Two-Level Optical Encryption for Secure Optical Communication

Yetian Huang[(1)], Haoshuo Chen[(2)], Hanzi Huang[(1)], Qianwu Zhang[(1)], Zhengxuan Li[(1)], Nicolas K. Fontaine[(2)], Roland Ryf[(2)], and Min Wang[(1)]

[(1)] Key laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai Institute for Advanced Communication and Data Science, Shanghai University, 200444 Shanghai, China
[(2)] Nokia Bell Labs, 791 Holmdel Rd., Holmdel, NJ 07733, USA
haoshuo.chen@nokia-bell-labs.com

Abstract: We demonstrate 60 Gbit/s transmission over 43-km SMF using low-coherence matched detection combined with spectral phase coding as two-layer optical encryption. Encrypted signal and carrier are multiplexed through polarization diversity and demultiplexed using polarization tracking. © 2020 The Author(s)

OCIS codes: (060.1660) Coherent communications; (060.4785) Optical security and encryption.

1. Introduction

With the explosive growth of optical networks, it becomes essential to improve the network security and protect highly classified information using advanced encryption solutions. Devices for optical fiber eavesdropping nowadays are commercially available. The way to partially extract light from optical fiber can be as simple as bending the fiber and detecting the leaked light from fiber cladding for eavesdropping [1]. In the past few years, many optical encryption schemes have been proposed, such as Quantum key distribution [2], Chaotic communication [3], Optical Code Division Multiple Access (O-CDMA) [4–6] and so on. With these techniques, data is much less vulnerable to eavesdropping. But most require the use of complicated optical components such as quantum light sources, femtosecond lasers or sophisticated synchronizations [7]. In the construction of next-generation optical networks, it is essential to explore more low-cost encryption solutions to establish secure optical communication.

Amplified spontaneous emission (ASE) noise has been applied in the applications such as optical steganography [8] and optical crosstalk mitigation [9] employing its low temporal coherence. ASE noise can be easily generated by a pumped gain medium such as erbium-doped fiber (EDF). The ASE generation process is completely random, therefore, it cannot be reproduced, which can be a useful property for optical encryption.

In this paper, we demonstrate a secure optical transmission system based on low-coherence matched coherent detection [9] using an ASE source. Two-level optical encryption is achieved, where a temporal delay between the signal and ASE carrier is used as the 1^{st} encryption key. Code applied for optical spectral phase coding on the broad ASE is the 2^{nd} key. Signal and ASE-carrier co-propagation over same single-mode fiber (SMF) is enabled by polarization multiplexing. Polarization tracking is employed at the receiver to separate the signal and carrier for matched coherent detection. 20-Gbaud QPSK and 8-PSK transmission over 43-km SMF is experimentally demonstrated.

2. Low-Coherence Matched Detection

A bandwidth-controllable low-coherece source (LCS) can be simply realized through spectrally filtering ASE noise produced by an EDFA. Due to it randomness, ASE noise with a wider spectrum will have a shorter coherence length, which increases the temporal matching requirement at the receiver. Figure 1 shows the measured interferogram for ASE noise with different spectral widths ($\mathbf{B_{ase}}$), which indicates its coherence length. It can be noticed that as $\mathbf{B_{ase}}$=1 nm, the temporal coherence length is as short as 5 ps, which corresponds to a 1-mm long optical fiber.

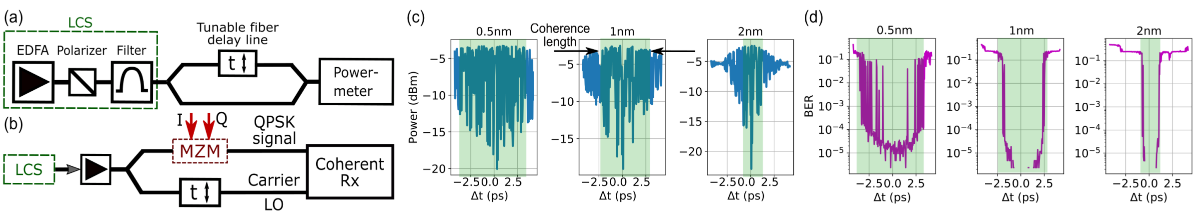

Fig. 1: Setup for (a) measuring inteferogram of a low-coherence source and (b) ASE-based low-coherence matched detection, (c) measured optical interferogram and (d) achieved BER for ASE with different $\mathbf{B_{ase}}$ versus time difference Δt.

