40Gb/s Secure Optical Communication Based on Symbol-by-Symbol Optical Phase Encryption

Zhensen Gao, Yuehua An, Anbang Wang, *Member, IEEE*, Pu Li, Yuwen Qin, Yuncai Wang, and Xu Wang, *Senior Member, IEEE*

***Abstract*—Achieving high speed physical layer security is a constant pursuit but critical challenge for the information society. In this paper, a novel symbol-by-symbol optical phase encryption technique relying on ultra-long, reconfigurable optical phase patterns and commercial off-the-shelf dispersive components is proposed for high speed physical layer security. A record 40Gb/s secure optical communication system with symbol overlapped, optical phase encrypted differential-phase-shift-keying modulated signal is experimentally demonstrated based on the proposed technique. Security robustness against various eavesdropper's attacks has been validated for three optical codes with a chip rate of 40Gchip/s and variable code-length of 128-chip, 512-chip and 1024-chip, respectively. The demonstrated technique exhibits the advantages of supporting high bit rate operation and advanced optical modulation formats, improving code flexibility and cardinality, which makes it very promising for future ultrafast secure optical communication.**

***Index Terms*—Secure optical communication, communication system security, optical encryption, optical signal processing.**

I. Introduction

WITH the tremendous growth of big data in optical network, information security is becoming increasingly important, particularly in those security-sensitive applications such as military secret exchange, banking business, and private information sharing. Conventional software encryption strategies relying on computational complexity are facing severe challenges, as the emergence of super-computers or quantum computation will soon be able to crack the cryptography algorithms and perform prime factorization within acceptable time [1]. In order to meet the security demand of optical fiber communication system, hardware based physical layer encryption approaches have received much attention to circumvent those computation threats [2], [3]. As one of the most prominent techniques, quantum key distribution based secure optical communication has made great achievements in the past decades, offering theoretically absolute security based on uncertainty principle. But unfortunately, great efforts towards fully compatibility with commercial fiber-optic components are still in progress [4].

Chaotic optical communication is another attractive solution for physical layer security. In chaotic secure communication, the confidential information is concealed into the noise-like chaotic signal utilizing a chaotic optical transmitter. Only the authorized user with a synchronized chaotic optical receiver will be able to recover the chaotic optical carrier and then extract the confidential data [5], [6]. However, conventional chaotic optical transceivers usually require the use of complex laser structures and are extremely sensitive to the parameters mismatch [7], leading to the contradiction between robustness and security. Moreover, the bit rate of confidential data is greatly restricted by intrinsic relaxation oscillation frequency of chaotic signal [8], [9]. Hence, it is essential to explore other potential hardware encryption solutions using commercial low-cost optical components for secure optical communication.

Optical code (OC) processing technique is emerging as another attractive candidate for achieving physical layer security in recent years, due to its striking advantages of fully compatibility with conventional fiber-optic components and modern optical signal processing technologies [10], [11]. As the key component for optical code generation and recognition, the optical encoder is able to transform the optical pulse into a noise-like signal according to the unique OC, which intuitively makes an eavesdropper impossible to intercept the confidential data without the authorized OC and hence improving the data confidentiality. However, because most optical encoders usually have a fixed OC that cannot be rapidly reconfigured, an eavesdropper is possible to break the security by exhaustive brute-force attack or analyzing the fine structure of the encoded waveform or spectrum [12]. It has been already demonstrated that conventional on-off-keying (OOK), differential-phase- shift-keying (DPSK) or even code-shift-keying modulation formats are very vulnerable to simple

Manuscript received April 20, 2020; revised May 31, 2020; accepted June 1, 2020. Date of publication June 5, 2020; date of current version June 16, 2020. This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB1801301, in part by the National Natural Science Foundation of China (NSFC) under Grant 11904057, Grant 61927811, Grant 61961136002, Grant 61671316, and Grant 61731014, in part by the Science and Technology Planning Project of Guangdong Province under Grant 2018B010114002, and in part by the Program for Guangdong Introducing Innovative and Enterpreneurial Teams. *(Corresponding authors: Yuehua An; Yuncai Wang.)*

Zhensen Gao, Yuwen Qin, and Yuncai Wang are with the School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China, and also with the Guangdong Provincial Key Laboratory of Photonics Information Technology, Guangzhou 510006, China (e-mail: gaozhensen@gdut.edu.cn; qinyw@gdut.edu.cn; wangyc@gdut.edu.cn).

