this technique provides high security. Moreover, it can be combined with other coding techniques. For example, if one-time-pad is used for additional security, even if an eavesdropper is able to extract the secret key from the hidden channel, data remains secured because of its mixed nature [6].

2. PROPOSED ALL OPTICAL CODING SCHEME

To present our basic idea as simply as possible, we first focus on mixing of data bits of two users denoted as U1 and U2. Figure 1 shows the proposed scheme. The bit streams of the two users are divided into blocks, containing a predetermined number of bits. Although the optimum number of bits per block will depend on the actual system design, we choose 8 bits per block for the examples of this paper. The top row of Fig. 1 shows how the data blocks of each user are numbered. The bottom part of Fig. 1 shows how the blocks of two users are swapped to create two new mixed bit streams. In the example shown, the even number blocks are swapped between the two users. Of course, a more complex swapping scheme can also be easily implemented. As long as an eavesdropper does not know the swapping scheme adopted, user's data remain secure even if the eavesdropper manages to recover the transmitted data before it arrives at the receiver. Conceptually, one can also think of the proposed scheme as coding of one user's data using the data of another user.

For further security, any of the arm of Fig. 1 can be encrypted with a secret key using the one-time-pad method. In this case only one secret key and one XOR operation will be needed to encrypt data from both users, which is a cost effective solution over the scheme of Ref. [5].

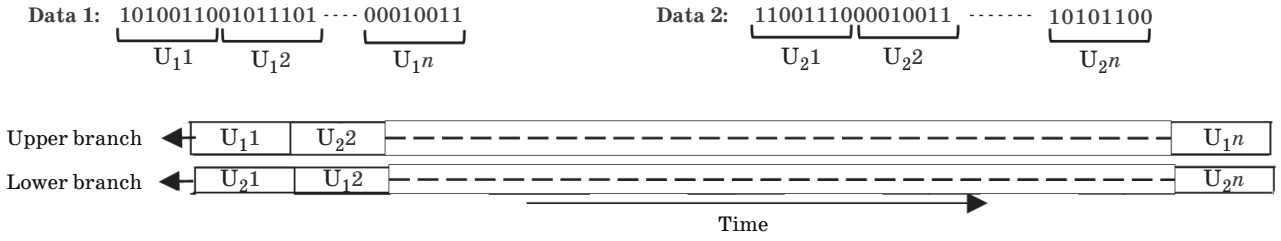

Fig. 1. Schematic of the swapping scheme. In U_nP notation, n represents the user number and P represents the block number.

If an eavesdropper wants to recover the data, he/she first has to crack the one-time-pad encryption and then need to know the swapping scheme adopted at the transmitter.

3. ENCRYPTOR AND DECRYPTOR DESIGNS

We checked the performance of the proposed coding scheme using the OptiSystem14.2 software. The encryptor and decryptor designed to implement the swapping scheme are shown in Fig. 2. The observation points, 1 to 4 at the transmitter and 5 to 8 at the receiver, are used to check the data sequences at different locations. At the encryptor side, each data stream at the transmitter is split into two branches. The upper branches employ two amplitude modulators (AM1 and AM3 for U1 and U2 respectively) that modify the optical signal according to an electrical control signal. The lower branches also employ two amplitude modulators (AM2 and AM4 for U1 and U2 respectively) driven with an inverted version of the control signal. The four AMs operating with a given control signals are responsible for swapping data blocks of two users.

Figure 2 shows in detail how the data blocks of U1 or U2 can be swapped using power combiners and amplitude modulators. For example, at the point OP4, after combining the outputs of AM1 and AM4, the data blocks appear U1, U2 (it can also be seen in Fig. 1 upper branch). The same control signals are used on the decryptor side to recover the data streams of both users.

