ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

# Security Enhancement of Optical Code Division Multiple Access System Using Multicode-Keying Encryption

Reshma A T[1], Vipin V R[2]

PG Student [OEC], Dept. of ECE, TKM Institute of Technology, Kollam, Kerala, India[1]

Assistant Professor, Dept. of ECE, TKM Institute of Technology, Kollam, Kerala, India[2]

**ABSTRACT:** This paper demonstrate the design and analysis of Optical Code Division Multiple Access (OCDMA) system by incorporating Multicode-Keying encryption technique. OCDMA has become a well-known technology to implement all-optical communication for transporting multipurpose information. In OCDMA system unique code is assigned to each subscriber, so it is considered to be relatively secure as compared to other optical networks. The advanced study of OCDMA has revealed that it is easy to intercept the data by eavesdroppers. Multicode-Keying is a multiple-bit-per symbol modulation technique, supporting higher bit rate without increasing the speed of photonics and electronics. Optical Codes with large cardinality support Multicode-Keying encryption for enhancing physical layer confidentiality in OCDMA system.

**KEYWORDS**: Confidentiality; Multicode-Keying; One-time-pad encryption; Optical Code Division Multiple Access; OptiSystem

## I. INTRODUCTION

Optical Code Division Multiple Access (OCDMA) has recently generated substantial research topic as a promising technology because of its stunning features like flexibility, reconfigurability, ease of network control and potential for enhanced physical layer security [1], [3].

Due to tremendous increase in the volume of information exchange and strong demands in security and privacy, the issues and degree of physical-layer confidentiality potentially supported by OCDMA have become an interesting research topic. In conventional ON-OFF Keying (OOK) OCDMA, data bits can be easily distinguished by an eavesdropper using a simple energy detector in the uplink side of the user, without the need of decoding the codeword in use.[1] This is because only data bits of 1 are transmitted with the user's one-and-only-one codeword (i.e., presence of energy) in OOK. Thus, two-code-keying, in which every user is assigned two distinct code words: one codeword for transmitting data bits of 1 and another codeword for bits of 0, was proposed. To further enhance the physical layer confidentiality one-time-pad encryption was added on the top of two-code keying.

The goal of this paper is to improve physical layer confidentiality [4] of OCDMA system by "Multicode-Keying Encryption" technique. The enhancement of confidentiality by means of "Multicode-Keying" with one-time-pad encryption is investigated in this paper.

## II. MULTICODE-KEYING ENCRYPTION

OCDMA confidentiality is improved by one-time-pad encryption with two-code-keying [2]. The one-time-pad (or encryption key) of a random sequence of 1 and 0 has the same length and rate as the plaintext (i.e., data bits) and is only used once. Each time , an exclusive-or (XOR) operation [5] is performed between one (binary) key and one data bit, generating an encrypted bit of 1 or 0 (called cipher text). Then the cipher text of 1 is transmitted with one codeword $C_1$ and 0 is transmitted with another codeword $C_0$. The encryption is not breakable as long as the eavesdropper doesn't have the key.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Multicode-Keying is a multiple-bit-per-symbol modulation technique. The main advantage of this technique is it supports higher bit rate without increasing the speed of photonics and electronics. One of the $2^m$ code words is conveyed to represent the transmission of one of the $2^m$ symbols. As a result the effective rate becomes m times the symbol rate. Interestingly, with $2^m$-code-keying, it is found that the encrypted symbols (i.e., code words in transmission) are determined by applying modulo-$2^m$ addition in (finite) Galois field of GF ($2^m$) to the associated data bits and encryption keys. For example, with m = 3, every three serial data bits $D_2\,D_1\,D_0 \in$ {000, 001, 010, 011, 100, 101, 110, 111} are mapped to one of the eight symbols: {0, 1, 2, 3, 4, 5, 6, 7} correspondingly. Similarly, the encryption keys contain the same set of eight symbols, which are equivalently binary coded as $K_2K_1K_0 \in$ {000, 001, 010, 011, 100, 101, 110, 111} respectively.

