Four Code Keying in OCDMA

Prabhjot Kaur* and Dr. Baljeet Kaur**
*Student
pmeet1515@gmail.com
**Assistant Professor
baljeetkaur@gndec.ac.in

Abstract: Optical code division multiple access (OCDMA) is a technology in which unique code is assigned to every user which provide it the unique characteristics of high security and make the OCDMA system more reliable. In order to enhance the security, coding is done. Here four code keying is demonstrated which is the type of multicode keying . This technique supports very high bit rate.

Keywords: Optical Code Division Multiple Access(O-CDMA), optisystem, four code keying , two code keying, encryption, confidentiality.

Introduction

After CDMA , these days OCDMA is the most promising and most talked about topic because of its tremendous asynchronous nature, highly secure communication, more reliable structure, and coded nature[1,3].To enhance the physical security one time pad encryption is added on the top of the two code keying and for further enhancement it is extended to four code keying. In this paper all optical CDMA with two code and four code keying using optisystem is implemented.

Multicode Keying Encryption

Four code keying and two code keying are the special cases of multicode keying. Multicode keying is multi-bit per symbol modulation scheme. In one time pad encryption XOR gate operation is performed between one binary key and one data bit, then the encrypted data bit of 1 and 0 is called ciphertext, is generated. In this encryption modulo addition is done by applying galois field( ).

When m=3, every three serial data bits (000, 001, 010, 011, 100, 101, 111) are mapped to eight symbols (0, 1, 2, 3, 4, 5, 6, 7). Similarly encryption keys are coded[5]. With the modulo addition through galois field( ) table encryption symbols are converted to binary form . The formula used is = XOR for i= 0, 1, 2.

Four code keying is applicable to modulo addition in GF [4,5].

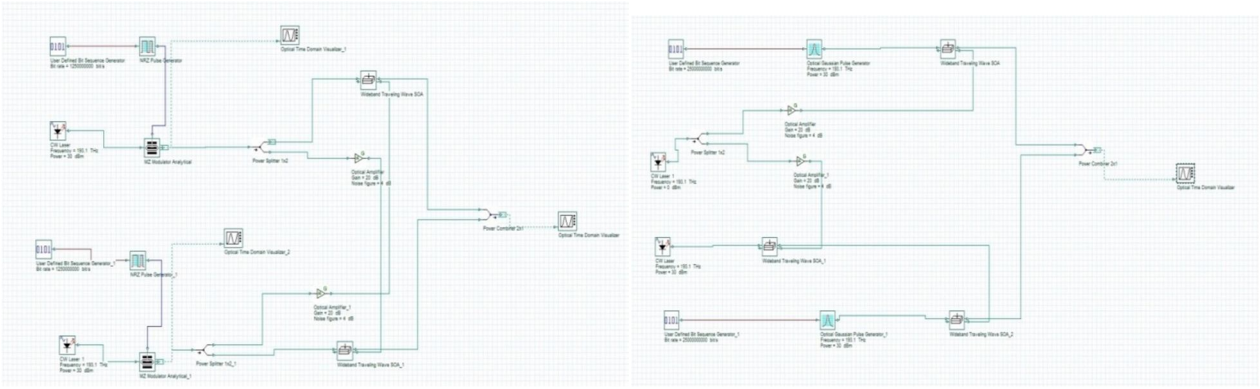
All Optical Implementation

Firstly the XOR gate is designed and is demonstrated at 10 Gb/s . Also codeword multiplexer (CMUX) is also implemented.CMUX is used because when NRZ format is used it can provide large enough (time) window to switch the codewords. So after designing two basic modules :

i) All optical XOR gate simulation
ii) All optical CMUX simulation

Two code keying and four code keying are simulated in optisystem software.

Principle: Basically is forward injected and is backward injected. The SOA's gain will get saturated by which is an optical pulse present at the top of SOA. It will prevent from passing through SOA. It results into and bottom Soa will give . By the power combiner 2*1 results are combined and XOR operation + is performed. While designing CMUX optically, At the top (backward injected) will saturate SOA's gain and it will prevent forward injected optical codeword from passing on to SOA. Similarly the backward injected pulse will behave the same . Similarly, the bottom SOA allows optical codeword +1 to pass only if = 0 (i.e., = 1). The middle SOA acts like an optical inverter. Combining both outputs at the 2 × 1 passive combiner, the all-optical 2 × 1 CMUX operation, is obtained as the output.