In this work, not-return-to-zero data streams (each at a 2.5 Gbit/s bit rate) are employed at a wavelength centered at 1550 nm. The average power of both the input data signals is 1 mW. For illustration we have taken the original data sequences of two users as 1010011001011101 and 1100111000010011 for U1 and U2 respectively. The control signal is in the form of 8-bit wide voltage pulses at a frequency that is $1/4^{th}$ of the original data, means first half of the signal voltage (for 8 data bits) is ON and last half of the signal voltage is OFF which drive AM1 and AM3.

On the other hand, an inverted version of this control signal drives AM2 and AM3. Of course, the modulation frequency will be even lower if block size was made longer. The data blocks of both users emerging from AM1 to AM4 are: AM1 — 1010011000000000, AM2 — 0000000001011101, AM3 — 1100111000000000, and AM4 — 0000000000010011 respectively. As expected, owing to the absence of control voltage, the time slots of the last eight bits after AM1 and AM3 or the first eight bits after AM2 and AM4 are empty. These empty slots are filled by combining the outputs of AM1 with AM4 and AM2 with AM3 respectively resulting in a mixed sequence of both data. The mixed version

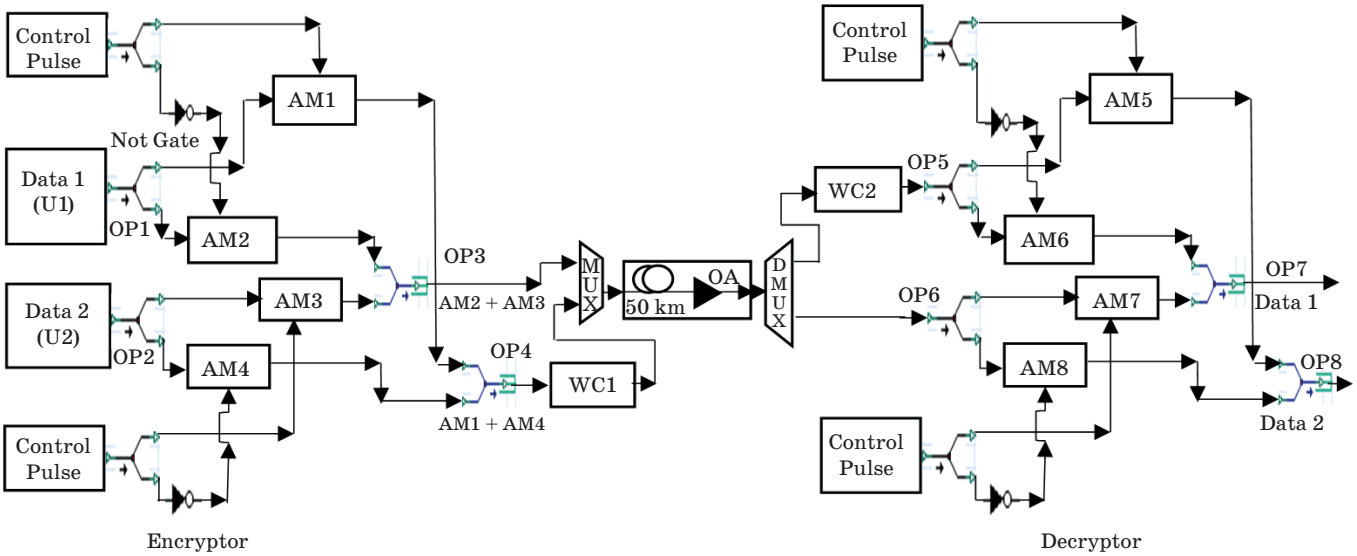

Fig 2. Encryptor and decryptor designs. WC represents wavelength converter, OA represents optical amplifier, AM represents amplitude modulator, OP represents observation points.