Table 1: Modulo-$2^m$ addition in GF ($2^m$)

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 |
| 2 | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 |
| 3 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 5 | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 |
| 6 | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 |
| 7 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

The encrypted symbol (or cipher text), also denoted in the binary form as $E_2E_1E_0$ is then computed by the formula $E_i = D_i\ XOR\ K_i$ for i = 0, 1, 2, which is equivalent to the modulo-$2^3$ addition in Table 1. The entries in the table denote the encrypted symbol of $E_2E_1E_0$(equivalent to codeword $C_{E_2\,E_1E_0}$ in transmission) for every pair of data symbol of $D_2\,D_1\,D_0$ and key symbol of $K_2K_1K_0$. The XOR operation in the two-code-keying encryption is equivalent to the modulo-2 addition in GF (2), which belongs to a sub-field of GF ($2^3$), as shown in Table 1. Similarly, the four-code keying encryption applies the modulo-$2^2$ addition in GF ($2^2$), also a subfield of GF ($2^3$).

## III. SYSTEM ARCHITECTURE

Multicode-Keying encryption is done in optical domain with the help of all-optical XOR gate and all-optical Code word Multiplexer (CMUX). Different from other designs, these two all-optical modules are designed to handle optical signals in the NRZ format in order to provide large enough (time) window to switch optical code words in the CMUX. Another advantage of using these two SOA-based modules is that SOAs with carrier recovery time <10 ps (i.e., >500 GHz) have been commercialized.

The polarization-independent all-optical XOR gate is based on the design in [6]. The gate, which was experimentally demonstrated at 10 Gb/s, utilized the gain saturation effect by the cross-gain modulation (XGM) in the SOAs without the need of clock signals or additional input control signals. In principle, a backward injected $K_i$ optical NRZ pulse at the top SOA will saturate the SOA's gain and thus prevent a simultaneously forward injected $D_i$ optical NRZ pulse from passing through the SOA. In other words, the $D_i$ pulse can pass through only if the $K_i$ pulse is absent. This results in $D_i\overline{K_i}$ at the output of the top SOA. Similarly, the bottom SOA gives $\overline{D_i}K_i$ . Combining both outputs at the 2 × 1 passive combiner, the all-optical XOR operation $D_i\overline{K_i} + \overline{D_i}K_i$ results.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

