Optical code division multiple access secure communications systems with rapid reconfigurable polarization shift key user code

Kaiqiang Gao
Chongqing Wu
Xinzhi Sheng
Chao Shang
Lanlan Liu
Jian Wang
Optical code division multiple access secure communications systems with rapid reconfigurable polarization shift key user code

Kaiqiang Gao,a Chongqing Wu,a,Xinzi Sheng,a Chao Shang,b Lanlan Liu,a and Jian Wanga
aBeijing Jiaotong University, Key Lab of Education Ministry on Luminescence and Optical Information Technology, Institute of Optical Information, Beijing 100044, China
bBeijing University of Posts and Telecommunications, State Key Laboratory of Information Photonics and Optical Communication, School of Electronic Engineering, Beijing 100876, China

Abstract. An optical code division multiple access (OCDMA) secure communications system scheme with rapid reconfigurable polarization shift key (Pol-SK) bipolar user code is proposed and demonstrated. Compared to fix code OCDMA, by constantly changing the user code, the performance of anti-eavesdropping is greatly improved. The Pol-SK OCDMA experiment with a 10 Gchip/s user code and a 1.25 Gb/s user data of payload has been realized, which means this scheme has better tolerance and could be easily realized.© The Authors. Published by SPIE under a Creative Commons Attribution 3.0 Unported License. Distribution or reproduction of this work in whole or in part requires full attribution of the original publication, including its DOI. [DOI: 10.1117/1.OE.54.9.096101]

Keywords: optical code division multiple access; polarization shift key code; secure communications system; bipolar code.

Paper 150333 received Mar. 17, 2015; accepted for publication Jul. 21, 2015; published online Sep. 1, 2015.

1 Introduction

With rampant eavesdropping technology, the security of optical fiber communication has become a serious problem that must be contemplated. It has been demonstrated that secure optical communications based on data encryption algorithm are usually cracked, and the physical method for anti-eavesdropping is reliable. By now, there are three main physical approaches: quantum encryption key distribution technology,1 secure chaotic communications,2 and optical code division multiple access (OCDMA). Due to the physical mechanism limitations, quantum communication is only suitable for low-speed signal transmission,3,4 and the single photon source and quantum receiver are quite expensive. Chaotic communication has been studied for many years, but there are more difficulties in practical applications.5 OCDMA based on conventional technologies is often said to be inherent security and has received extensive attention.6

Among the approaches of OCDMA, the core technique is how to apply a physical quantity to express the user code. In 2004, McGeehan et al. demonstrated a time wavelength polarization coding using the fiber delay line.7 Since 2006, Kitayama et al. made a lot of advanced progress in OCDMA. In Refs. 8 and 9, a method based on a time-phase code using the hybrid planar lightwave circuit and super structured fiber Bragg grating en/decoders was proposed. In 2010, a two-dimensional time-domain spectral phase encoding/wave length hopping coherent differential phase shift key (DPSK)-OCDMA system using fiber Bragg gratings (FBGs) and a phase modulator was proposed.10 In 2014, they completed the 40G-OCDMA-PON system.11 In 2015, Al-Khafaji et al. proposed a bipolar OCDMA solution,12 binary user data bits are encoded by two alternative spectral-amplitude encoders, which are assigned to distinct time slots representing bit 1 and bit 0, and the performance analysis shows that it has a better tolerance of multiple access interference than unipolar spectral amplitude coding-OCDMA in different transmission rates.

All of the systems above are based on a passive optical path with a fixed structure, such as FBGs or fiber delay lines that causes the limited sets of the user coder. For achieving sufficient orthogonality among the user codes, researchers utilize algorithms to construct optical orthogonal codes (OOCs), which always include a large number of chips in code. To extend the chip accommodation, the works of Refs. 7–12 and 14 utilize time, wavelength, and polarization multiplexing approaches. However, these schemes lead to complicated and redundant system structures. Besides that, OOCs are usually unipolar codes. In case of the same code length, the result of correlation between bipolar codes is much better than that of unipolar codes for multiuser access. Bipolar codes have been used in a phase shift encoder and decoder15–17 based on phase modulator or FBG, but coherent detection is not easy for a reconfigurable decoder. In Ref. 15, a DPSK demodulator is needed, and the cost and complexity of the system is much higher. Furthermore, Shake14 indicated that “A source cryptography provides a much greater degree of confidentiality than does time-spreading/wavelength-hopping O-CDMA encoding” and “Rapid reconfiguration of codes can also increase the difficulty of interception.” Therefore, a bipolar OCDMA scheme with reconfigurable user code has significant meaning.