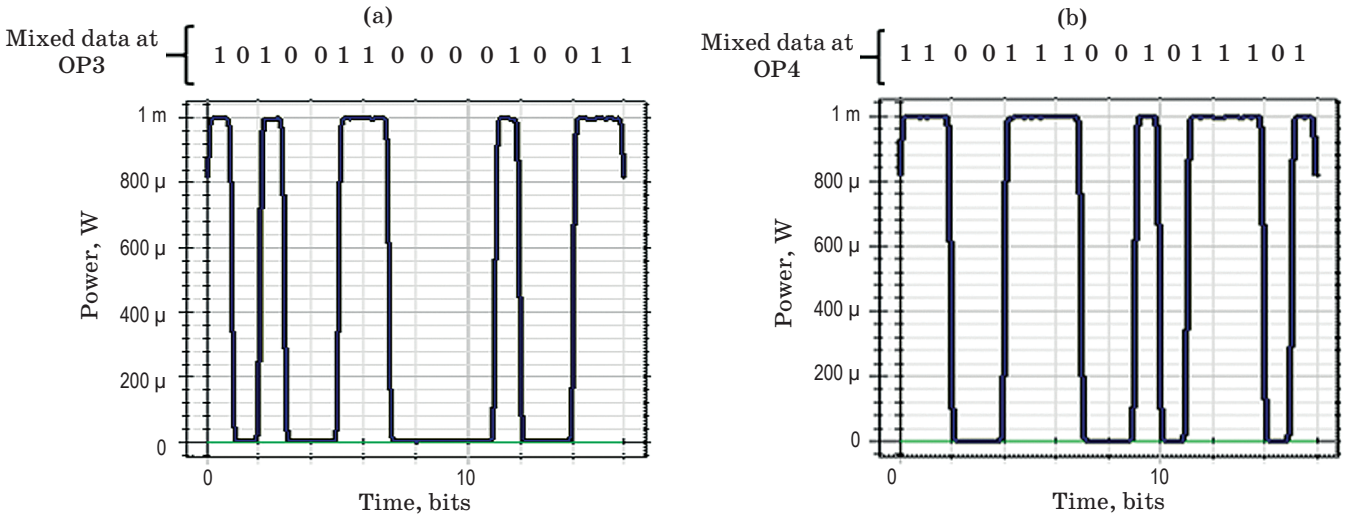

Fig. 3. Bit sequences at (a) OP5 and (b) OP6 at the receiver before decoding.