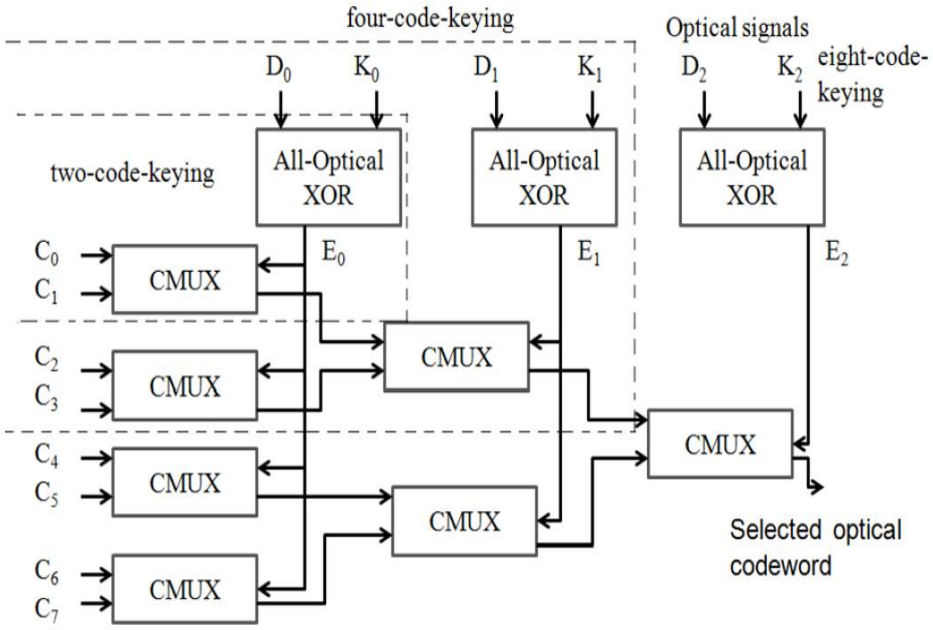


Fig. 1 All-optical design for Multicode-Keying Technique

Our polarization-independent all-optical CMUX is designed to function like a 2 × 1 codeword selector by means of the XGM in the SOAs. The NRZ encrypted symbol $E_i$ from the all-optical XOR gate is sent into the back input of the top SOA as shown in Fig.1. In principle, a backward injected $E_i$ pulse at the top SOA will saturate the SOA's gain and thus prevent a simultaneously forward injected optical codeword $C_j$ from passing through the SOA. In other words, $C_j$ can pass through only if $E_i = 0$. The middle SOA is configured to function as an optical inverter. Inducing the XGM, the backward injected $E_i$ pulse saturates the SOA's gain and prevents a forward injected CW laser beam from passing through the SOA, thus giving $E_i$ as the output. Similarly, the bottom SOA allows optical codeword $C_{j+1}$ to pass only if $E_i = 0$ (i.e., $E_i = 1$). Combining both outputs at the 2 × 1 passive combiner, the all-optical 2 × 1 CMUX operation, $C_i\overline{E_i} + C_{j+1}E_i$, is obtained as the output.

A novel all-optical design of the hardware for Multicode-keying encryption technique is shown in Fig.1. Both data symbols and encryption keys are now in the optical form. Multicode-keying encryption is used to represent $2^m$ code words with m serial data bits per symbol. The block diagram shown above is used to represent $2^3$ code words with m = 3.

## IV. SIMULATION MODELING

The simulation setup of proposed Multicode-Keying Encryption technique modelled using OptiSystem Version 12 simulation software is shown in the Fig.2. The block diagram shown above is the design of eight-code keying encryption technique. Eight-code Keying consist of three all-optical XOR gate, seven all-optical CMUX. The XOR 1 output $E_0$ is amplified by an Optical amplifier (OA). Then it is split into four by a 1 × 4 Power Splitter. Thus encrypted data $E_0$ from XOR 1 act an input of CMUX 1, CMUX 2, CMUX 3 and CMUX4. The selected code words coming from these CMUXs given to CMUX 5 and CMUX 6.The encrypted data $E_1$ is given from XOR 2 to CMUX 5 and CMUX 6. The outputs from CMUX 5 and CMUX 6, encrypted data $E_2$ from XOR 3 are act as the input of CMUX 7.As the name suggest it uses eight code words to represent eight data symbols. The code words, data bits and keys are given in Table 2.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Table 2: Code words in Subsystems

| | |
|---|---|
| $C_0$ | 1001001000000000000 |
| $C_1$ | 1000010000100000000 |
| $C_2$ | 1000100010000000000 |
| $C_3$ | 1000001000001000000 |
| $C_4$ | 1000010000100000000 |
| $C_5$ | 1000000100000100000 |
| $C_6$ | 1000001000001000000 |
| $C_7$ | 1000000010000000100 |

The data bits and Keys in the XORs are given in Table 3. The code words are selected according to the Cipher bits coming from XOR 1, XOR 2 and XOR 3.

Table 3: Data bits And Keys

| | |
|---|---|
| XOR 1 | $D_0$=1110000000<br>$K_0$=0100110110 |
| XOR 2 | $D_1$=1111001010<br>$K_1$=0101110000 |
| XOR 3 | $D_2$=0110001000<br>$K_2$=1100111110 |

According to the data bits and keys in Table 3, the cipher bits obtained by the XOR operation are $E_0$ = 1010110110; $E_1$ = 1010111010; $E_2$ = 1010110110. These cipher bits are acting as the input of CMUXs as shown in Fig. 2.