In this paper, a novel bipolar OCDMA network is proposed by analyzing the Jones matrix of a polarization shift keying (Pol-SK) modulation. We take advantage of the fact that light can be transmitted on two orthogonal polarization states to encode {p-state, s-state} as chips that indicate a bipolar code {+1, −1} in a CDMA system. We demonstrate a back-to-back Pol-SK OCDMA system, which
generates polarized chips at 10 Gbps and recovers 1.25 Gbps original datum from this Pol-SK optical signal. This bipolar code could be rapidly reconfigured and has the advantages of enlarging the capacity of a code set and being easily judged.

This paper is structured as follows. Section 2 describes the principle of generating bipolar multiplication with ±1. A true-table of bipolar multipliers is shown in Table 2.

As a continuous wave (CW) linear light is encoded by a polarization modulator, a special SOP sequence can be obtained. This is the principle of generating the Pol-SK OCDMA code.

In order to describe the behaviors of the Pol-SK OCDMA system, we use the vector as a user code for the payload data. A special user code could be expressed as follows:

\[ \mathbf{C}_{\text{user}} = \{ c_1, c_2, \ldots, c_n \}, \quad (1) \]

where \( n \) is the code length; \( c_i = \pm 1, (i = 1, 2, \ldots, n) \). Thus, the payload data of the user could be expressed as

\[ \mathbf{D}_{\text{payload}} = [d_1, d_2, \ldots, d_m], \quad (2) \]

where \( m \) is the sequence length; \( d_i = \pm 1, (i = 1, 2, \ldots, m) \). Modulating the repeated OCDMA code sequence by the user data, the spreading spectrum matrix can be written as

\[ \mathbf{S}_{\text{m,dom}} = \text{diag}[d_1 \mathbf{C}_{\text{user}}, d_2 \mathbf{C}_{\text{user}}, \ldots, d_m \mathbf{C}_{\text{user}}]. \quad (3) \]

In the correlator of the receiver, its property can be described by the matrix as follows:

\[ \mathbf{M}_{\text{m,dom}} = \text{diag}[\mathbf{C}_r, \mathbf{C}_r, \ldots, \mathbf{C}_r]. \quad (4) \]

The result of correlation is

\[ \mathbf{S}_{\text{m,dom}} = \mathbf{M}_{\text{m,dom}} \mathbf{S}_{\text{m,dom}}^\text{in} = \text{diag}[d_1 \mathbf{C}_r \cdot \mathbf{C}_{\text{user}}, d_2 \mathbf{C}_r \cdot \mathbf{C}_{\text{user}}, \ldots, d_m \mathbf{C}_r \cdot \mathbf{C}_{\text{user}}]. \quad (5) \]
After the integrator, the recovery data are
\[ D_{\text{recovery}} = (C_r \cdot C_{\text{user}})[d_1, d_2, \ldots, d_m]. \] (6)

We define the correlation coefficient as follows:
\[ R = (C_r \cdot C_{\text{user}}). \] (7)

Because \( c_i = \pm 1, (i = 1, 2, \ldots, n) \), the weight \( K \) is equal to \( n \) in any case of the user code.
\[ K = (C_{\text{user}} \cdot C_{\text{user}}) = \sum_{i=1}^{n} c_i^2 = n. \] (8)

The cross-correlation coefficient is
\[ X_r = (C_r \cdot C_{\text{user}}) = \sum_{i=1}^{n} c_{ri}c_i. \] (9)

From Eq. (9), the maximum cross-correlation coefficient is no more than \((n - 2)\), and the difference between the weight and the cross-correlation coefficient depends on the number of distinct chips in \( C_r \) and \( C_{\text{user}} \). By updating the user code, the number of changed chips is \( q \), and the cross-correlation coefficient \( X_r \) becomes \((n - 2q)\), which means it is easier to make the threshold decision invalid, this could result in enhanced security in a reconfigurable OCDMA system.

