26th Optoelectronics and Communications Conference (OECC)
2021 © OSA 2021

Secure Optical Communication based on Orthogonal DQPSK/CSK Modulation and Symbol Overlapped Random Optical Phase Encryption

Zhensen Gao[1]*, Qiongqiong Wu[1], Songnian Fu[1], Xu Wang[2], Yuncai Wang[1] and Yuwen Qin[1]
[1]*Guangdong Provincial Key Laboratory of Photonics Information Technology, Guangdong University of Technology, Guangzhou 510006, China*
[2]*School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK*
**Corresponding author: gaozhensen@gdut.edu.cn*

Abstract: We propose a novel physical layer secure optical communication scheme utilizing symbol overlapped random optical phase encryption to secretly transmit two private messages with orthogonal DQPSK/CSK modulation. A 3-bit/symbol 30Gb/s secure optical system is demonstrated. © 2021 The Author(s)

1. Introduction

Nowadays, achieving physical layer security is becoming increasingly important and has received much attention to complement with the software encryption [1]. Quantum communication and chaotic optical communication are two prominent techniques for physical layer secure communication, but great efforts towards high capacity transmission and relaxing requirement on the optical components are still to be expected [2, 3]. Optical encryption is another promising solution for physical layer secure optical communication [4], thanks to its striking advantages of fully compatibility with commercial fiber-optic components and high processing speed. However, the capacity and security of optical encryption system are greatly related to the optical modulation formats and encryption techniques. Previous demonstrated optical encryption systems usually employ simple on-off-keying (OOK) or differential-phase-shift-keying (DSPK) modulation to transmit a single private message in the whole optical channel [5, 6], and the optical encryption code pattern is generally not flexible [7], which not only limits the transmission capacity within 10Gb/s but also reveals security vulnerability [8]. It is therefore quite essential to develop advanced optical modulation and encryption techniques to efficiently use the limited transmission resources and enhance the security of optical system.

In this work, we propose, for the first time, a secure optical communication scheme supporting orthogonal differential-quadrature-phase-shifting-keying (DQPSK) and code-shifting-keying (CSK) modulation to secretly transmit two private messages simultaneously based on symbol overlapped random optical phase encryption. The proposed scheme presents a novel way to enhance transmission capacity and security of optical encryption system.

2. Operating principle

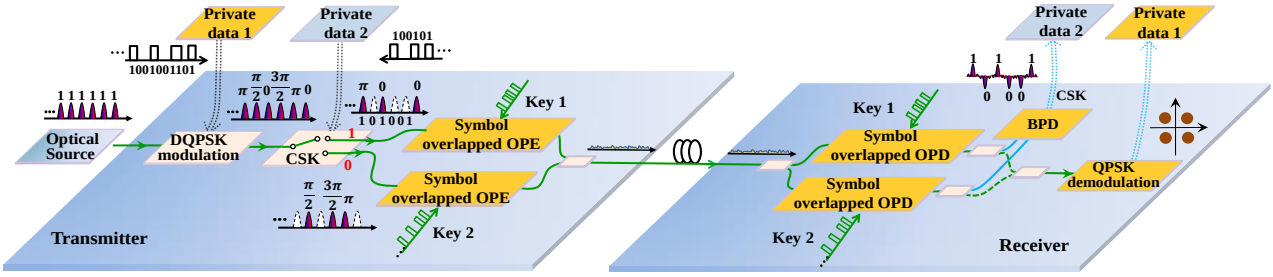

Fig.1 Principle of the proposed secure optical communication scheme.

Figure 1 illustrates the proposed secure optical communication scheme based on orthogonal DQPSK/CSK modulation format and symbol overlapped optical phase encryption. At the transmitter side, the ultra-short optical pulse trains generated by an optical source is firstly modulated into DQPSK format by private data 1. After that, the DQPSK modulated optical pulses are switched into two branches by an optical switch which is driven by private data 2 for CSK modulation. A portion of the original DQPSK pulses will be directed into the upper branch if the private data 2 is binary 1, otherwise, the rest of the pulses will be directed into the lower branch. Hence, the two individual private data sequences are modulated onto one optical pulse at 3-bit/symbol. The switched optical pulses at each optical branch are then injected into an optical phase encryption (OPE) module, which consists of a

pair of dispersive components and a phase modulator between them. The dispersive components are utilized to significantly stretch and compress the optical pulses to introduce symbol overlapping for symbol-by-symbol optical phase encryption by random key streams (key 1 for upper branch or key 2 for lower branch in Fig. 1). Different DQPSK pulse will be phase encrypted by different portion of the pattern streams and exhibits as a noise-like waveform. The encrypted noise-like signals from the two branches are then combined by an optical coupler (OC) to generate optical phase encrypted orthogonal DQPSK/CSK noise-like signal for secure transmission. At the legal user's receiver end, the encrypted signal is firstly split into two parts and directed into two separate optical phase decryption (OPD) modules respectively. The OPD module has similar configuration to the OPE except that the inverse code pattern streams are employed to drive the phase modulator to perform optical phase decryption. After the OPD, the orthogonal DQPSK and CSK modulated optical pulses will be regenerated from the noise-like encrypted signal. The private data 1 can be further extracted by combining the decrypted signals from the two branches and then performing DQPSK demodulation. As for the CSK modulation, balanced photo-detection (BPD) between the upper and lower branch decrypted signals can be adopted to recover the private data 2. In the proposed scheme, the two orthogonal DQPSK and CSK data can be simultaneously encrypted and securely transmitted. An eavesdropper without knowing the correct values of D_1, D_2 and the key streams, which contribute to the key space together, will unable to extract the orthogonal private data, so that the security of the system can be guaranteed.