Yuehua An, Anbang Wang, and Pu Li are with the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, Taiyuan University of Technology, Taiyuan 030024, China (e-mail: anyuehua@163.com; wanganbang@tyut.edu.cn; lipu8603@126.com).

Xu Wang is with the School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, U.K. (e-mail: x.wang@hw.ac.uk).

Color versions of one or more of the figures in this letter are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LPT.2020.3000215

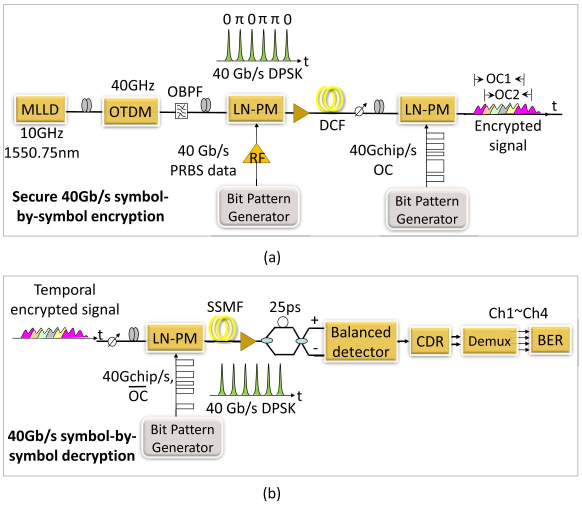


Fig. 1. Experimental setup of the secure symbol-by-symbol optical phase encryption system (a) 40Gb/s optical encryption (b) optical decryption scheme.

power detector or DPSK demodulation attack [13], [14]. Furthermore, the bit rate of OC processing systems is greatly limited by the chip rate and OC length, and the operation speed is generally restricted to 10Gb/s in conventional systems [15], [16]. Advanced optical encryption and modulation formats are thus highly desirable to eliminate the security vulnerability and enhance the transmission speed beyond 10Gb/s for high speed secure communication.

In this work, we propose a novel time stretched symbol-by-symbol optical phase encryption scheme with advanced phase modulation formats for high speed secure optical communication, which is capable of breaking the constraint between the bit rate, chip rate, and OC length. Ultra-high bit rate and chip rate, as well as ultra-long OC length can be simultaneously supported based on this scheme. A record 40Gb/s secure optical communication system with differential-phase-shift-keying modulated data and ultra-high chip rate of 40Gchip/s, ultra-long OC of up to 1024 chips is successfully demonstrated. The demonstrated system is very robust against both power detection and DPSK demodulation attacks, exhibiting great potential for combining hardware and digital encryption techniques to significantly enhance the security of fiber optical communication system.