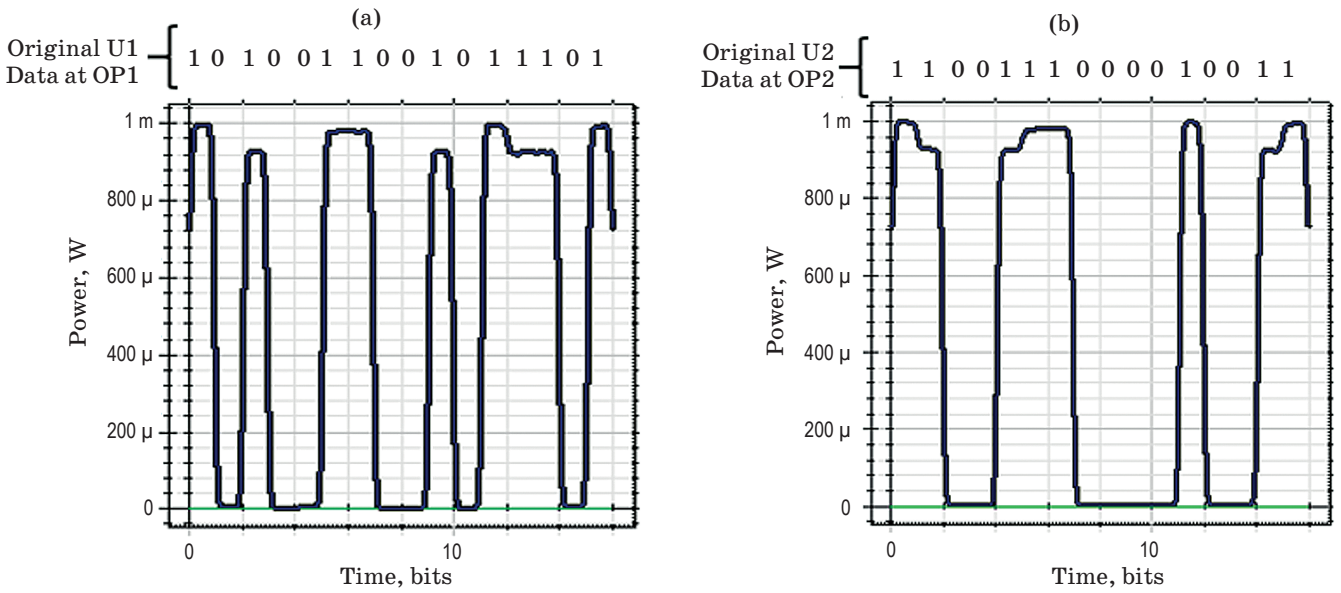

Fig. 4. Recovered bit sequences at (a) OP7 and (b) OP8 at the receiver after decoding.

at both the encryptor and decryptor side can be seen in Fig. 3.

The decryptor uses the same process with an identical control signal to recover the actual data of both users from the mixed sequence. Figure 4 shows the both original data sequences at OP7 and OP8 recovered by the decryptor. The perturbations at the power levels of decrypted data (see Fig. 4) are due to a finite extinction ratio of AMs [4]. Amplitude modulators transmit some undesired power even when the control signal is off which disturb the power level of the combined bits at OP7 and OP8.

4. SYSTEM LEVEL SIMULATION

Further, to check the performance of proposed idea on system level a multiple 50 km fiber spans with an optical amplifier providing 10 dB gain are considered. Our numerical simulations include self-phase modulation (provide parameter value here), dispersion (16.75 ps/nm/km), polarized mode dispersion ($D = 0.05$ ps/km$^{1/2}$), and fiber loss (0.2 dB/km). At both OP3 and OP4 the optical signal with 1550 nm wavelength is present after mixing of data blocks. To send these signals over optical fiber it is necessary to convert the wavelength of

at least one arm. Here we have used a wavelength converter in the lower arm which shifts the operating wavelength (1550 nm) to 1549.2 nm (see Fig. 2). It induces another layer of security, because to crack the data the eavesdropper also needs to know the shifted wavelength.

After multiplexing, the wavelength division multiplexed signal is transmitted over multiple spans of fibers. Figure 5 shows the eye diagrams of both signals (1550 and 1549.2 nm) after 500 km (after 10 spans of 50 km fiber) for users received the cyphertext. Here we used fiber tapping scenario to detect the signal and assumed that the authorized users can access both the signals to recover the original data after decoding. To measure these eye diagrams the cyphertext (swapped data) is taken as a reference signal. These eye diagrams show good level of eye opening at 1550 and 1549.2 nm with acceptable bit error rate (BER) less than 10^{-9}. Here, to check the performance for un-authorized used, we have assumed that the eavesdropper has no knowledge of the swapping scheme and the operating wavelength, and have no meta information of the data. Obviously, to recover the original data an unauthorized users have to find the appropriate operating wavelengths and have to do exhaustive search of different combinations of data blocks. So, an unauthorized user (eavesdropper) cannot get any information as can be seen from the eye diagram shown in Fig. 6 with zero eye opening. To measure this eye diagram the original data (U1 data) bit sequence is considered as a reference signal and the user is tuned at 1555 nm [7–8].

The numerical results shown in Figs. 5 and 6 validate our proposed scheme of mixing of data streams of two users. Security can be further enhanced by employing one-time-padding on one of the branches of proposed encryptor. An advantage of this approach is that only one key is required to encrypt the data of both users. With this extension the data is doubly secure.