Electrical signal can be recovered through the interference between the ASE-carried signal and unmodulated ASE carrier which is similar to conventional coherent detection. However, this interference only happens within the coherence length of the ASE source [9]. The setup to characterize the performance of low-coherence matched detection is shown in Fig. 1(b). Fig. 1(d) gives the measured BER versus the time difference Δt between the signal and LO path. It can be seen that within the coherence range, where strong coherent interference occurs, signals can be recovered with low BER. Since the coherence length of ASE noise is so short, it is challenging to match this optical path length without any prior knowledge. The fiber added to decorrelate the signal and carrier at the transmitter can be meters to kilometers. Eavesdropper needs to search more than ten million possibilities (the ratio between the coherent length, e.g.,1 mm and maximum delay range, e.g.,10 km) physically to break the security. This temporal delay can be dynamically changed and forms the 1^{st} key, which is only shared between the transmitter and authorized receiver.

3. Enhanced Spectral Phase Coding

Spectral phase coding through applying different phase modulation to different frequency bins has been used in O-CDMA [4]. Wavelength selective switch (WSS) can be employed to achieve this broadband and frequency-dependent phase modulation due to its programmability. However, spectrum signature will be introduced after the phase modulation due to the diffraction effects from the WSS, which can be used by the eavesdropper to predict the code. We use dispersion as the coding scheme, which is realized by applying a quadratic phase to the ASE-carried signal using a WSS. Figure 2(b) shows the optical spectrum after applying -25 ps/nm or -10 ps/nm dispersion to the signal with $\mathbf{B_{ase}}$ of 4 nm. The spectral roll-off is caused by the artifacts and increases as a larger dispersion is applied. In order to remove the coding-induced spectrum signature, we use a delayed ASE carrier to cover the spectrally coded signal to produce a flat spectrum, see Fig. 2(b). It has been verified that low-coherence matched detection has a strong optical crosstalk tolerance [9] so that this additional noise has a small impact to the system performance.

4. Transmission Experimental Results

The setup for the secure optical transmission system with two-level optical encryption based on low-coherence matched detection is shown in Fig. 2(a). At the transmitter (Alice), 20-Gbaud QPSK or 8-PSK signal is generated through a single-polarization Inphase and Quadrature (IQ) Mach-Zehnder modulator (MZM). One copy of the ASE source without modulation is used as the LO for matched detection at the receiver (Bob). We use 40-m SMF as the temporal delay key to decorrelate the signal and LO. Spectral phase (de)coding is achieved employing an WSS to modulate the spectrum of the signal with a continuous quadratic phase at Alice. The spectrum signature from spectral phase coding is buried in another delayed copy of the ASE carrier, whose power is adjusted by an optical attenuator to produce a flat spectrum.

We use polarization diversity to transmit the signal and ASE LO over the same SMF. Polarization tracking is applied at Bob through an electrically driven polarization controller (EDPC) followed by a polarization beam