II. Principle and Experiment Setup

Fig 1 illustrates the proposed symbol-by-symbol optical phase encryption technique and experimental setup for high speed secure communication. As shown in Fig. 1(a), an actively mode-locked laser diode (MLLD) operated at 10GHz is used as the laser source to generate a series of optical pulses with nearly transform-limited pulse width of 2.8ps and center wavelength of 1550.75nm. Then, the 10GHz optical pulse train is time-division-multiplexed into 40GHz pulses by a four-stage planar lightwave circuit (PLC) based optical-time-division-multiplexer (OTDM), which is equivalent to directly use an expensive 40GHz MLLD that is unavailable at the time of this experiment. After that, a pseudo-random-bit-sequence (PRBS) with a bit rate of 40Gb/s and data length of $2^9 - 1$ is precoded into DPSK data format and output by a bit pattern generator (BPG). The DPSK data is then used to phase modulate the optical pulse train through a 40GHz phase modulator to generate the 40Gb/s DPSK optical signal. In order to alleviate the dispersion mismatch in the whole system, an optical band-pass filter (OBPF) with 3dB bandwidth of ∼2nm is used before the phase modulator to cut off part of the spectrum, which slightly shape the optical spectrum and leads pulse width spreading to ∼4ps. The resulting spectrum and corresponding waveform are shown in Fig.2 (a) and (b), respectively. To perform symbol-by-symbol optical phase encryption, a spool of dispersion-compensation fiber (DCF) with chromatic dispersion value of around −331ps/nm is used to stretch the 40Gb/s DPSK optical pulse train in the time domain. Each symbol of the stretched pulses occupies ∼662ps time duration and thus the adjacent consecutive symbols are significantly overlapped with each other, which makes the MLLD optical source quite beneficial for enhancing security than using a continuous-wave carrier with a narrow spectral bandwidth and reduced symbol overlapping. Fig. 2(c) shows the measured waveform of the stretched pulses, which exhibit as a noise-like signal, making an eavesdropper unable to aware the existence of the confidential DPSK signal. Afterwards, an ultra-long, length-variable optical code (OC) with a chip rate of 40Gchip/s generated from a separate bit pattern generator is used to drive another phase modulator to perform time domain optical phase encryption. Since each symbol of the stretched pulses covers more than one-bit period, different stretched symbol will correspond to different part of the ultra-long OC, and equivalently be phase encrypted by respective code pattern, OC1, OC2..., which has an effective chip number of ∼26. The pattern and length of the OC can be rapidly reconfigured to another one in practical system to greatly expand the code cardinality and enhance the security, so as to prevent the eavesdropper from breaking the OC offline.

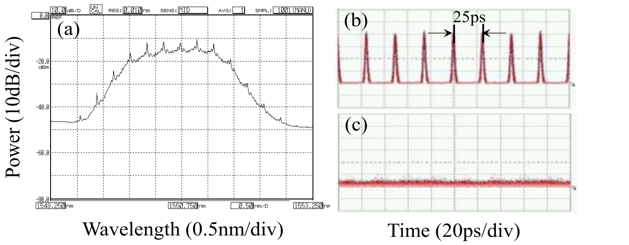


Fig. 2. (a) Spectrum and (b) waveform of the 40Gb/s DPSK optical signal before symbol-by-symbol phase encryption; (c) is the waveform of the time stretched optical pulses.

At the receiver side, for a legitimate user to recover the original DPSK optical pulses, the symbol-by-symbol phase encrypted signal firstly has to be phase decrypted and then be temporally compressed using a matched dispersive element with reverse dispersion compared to that of the DCF. Any malicious user will fail to access the confidential DSPK data without knowing the exact OC and dispersion value of DCF. As shown in Fig. 1(b), at the receiver side for a legitimate user, the optical decryption is configured in a symmetric structure with respect to the encryption part, with a separate 40GHz phase modulator driven by the inverse code of OC at a chip rate of 40Gchip/s to remove the random phase imposed by the phase encryption, and using another piece of standard single mode fiber (SSMF) with opposite dispersion of approximately +331ps/nm to fold the stretched symbols and regenerate the 40Gb/s DPSK optical pulse train. A tunable optical delay line with sub-picosecond resolution is placed before the phase modulator to temporally align the timing error between the encryption and decryption side. For a practical system, clock synchronization for the transceiver can be realized based on standard protocols such as 1588v2 before performing any optical encryption. After that, a delay line interferometer (DI) with one bit delay of 25ps followed by a balanced photodetector (BPD) is used for DPSK demodulation and detection. The extracted DPSK data is directed into a 40Gb/s clock and data recovery (CDR) circuit and then demultiplexed into four-channel 10Gb/s tributaries by an electrical demultiplexer for bit-error-ratio (BER) measurement.