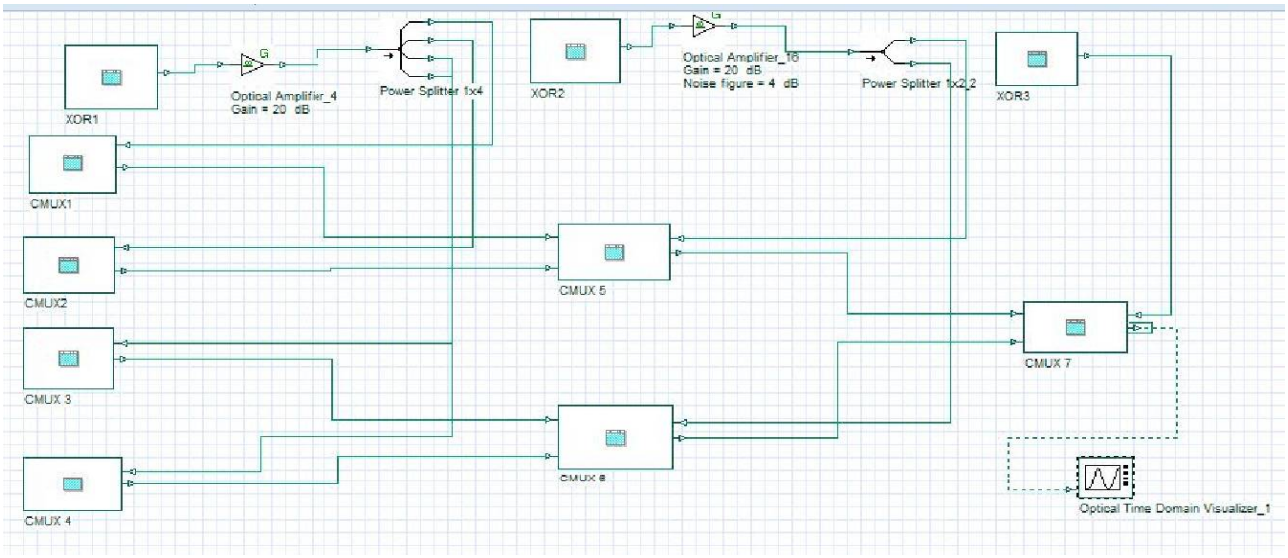


Fig. 2 All-Optical Eight-code Keying simulation setup

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

## V. RESULTS AND DISCUSSIONS

The results obtained from Optical Time Domain Visualizer of OptiSystem version 12 is shown in the Fig.3. Eight code words are applied in this encryption technique. The code words used are $C_0C_1C_2C_3C_4C_5C_6C_7$. The CMUX 7 gives the sequence of code words $C_7C_0C_7C_7C_2C_5C_7C_0$. So due to the increased number of code words, eavesdropper find difficulty to figure out the data symbols from these code words.

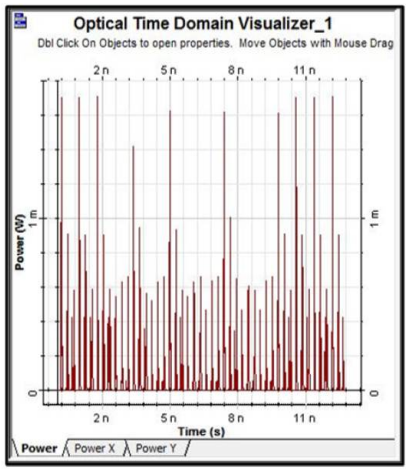


Fig. 3 All-optical Eight-code Keying Encryption

## VI. CONCLUSION

In this paper the confidentiality improvement of OCDMA system with "Multicode-Keying Encryption" technique is analyzed. The cipher bits obtained from the All-optical XOR Gate is mapped to $2^m$ code words. So even though code words are not hidden, the eavesdropper's find difficulty in figuring out how the code words are mapped to the data symbols. Also optical encryption by using all-optical XOR gate has low latency and immune to electromagnetic interference. The all-optical design is scalable and integrable, and able to handle both data bits and encryption keys in the optical and non-return-to-zero (NRZ) format.

## 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. J. H. Kim, Y. M. Jhon, Y. T. Byun, S. Lee, D. H. Woo, and S. H. Kim, 'All-optical XOR gate using semiconductor optical amplifiers without additional input beam,' IEEE Photon. Technol. Lett., vol. 14, no. 10, pp. 1436–1438, Oct. 2002.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

## BIOGRAPHY

**Reshma A T** received her B.Tech degree in Electrical and Electronics Engineering from University of Kerala in 2014. She is currently pursuing second year M.Tech in Optoelectronics and Communication Systems at TKM Institute of Technology.

**Vipin V R** received his B.E degree in Electronics and Communication Engineering in 2008 and M.E in Communication Systems in 2013 from Anna University. He is currently working as Assistant Professor in the Department of Electronics and Communication Engineering at TKM Institute of Technology.