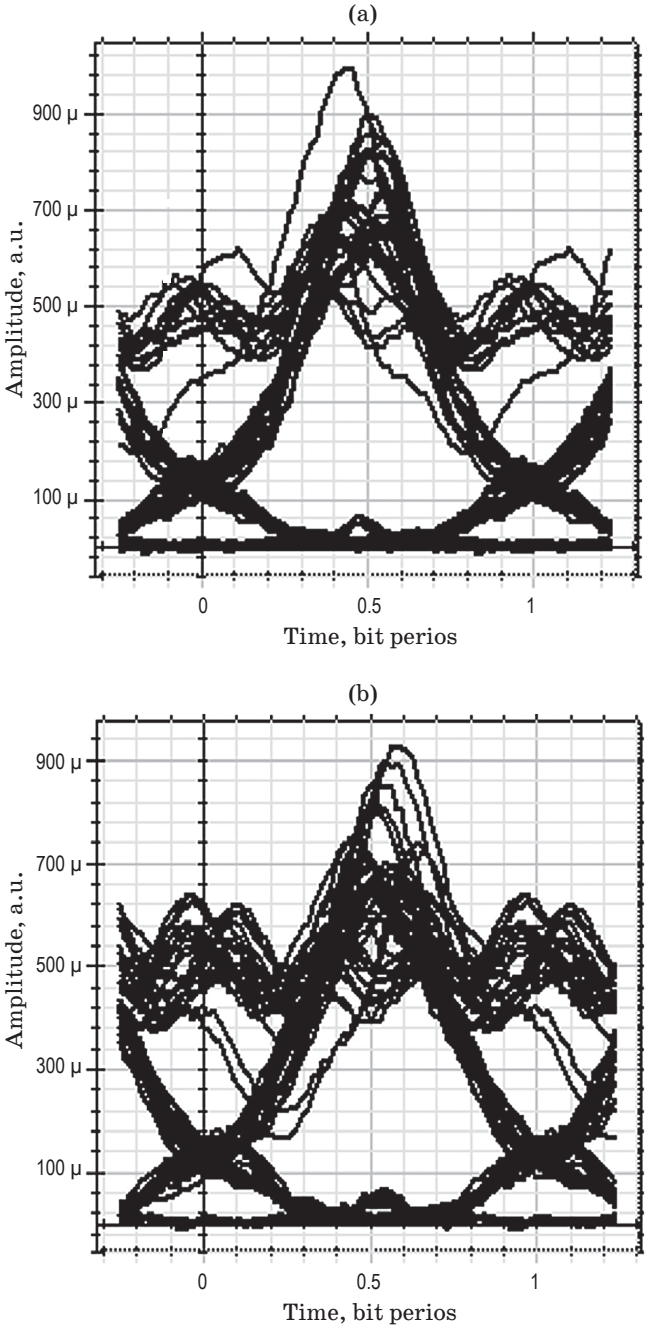

Fig. 5. Eye diagrams at (a) 1550 nm and (b) 1549.2 nm after 500 km for authorized users.

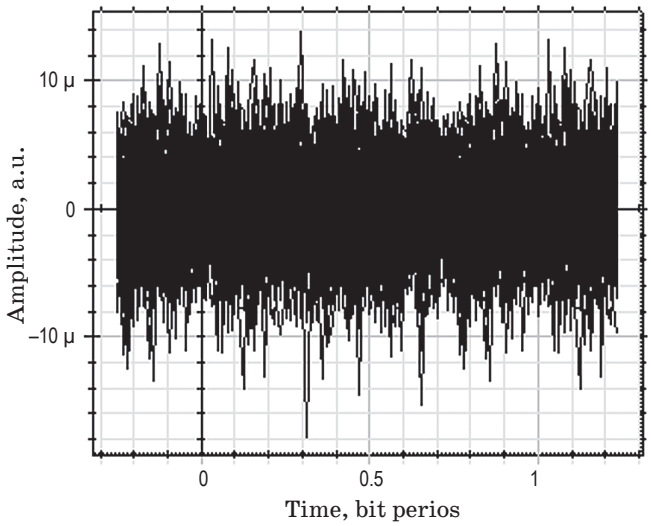

Fig. 6. Eye diagram for an unauthorized user after 400 km.