III. Results and Discussion

In order to investigate the security of the 40Gb/s optical phase encryption system, three types of OCs with different lengths of 128, 512 and 1024 that are shorter, equal or longer than the data pattern sequence are used for phase encryption in a back-to-back scenario. The three OCs are randomly selected from Gold code plus a zero for testing the en/decryption performance, which however could also be a random binary or even multi-level sequence. In this scheme, it is evident that the eavesdropper cannot extract the confidential DPSK data if she has no knowledge of both the OC and dispersion value simultaneously. However, even if the information of OC is unavailable, an eavesdropper may be sophisticated enough and try to solely employ a tunable dispersion compensator for temporal compression in the receiver. Fig. 3(a) shows the spectrum obtained for a sophisticated eavesdropper using the matched reverse dispersion value but an incorrect OC with 1024-chip. Due to the imposed phase encryption on the overlapped symbols, the spectral profile has no any fine features and it is obviously distinct from the original 40Gb/s DPSK data modulated optical spectrum shown in Fig. 2(a), indicating that the phase relationship between different symbols has been completely broken by the optical encryption. The corresponding waveform and detected eye diagram after BPD are shown in Fig. 3 (b)∼(c), from which it can be readily observed that the compressed signals are still symbol overlapped with each other and the eye diagram exhibits as a noise, showing high security robustness against a sophisticated eavesdropper's attack, let alone an ordinary eavesdropper without any information of the OC and dispersion value.

On the contrary, by simultaneously using a matched reverse dispersion compensation fiber and applying the correct OC, the symbol overlapped signal can be phase decrypted and the original DPSK data can be retrieved as well. Fig. 4(a1)-(a3), (b1)-(b3) and (c1)-(c3) show the measured waveforms of the encrypted signals, optical spectra and corresponding waveforms of the correctly decrypted signals for the three trials with different OC lengths of 128, 512 and 1024, respectively. From the middle column of Fig.4, one can see that the spectral profiles and fine spectral structures of the decrypted signals resembles the original DPSK optical spectra, indicating that the phase relationship between adjacent symbols have been preserved. Compared with the noise-like encrypted waveforms shown in Fig.4 (a1)-(c1), the correctly decrypted signals for the legitimate user recovers the original 40GHz optical pulse trains with clear eye opening. Since each symbol experiences a different effective optical phase pattern, the decryption performance is slightly different for each symbol when the rise and fall transitions of code patterns are taken into account, which causes slight pulse amplitude fluctuation, as shown in Fig.4 (a3)-(c3). Nevertheless, the confidential data carried by the optical phase can be fully extracted. Fig.5 (a) and (b) show the measured eye diagrams for the decrypted 40Gb/s optical pulse trains after the balanced detection and CDR, respectively. Wide eye openings have both been achieved, which demonstrates that the phase information of original 40Gb/s signal has been successfully recovered. Note that the waveforms of the correctly decrypted signal in Fig. 4 (a3)-(c3) is broader than the original optical pulse train, which is mainly attributed to the slight dispersion mismatch of the SSMF in the decryption side.

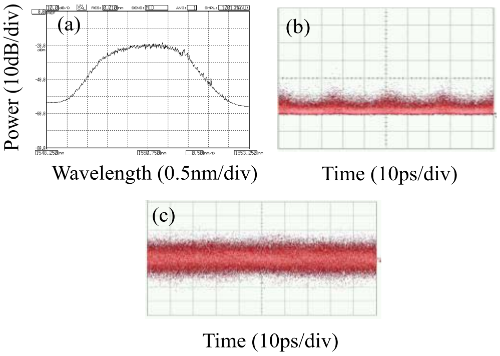


Fig. 3. (a) Measured spectrum and (b) waveform for an eavesdropper with matched dispersion but incorrect OC; (c) Measured eye diagram after BPD for the eavesdropper.