3. System configuration and results

Figure 2 shows the detailed system configuration for investigation of the secure communication performance based on commercial VPI photonics simulation platform. A mode-locked laser diode is used to generate ultra-short optical pulses with ~2ps pulse width and a repetition rate of 10GHz. The generated pulse train is injected into an IQ optical modulator to perform DQPSK modulation with a bit rate of 20Gb/s. Then, CSK modulation with a private data rate of 10Gb/s is realized by employing a Mach-Zehnder modulator based 10GHz optical switch. For the generation of OPE/OPD at each branch, a pair of chirped fiber Bragg grating with opposite dispersion ($-D_1$, $+D_1$ and $-D_2$, $+D_2$) is utilized for pulse stretching and compression. A 40GHz phase modulator driven by different pseudorandom binary sequences (PRBS) with bit rate of R_1 and R_2 is placed between the dispersive elements to perform symbol overlapped optical phase encryption. The encrypted orthogonal DQPSK/CSK signals from the two branches are combined and securely transmitted to the receiver side. The OPD modules individually driven by the inverse PRBS for each branch are then used to perform optical phase decryption, followed by CSK private data detection with a 40GHz BPD and DQPSK demodulation using a delay-line based 10GHz DQPSK optical demodulator.

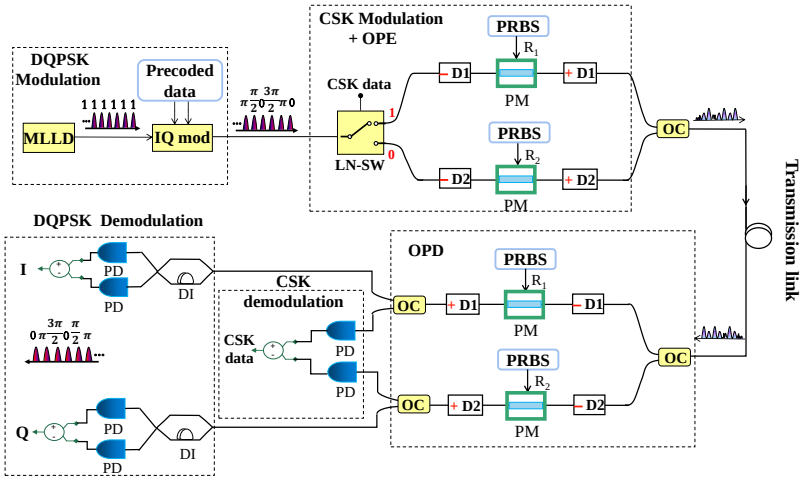

Fig.2 System configuration of the orthogonal DQPSK/CSK secure optical communication scheme.

With the abovementioned system configuration, the encryption performance is shown in Figs. 3(a)~(f) when R_1=10Gb/s, R_2=20Gb/s, D_1=1500ps/nm, D_2=800ps/nm for OPE/OPD. Compared with the original 10Gbaud/s DQPSK data modulated optical pulses after the optical switch in Fig. 3 (a)~(b), it is obvious that the waveforms of encrypted signal in Fig. 3 (c)~(d) for the two branches are completely different from the original signal. Each short optical pulse is temporally expanded and encrypted by the OPE modules in the upper or lower branch determined by the orthogonal CSK private data due to the symbol overlapped random optical phase encryption. After combining the encrypted DQPSK/CSK signal from the branches, the waveform and corresponding eye diagram exhibit as

noise-like signals, as shown in Fig.3 (e)~(f). It is extremely difficult for an eavesdropper to extract the orthogonal DQPSK/CSK private data without knowing the exact key parameters, let alone using simple power detection or DQPSK demodulation to attack. Fig.3 (g) and (h) show that the eye diagram for CSK data and constellation diagram for DQPSK data are fully closed when an eavesdropper randomly selects an incorrect key for brute-force attack.