In traditional schemes the encryption has been done in frequency domain only [9]. If eavesdropper wants to crack the data, he/she has to not only crack the one-time-pad encryption but also need to know details of the exact swapping scheme. It means, if one-time-padding is used to further enhance the security, the proposed scheme enables the user to preserve confidentiality even if the eavesdropper has access to the key required to recover the original data.

This case is presented with two users only, further data from greater number of users can be encrypted with same swapping scheme. Same structure of transmitter can be used and the data blocks of users can make with predefined control signal and then these data blocks can be combined to make swapped signals. The number of swapped signals will be equal to the number of users which can be further transmitted over the fiber. At the receiver side de-swapping and then combining will be done to recover the original data. The number of users will be limited depend upon the control signal length. Multiple bits swapping is recommended for the better performance because single bit swapping will degrade the performance if delay will be induced. So, efficient synchronization between transmitter and receiver is recommended. The order/pattern of swapping is depending on the shape of the control signal. It is clear that same control signal should be used at receiver side to recover the original data. To add the further layer of security all the swapped signals can be further encrypted with one-time padding techniques using all-optical gating.

Also, to make the swapping scheme more secure a random sequence signal (representing fake data) can be used to do swapping with the original data. This scheme is also useful for avoiding the correlation of original data with the mixed sequence.

5. CONCLUSION

We have described a novel technique that enhances security by mixing the data of different users. The observed eye diagrams show good level of eye opening with acceptable BERs less than 10^{-9} for the two data channels. An advantage of this approach is that if one-time-padding is used to further enhance the security then only one arm of the proposed two user setup would require encryption.

Author thanks University Grants Commission of India for awarding a Raman Fellowship that enabled him to work at the Institute of Optics of University of Rochester, USA. Author also would like to thank Prof. Govind P. Agrawal, Professor, the Institute of Optics, University of Rochester, NY, USA for valuable discussions and necessary support.

REFERENCES

1. *Kotb A., Zoiros K.E., Guo C.* Ultrafast performance of all-optical AND and OR logic operations at 160 Gb/s using photonic crystal semiconductor optical amplifier // OLT. 2019. V. 119. P. 105611.
2. *Kotb A., Guo C.* Theoretical demonstration of 250 Gb/s ultrafast all-optical memory using Mach–Zehnder interferometers with quantum-dot semiconductor optical amplifiers // IEEE JSTQE. 2019. V. 27. № 2. P. 1–7.
3. *Nair N., Kaur S., Goyal R.* All-optical integrated parity generator and checker using an soa-based optical tree architecture // COP. 2018. V. 2. № 5. P. 400–406.
4. *Kostinski N., Kravtsov K., Prucnal P.R.* Demonstration of an all-optical OCDMA encryption and decryption system with variable two-code keying // IEEE PTL. 2008. V. 20. № 24. P. 2045–2047.
5. *Chang W.H., Yang G.C., Chang C.Y., Kwong W.C.* Enhancing optical-CDMA confidentiality with multicode-keying encryption // JLT. 2015. V. 33. № 9. P. 1708–1718.
6. *Kaur N., Goyal R., Rani M.* A review on spectral amplitude coding optical code division-multiple access // JOC. 2016. V. 38. № 1. P. 77–85.
7. *Huang H., Lehmann K.* Noise caused by a finite extinction ratio of the light modulator in CW cavity ring-down spectroscopy // APB. 2009. V. 94. P. 355–366.
8. *Rani M., Bhatti H.S., Singh V.* Exact solitary wave solution for higher order nonlinear Schrodinger equation using he's variational iteration method // OE. 2017. V. 56. № 11. P. 116103.
9. *Lin J.S., Yang G.C., Chang C.Y., Kwong W.C.* Study of multicode-keying incoherent optical CDMA without the conventional symbol-synchronous assumption // JLT. 2015. V. 34. № 16. P. 3663–3674.