### 3 Experiments of Polarization Shift Key Optical Code Division Multiple Access System

#### 3.1 Experimental Setup

For demonstrating the theory above, the experimental setup of the Pol-SK OCDMA system is shown in Fig. 2. We demonstrate data transmission for only a single user. In the transmitter, the CW light source is IDPhotonics Tunable Laser at 1567.1 nm with a 100-kHz band width and 10-dBm output power providing continuous and stabilized SOPs. Polarization controllers are deployed to adjust the incident light to be a linearly polarized beam, whose direction is 45 deg azimuth with the polarization axis of the lithium niobate (LN) phase modulator (PM). PC1 regulates the input SOP to the \( p \)-state. The first LN phase modulator (LN-PM1) is the Pol-SK OCDMA code generator. The input electric signal is bipolar square signal at 10 Gchip/s with \( \sim 7\, V_{pp} \), and the input light is continuous with a linearly stabilized SOP called the \( p \)-state. The output of LN-PM1 is a sequence of SOPs consisting of \( p \)-states and \( s \)-states. When splitting the orthogonal SOPs’ sequence into two independent beams by using a polarization beam splitter (PBS), the pattern of the \( s \)-states’ beam is approximate to the encoding signal and the other one is inverted. The second LN phase modulator (LN-PM2) is the payload modulator with 1.25 Gbit/s (\( 2^{29} - 1 \) pseudo-random bit sequence). When the bipolar payload bit is \(-1\), SOPs are changed again. Otherwise, for a bit equal to \(+1\), the SOPs remain unchanged. These modulators are GETC44 1550 nm \( \text{LiNbO}_3 \) phase modulators with a...
12 GHz band width. A programmable pattern generator (PPG) produces the electronic signal of the user code sequence. In the transmission link, an erbium-doped fiber amplifier is deployed to compensate the optical power attenuation of the modulators and a 5 km fiber. In the receiver, there is another LN phase modulator as the correlator and an electric channel of PPG to produce the local OCDMA code. The PPG is an Anritsu MP1800A Signal Quality Analyzer. In order to synchronize the arriving optical signal and the local code, an adjustable fiber adapter is mounted to tune the optical path. The chip cycle of 10 Gchip/s is 100 ps during which the light wave travels $\sim 2c$ m in the fiber. A fiber cutter with a measurable scale could control the error within 1 mm, which means the fiber delay control has a <5 ps scale. Each user data is detected respectively by using a u2t photonics balanced photodetector for differential detection, as only the local code matches user code. The detected electrical signal is passed through a low pass filter (LPF) instead of the integrator and is received by a LeCroy Wave Expert 100H Sampling Oscilloscope for waveform observation.

### 3.2 Experiment of Polarization Rotation

In the experimental system shown in Fig. 2, the code generator, the modulator of the user data, and the correlator are all LN-PM. Figure 3 shows an experiment of polarization rotation in the LN-PM, which demonstrates how to rotate the SOP to a perpendicular state. Because of the limitation of the sampling rate in the polarization analyzer (PA), a bipolar ramp signal with a low repetition rate (1 Hz) is applied. When the LN-PM is used as the code generator, we use a CW laser as the incident light source and deploy a polarization controller to make the arriving light a linear polarized light whose direction is $\pi/4$ azimuth to the polarization axis of LN-PM with a single-mode fiber pigtail. In the LN-PM, light is separated into $E_x$ and $E_y$, two polarized components of the vertical and horizontal directions with the same amplitude and phase. Then a ramp signal $V(t)$ at a 1-Hz output from the EE1641B1 function generator is applied on the LN-PM to change the refractive index in the direction of the $E_x$ component in order to achieve the polarization rotation.

The PA is a General Photonics POD-101D DSP Inline Polarimeter. Data acquired from the PA and the ramp signal that periodically correspond to Stokes vector are shown in Fig. 4. When the $V_{pp}$ of the modulating signal is 7.02 V, the track’s endpoints of the output SOPs, which are labeled as the $p$-state and $s$-state, are orthogonal.

The relationship between the modulation signals and degrees of polarization rotation on the equator of the Poincare sphere is shown in Fig. 5. The rotation angle is equal to $2\theta$ in the Jones matrix $J_{PolM}$. The range of $2\theta$ covers from 0 to $\pi$, which indicates that the LN-PM achieves the orthogonal polarization rotation brilliantly.
3.3 Experiment Results of Back to Back Polarization Shift Key Optical Code Division Multiple System

The waveforms from the tap points of the system are shown in Fig. 6. The s-state signal is detected by a PBS and positive intrinsic and negative photodiode at a tap point in the transmission part. The balance detector signal with many glitches is quite confusing. However, an LPF improves the recovery of the raw pattern of the payload signal. This demonstrates that the output data waveform from the receiver is similar to the one from the transmitter.

Because the waveform of the optical Pol-SK signal could not be observed directly, we measured its spectrum to analyze the signal. The spectrum of the CW laser source and the polarization modulated signals’ output from the code generator are shown in Fig. 7. The Pol-SK signal has more harmonics than on-off key (OOK) (nonreturn to zero or return to zero) code, containing both odd and even harmonics, increasing the frequency hopping and security.

The bit error ratio test is shown in Fig. 8, which means that the 1 to 2 dB improvement could be obtained when employing a bipolar code compared with the unipolar detection. This is because the proposed bipolar scheme takes advantage of differential detection to depress the influence of noise.