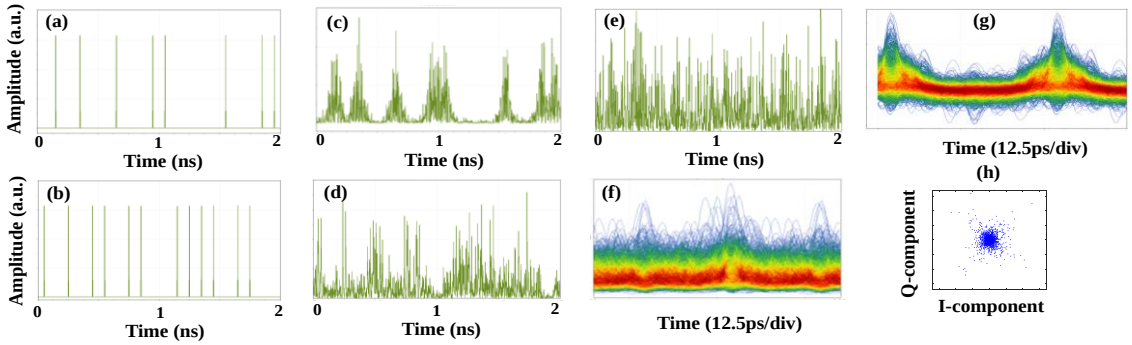

Fig.3 (a)~(d) Waveforms of CSK data before and after OPE modules for upper and lower branch; (e)~(h) Encrypted waveform and eye diagram of orthogonal DQPSK/CSK signal; and (g)~(h) incorrectly decrypted CSK/DQPSK signal for an eavesdropper.

The decryption performance for the legal user is further investigated. When the correct key parameters are applied into the OPD at the receiver side, the original DQPSK modulated short optical pulses are successfully recovered, whose waveform is shown in Fig.4 (a). After balanced photon-detection, the CSK data can be easily extracted. Fig.4 (b) and (c) show the waveform of the CSK data and corresponding eye diagram with clear eye opening. The constellation diagram for the DQPSK data after demodulation is also recovered as shown in Fig.4 (d). The error vector magnitude (EVM) performance for the DQPSK data and bit error ratio (BER) for the CSK data are illustrated in Fig.4 (e)~(f) by comparing with different case of key parameters R_1=R_2=10Gb/s, D_1=800ps/nm, D_2=400ps/nm. High dispersion value and encryption bit rate are desirable to get a reduced EVM and BER for the orthogonal DQPSK/CSK data due to the improved auto/cross-correlation ratio at the decryption part. EVM lower than the FEC limit of 35.2% for DQPSK can be obtained for both cases. As for the binary CSK data, BER lower than 10^{-9} can be also achieved, which demonstrate the feasibility of the proposed scheme.

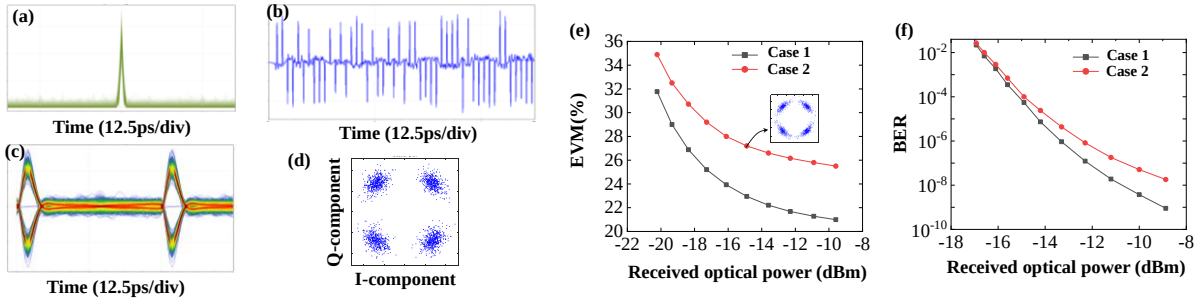

Fig.4 (a)~(b) Waveforms of decrypted DQPSK pulse and CSK signal after BPD; (c)~(d) Eye diagram of CSK signal and the constellation diagram of DQPSK signal; (e)~(f) EVM and BER performances for DQPSK and CSK signal, respectively.

4. Conclusion

We proposed a physical layer secure optical communication scheme that enables simultaneous transmission of orthogonal DQPSK/CSK modulated private data in a single optical channel. Symbol overlapped random optical phase encryption was utilized to transform the orthogonal signal into noise-like signal for guaranteeing secrecy. A total of 30Gb/s private data with orthogonal modulation format was encrypted and successfully recovered.

Acknowledgement

The work was supported by National Key Research and Development Program of China under grant 2018YFB1801301 and National Natural Science Foundation of China (NSFC) under grant U2001601 and 11904057.

References

[1] N. S. Kapov, et al., IEEE Commun. Mag., **54**, 110-117 (2016).
[2] Y. Gong, et al., Light Sci. Appl., **9**, 170 (2020).
[3] A. Argyris, et al., Nature, **438**, 343-346 (2005).
[4] Z. Gao, et al., Opt. Lett., **36**, 1623-1625 (2011).
[5] N. Jang, et al., Opt. Lett., **44**, 1536-1539 (2019).
[6] T. Kodama, et al., CLEO, JTh2A.77 (2019).
[7] M. Furdek, et al., ICTON, Tu.D3.5 (2014).
[8] B. Dai, et al., Opt. Eng., **57**, 100502 (2018).