(a) (b)

Fig 3.1(a) All optical XOR simulation setup, (b) All optical 2*1CMUX simulation setup

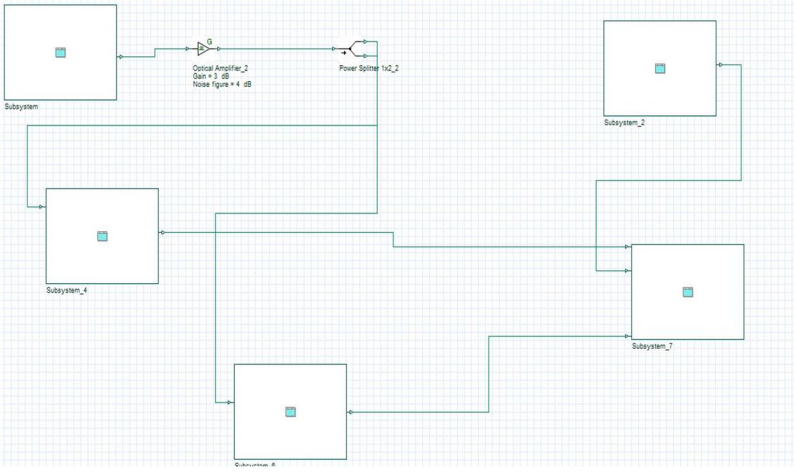
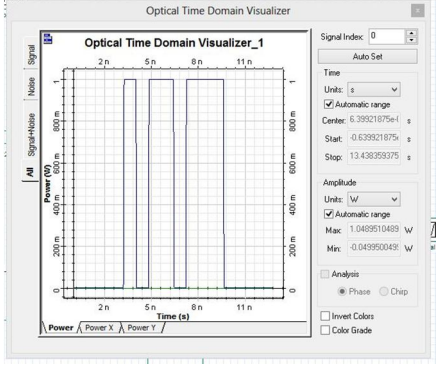
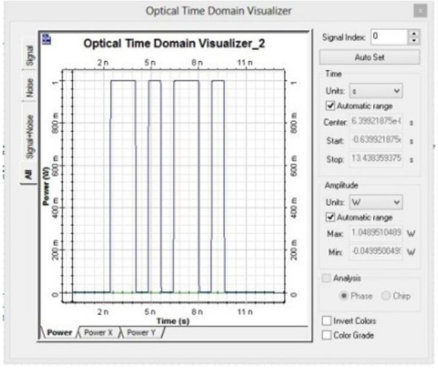


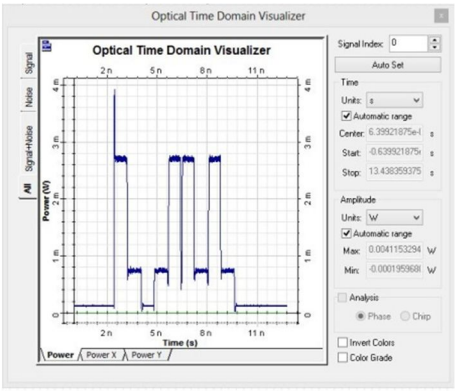
Fig 3.2 Four code keying simulation setup

Simulation Results





(a) (b)



(c)

Fig 4.1 All optical XOR gate simulation results at 1.25 Gbits/s (a)data bits Do=0101101110; (b)encryption keys Ko=1101011010; (c)cipher bits Eo=1000110100, all in optical NRZ format

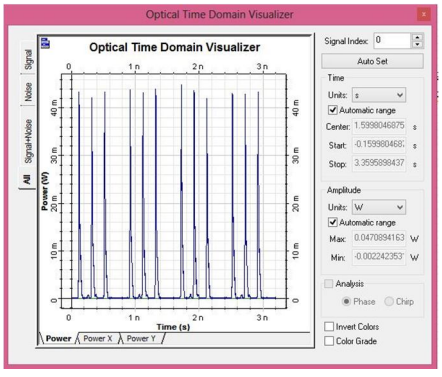
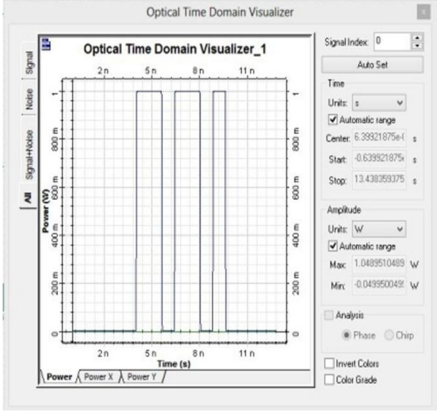
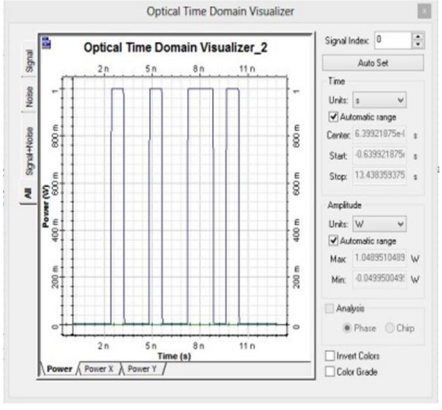