4 Conclusion

We have proposed and demonstrated a bipolar OCDMA scheme with a Pol-SK data format by polarization...
modulation. It is proved that the polarized state and the pass-
switch polarization rotation can be described by a bipolar
code. A reconfigurable user code enhances system security.
There are now two methods against eavesdropping attacks:
data encryption and physical encryption. CDMA is a popular
physical encryption method both in optical communication
and wireless communication; the key technology is how to
configure the user code. In traditional OCDMA, the user
code is configured by OOK or by PSK. Because optical
OOK code is always positive, the result of cross-correlations
among user codes is unsatisfactory for threshold decision.
The PSK method utilizing many FBGs is not convenient for
changing codes, and bipolar phase modulation needs cohe-
rent detection, which increases the system cost. Compared to
these OCDMA systems with a fixed code, by frequently
changing the user code, the proposed scheme has a good per-
formance against eavesdropping attacks, which makes it an
attractive candidate for secure communication systems.
In particular, the Pol-SK OCDMA experiment with a
10 Gchip/s user code and a 1.25 Gb/s user data for the pay-
load has been realized, which means it has a better tolerance
and is easy to achieve.

Acknowledgments
This work is supported by the National Natural Science
Foundation of China (61275075), Beijing Natural Science
Foundation (4144080), and BJTU Fundamental Research
Funds (2014RC016).

References
1. H. F. Zhang et al., “A real-time QKD system based on FPGA,” J.
Lightwave Technol. 30(20), 3226–3234 (2012).
2. Q. Zhao, P. Liu, and H. Yin, “Performance improvement of secure cha-
ocit optical communications utilizing symmetrical dispersion compensa-
tion technique,” Proc. SPIE 8309, 83092E (2011).
3. L. Oesterling, D. Hayford, and G. Friend, “Comparison of commercial
and next generation quantum key distribution: technologies for secure
communication of information,” in IEEE Conf. on Technologies for
Homeland Security, pp. 156–161 (2012).
4. K. Harasawa et al., “Quantum encryption communication over a 192-
km 2.5-Gbit/s line with optical transceivers employing Yuen-2000
protocol based on intensity modulation,” J. Lightwave Technol.
29(3), 316–323 (2011).
5. Z. Kang et al., “Multimode synchronization of chaotic semiconductor
ring laser and its potential in chaos communication,” IEEE J. Quantum
Electron. 50(3), 148–157 (2014).
6. N. Kostinski, K. Kravtsov, and P. R. Prucnal, “Demonstration of an all-
optical OCDMA encryption and decryption system with variable two-
code keying,” IEEE Photonics Technol. Lett. 20(24), 2045–2047
(2008).
7. J. E. McGeehan et al., “3D time-wavelength-polarization OCDMA
coding for increasing the number of users in OCDMA LANs,” in
Optical Fiber Communication Conf., Vol. 2, pp. FES5 (2004).
8. X. Wang and N. Wada, “Experimental demonstration of OCDMA traf-
ﬁc over optical packet switching network with hybrid PLC and SSFBG
end/decoders,” J. Lightwave Technol. 24(8), 3012–3020 (2006).
9. K. Kitayama, X. Wang, and N. Wada, “Experimental demonstration of
2 x 10 Gb/s OCDMA system using cascaded long-period fiber gra-
tings formed in dispersion compensating fiber,” J. Lightwave Technol.
24(4), 1654–1662 (2006).
10. Z. Gao et al., “2D time domain spectral phase encoding/wavelength
hopping coherent DPSK-OCDMA system using fiber Bragg gratings
and phase modulator,” in Communications and Photonics Conf. and
Exhibition, pp. 439–440 (2010).
11. Z. Gao et al., “Time domain spectral phase encoding DPSK data modu-
lation using single phase modulator for OCDMA application,” in
Conference on Lasers and Electro-Optics (CLEO) and Quantum
Electronics and Laser Science Conf., pp. 1–2 (2010).
12. R. Matsumoto et al., “40G-OCDMA-POD system with an asymmetric
structure using a single multi-port and sampled SSFBG encoder/decoders,” J. Lightwave Technol. 32(6), 1132–1143 (2014).
13. H. M. R. Al-Khafaji et al., “A new two-code keying scheme for SAC-
OCDMA systems enabling bipolar encoding,” J. Mod. Opt. 62(5),
327–335 (2014).
14. T. H. Shake, “Security performance of optical CDMA against eaves-
dropping,” J. Lightwave Technol. 23(2), 655–670 (2005).
15. Z. Gao et al., “Rapid reconfigurable OCDMA system using single-
phase modulator for time-domain spectral phase encoding/decoding
and DPSK data modulation,” J. Lightwave Technol. 29(3), 348–354
(2011).
16. S. Kim, K. Yu, and N. Park, “A new family of space/wavelength/time
spread three-dimensional optical code for OCDMA networks,” J.
Lightwave Technol. 18(4), 502–511 (2000).
17. I. F. A. Faiﬂes et al., “Spectral phase en/decoders for OCDMA access
network,” in Advanced Photonics & Renewable Energy, 21–24 June
2010, Karlsruhe, Germany, paper BThB3, Optical Society of America, Washington, D.C.