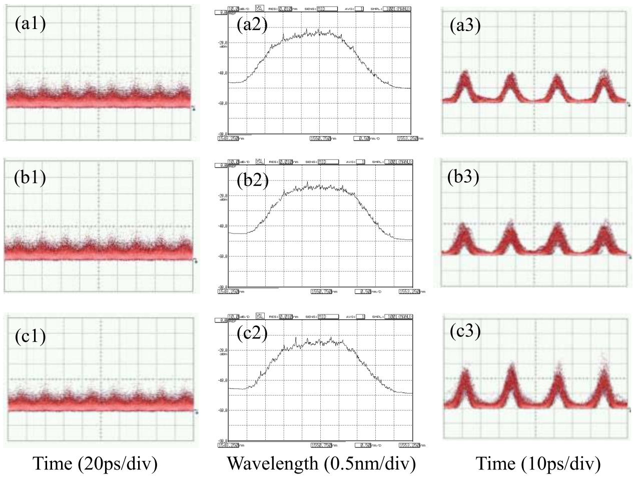
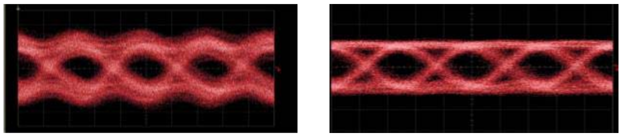


Fig. 4. Encrypted waveforms, decrypted optical spectra and waveforms by a legitimate user for (a1-a3) 128-chip, (b1-b3) 512-chip and (c1-c3) 1024-chip.

Fig. 6 shows the measured auto-correlation traces of the original 40GHz optical pulse train after the OBPF, the correctly and incorrectly decrypted signals by using an auto-correlator with 60ps scanning range. It can be seen that the



(a) Time (10ps/div) (b) Time (10ps/div)

Fig. 5. (a) Measured eye diagrams of the recovered 40Gb/s data after balanced detection and (b) after CDR.

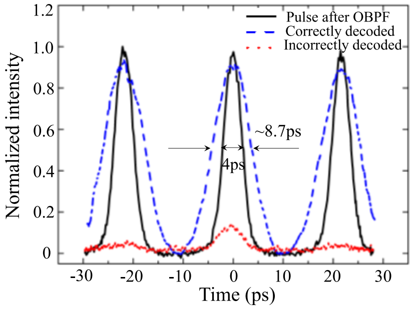


Fig. 6. Auto-correlation traces of the original signal, correctly and incorrectly decrypted signals.

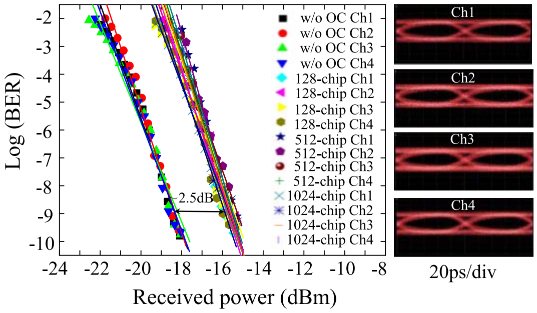


Fig. 7. BERs of the demultiplexed four-tributary 10Gb/s DPSK data of the 40Gb/s signal.

optical pulse has been broadened from ~4ps to ~8.7ps due to the non-ideal dispersion compensation, which corresponds to ~350m SSMF length mismatch with a dispersion slope of ~16.75ps/nm/km. An OBPF is hence used in the transmitter part to alleviate the dispersion mismatch induced impairment in the experiment. Despite of the slight mismatch, an auto-correlation signal with high peak power for the correctly decryption has been successfully obtained. In contrast, only a cross-correlation signal with low peak power is obtained for the incorrectly decryption.

The BER performances of the 40Gb/s DPSK signals are finally evaluated after being demultiplexed into four individual 10Gb/s data using an electrical demultiplexer for the three codes, as shown in Fig. 7. The eye diagrams of the demultiplexed four-tributary 10Gb/s data are also shown in the right side of Fig.7 with clear eye opening. A power penalty of around 2.5dB has been introduced for the correct decryption when comparing with the case of without en/decryption, which is mainly caused by the dispersion mismatch and code pattern transition induced non-ideal decoding. BER lower than 10^{-9} has been achieved for all the demultiplexed channels of the three OCs, which verifies the feasibility of the system for high speed secure optical communication.