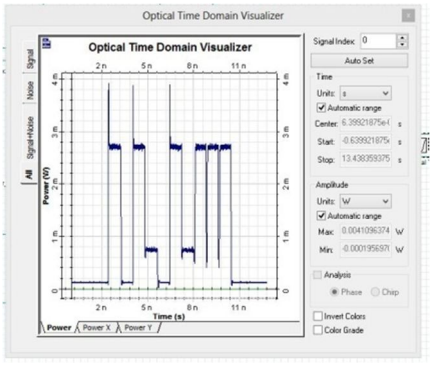
Fig 4.2 All optical two code keying encryption simulation results , With E0=1000110100, the selected optical codewords at the output of the all optical 2*1 CMUX are C1C0C0C0C1C1C0C1C0C0



(a)



(b)



(c)

Fig 4.3 XOR gate simulation results at 1.25 Gbits/s; (a)data bits D1=0011011010 (b)encryption keys K1=1001001101 (c)encrypted bits E1=101001011, all in the optical NRZ format

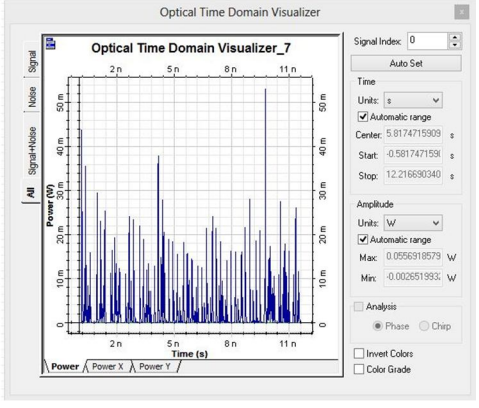


Fig 4.4 Four code keying encryption results

The simulation set-up of four-code- keying encryption, according to Fig 3.2.. In addition to the two codewords C0 and C1, data bits D0, and encryption keys K0 used in the 2-code-keying encryption simulation in 3.1(a) and 3.1(b) , two codewords C2 = 10001000100000000000 and C3 = 10000010000010000000, data bits D1 = 0011011010, and K1 = 1001001101 are applied in this four-code-keying encryption demonstration. The XOR1 module comes from the set- up in above Fig 3.1 (a), generating E0 = D0 ⊕K0 = 1000110100. The CMUX1 module comes from the set-up in 3.1(b) for selecting C0 and C1 in accordance to E0. The CMUX2 module is then modified from CMUX 1 with the two codewords being set to C2 and C3. Similarly CMUX 3 with the power-splitter input connected to the XOR2 output, the top SOA connected to the CMUX1 output, and the bottom SOA connected to the CMUX2 output. In the configuration, the associated"data"and"key"symbols become D1D0 = 0123123130 and K1K0 = 3103013212, respectively. These combinations of D1D0 and K1K0 generate the cipher symbols E1E0 = 3020130322 in accordance with the galois field(2^m) As a result, the CMUX3 output gives the sequence of codewords C3C0C2C0C1 C3C0C3C2C2[6].

Conclusion

In this paper, the use of optical codes for enhancing the physical-layer confidentiality in O-CDMA systems and networks by means of the four code keying encryption is studied. The operating principle of the proposed technique is introduced and the associated all-optical hardware is designed. The all-optical hardware design and the operations of two- and four-code-keying encryption were successfully validated by the proof- of-principle OptiSystemTM simulation.

References

[1] E. Narimanov, W.C. Kwong, G.-C. Yang, and P. R. Prucnal, 'Shifted carrier-hopping prime codes for multicode keying in wavelength-time OCDMA,' IEEE Trans. Commun., vol. 53, no. 12, pp. 2150–2156, Dec. 2005.

[2] C.-Y. Chang, G.-C.Yang, andW. C.Kwong, 'Wavelength-time codeswith maximum cross-correlation function of two for multicode-keying optical CDMA,' J. Lightw. Technol., vol. 24, no. 3, pp. 1093–1100, Mar. 2006.

[3] C. Yang, R. P. Scott, D. J. Geisler, N. K. Fontaine, J. P. Heritage, and S. J B. Yoo, 'Four-state data encoding for enhanced security against upstream eavesdropping in SPECTS O-CDMA,' J. Lightw. Technol., vol. 29, no. 1, pp. 62–68, Jan. 1, 2011.

[4] T. H. Shake, 'Security performance of optical CDMA against eavesdropping,' J. Lightw. Technol., vol. 23, no. 2, pp. 655–670, Feb. 2005

[5] N. Kostinski, K. Kravtsov, and P. R. Prucnal, 'Demonstration of an all optical OCDMA encryption and decryption system with variable two- code keying,' IEEE Photon. Technol. Lett., vol. 2, no. 24, pp. 2045–2047, Dec. 2008.

[6] Wen-Hao Chang, Guu-Chang, fellow, IEEE, Cheng-Yuan Chang, Member, IEEE and Wing C. Kwong, Senior member, IEEE: Enhancing Optical CDMA confidentiality with Multicode Keying Encryption; Journal Of Lightwave Technology , Vol 33,No.9 MAY 2015.