IV. Conclusion

To conclude, we propose and experimentally demonstrate a symbol-by-symbol optical phase encryption scheme with advanced phase modulation formats for applications in high speed secure optical communication. A 40Gb/s, 40Gchip/s, secure optical communication system with DPSK modulation format based on the proposed technique has been successfully demonstrated. By using commercial hardware optical components for encryption, the demonstrated system can be operated easily in a plug-and-play way and enable rapid reconfiguring the length-variable, ultra-long optical code with large code cardinality. It also exhibits the potential to support higher order quadrature-amplitude-modulation formats and wavelength/space division multiplexing technology to further enhance the capacity beyond 100Gb/s, and thus making it a very promising solution for future high speed secure optical communication and realizing even one time pad.

References

[1] Y. Zhang *et al.*, "DNA origami cryptography for secure communication," *Nature Commun.*, vol. 10, Nov. 2019, Art. no. 5469.

[2] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 725–736, Sep. 2011.

[3] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, Aug. 2016.

[4] F. Cavaliere, E. Prati, L. Poti, I. Muhammad, and T. Catuogno, "Secure quantum communication technologies and systems: From labs to markets," *Quantum Rep.*, vol. 2, no. 1, pp. 80–106, Jan. 2020.

[5] A. Argyris *et al.*, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 7066, pp. 343–346, Nov. 2005.

[6] R. M. Nguimdo, P. Colet, L. Larger, and L. Pesquera, "Digital key for chaos communication performing time delay concealment," *Phys. Rev. Lett.*, vol. 107, no. 3, Jul. 2011, Art. no. 034103.

[7] Y. C. Kouomou, P. Colet, L. Larger, and N. Gastaud, "Mismatch-induced bit error rate in optical chaos communications using semiconductor lasers with electrooptical feedback," *IEEE J. Quantum Electron.*, vol. 41, no. 2, pp. 156–163, Feb. 2005.

[8] R. Lavrov, M. Jacquot, and L. Larger, "Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s chaos communications," *IEEE J. Quantum Electron.*, vol. 46, no. 10, pp. 1430–1435, Oct. 2010.

[9] N. Jiang, A. Zhao, C. Xue, J. Tang, and K. Qiu, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," *Opt. Lett.*, vol. 44, no. 7, pp. 1536–1539, 2019.

[10] X. Wang, Z. Gao, X. H. Wang, N. Kataoka, and N. Wada, "Bit-by-bit optical code scrambling technique for secure optical communication," *Opt. Express*, vol. 19, no. 4, pp. 3503–3512, 2011.

[11] E. Wohlgemuth, Y. Yoffe, T. Yeminy, Z. Zalevsky, and D. Sadot, "Photonic-layer encryption and steganography over IM/DD communication system," *Opt. Express*, vol. 26, no. 25, pp. 32691–32703 2018.

[12] Z. Si, F. Yin, M. Xin, H. Chen, M. Chen, and S. Xie, "Code extraction from encoded signal in time-spreading optical code division multiple access," *Opt. Lett.*, vol. 35, no. 2, pp. 229–231, 2010.

[13] Z. Jiang, D. E. Leaird, and A. M. Weiner, "Experimental investigation of security issues in O-CDMA," *J. Lightw. Technol.*, vol. 24, no. 11, pp. 4228–4234, Nov. 2006.

[14] B. Dai, Z. Gao, X. Wang, N. Kataoka, and N. Wada, "Demonstration of differential detection on attacking code-shift-keying OCDMA system," *Electron. Lett.*, vol. 46, no. 25, pp. 1680–1682, 2010.

[15] Y. Okamura, O. Iijima, S. Shimizu, N. Wada, and M. Hanawa, "Simultaneous detection of 10-Gbit/s QPSK×2-ch. Fourier-encoded synchronous OCDM signals with digital coherent receiver," *Opt. Express*, vol. 21, no. 3, pp. 3298–3307, 2011.

[16] T. Kodama and G. Cincotti, "DPSK-based 65536-ary ciphering for secure optical communications," in *Proc. Conf. Lasers Electro-Opt.*, May 2019, pp. 1–2, Paper JTh2A.77.