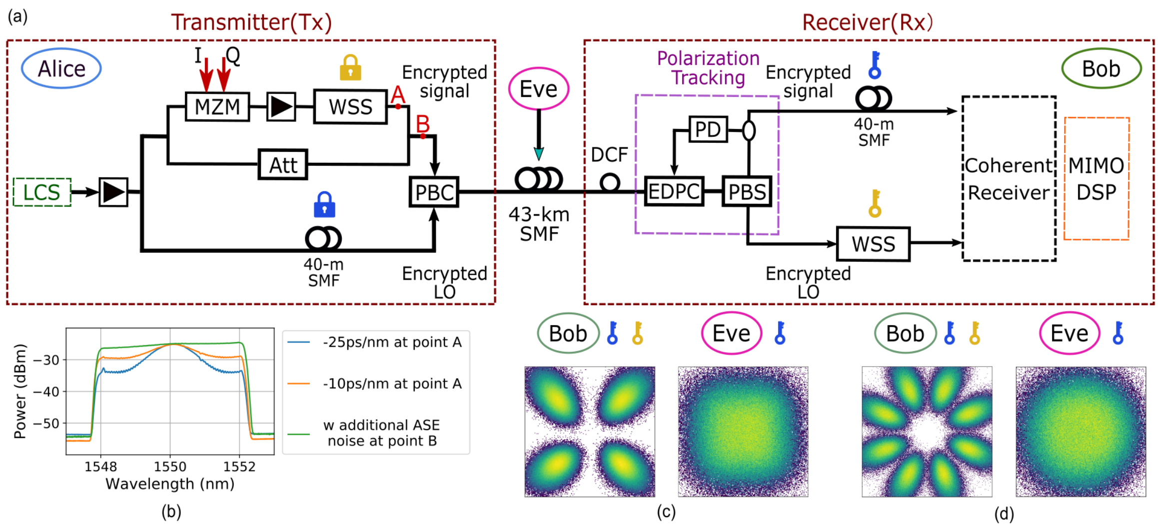

Fig. 2: (a) Setup for the secure optical transmission system with two-level optical encryption based on low-coherence matched detection, (b) measured optical spectra of the signal carried by 4-nm ASE noise after spectral phase coding, as applied dispersion is -25 ps/nm and -10 ps/nm, and is flattened after combining with a delayed ASE carrier, recovered constellation of (c) QPSK and (d) 8-PSK signal with two-level optical encrytion after 43-km SMF transmission with (Bob) and without (Eve) encryption keys.
(Eve: eavesdropper, WSS: Wavelength selective switch, PBC: polarization beam combiner, PBS: polarization beam splitter, EDPC: electrically driven polarization controller, DCF: dispersion compensating fiber, Att: attenuater, LO: local oscillator)

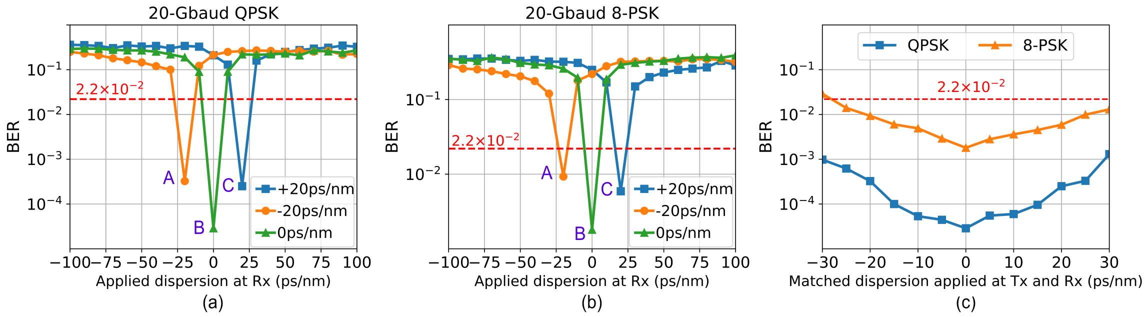

Fig. 3: After 43-km SMF transmission with temporal delay matched, measured BER versus applied dispersion at Rx and different spectral phase coding (dispersion) applied at Tx for (a) QPSK and (b) 8-PSK, (b) same dispersion applied at both Tx and Rx for different modulation.

splitter (PBS) to demultiplex the signal and ASE LO for matched detection. Partial optical light from the PBS output port for the signal is directly detected by a photo-detector (PD) and captured by an oscilloscope. The tracking mechanism is through controlling the EDPC to maximize the RF power which effectively is a measure of the residual amplitude modulation from the MZM [10]. Bob has 40-m SMF added to the signal path to temporally match the signal and ASE LO. Identical quadratic phase modulation is applied to the ASE LO using another WSS to match the spectral phase of the signal. In principle, a reverse quadratic phase modulation can be applied to the signal to undo the spectral phase coding, however this will not match the spectral amplitude.

After 43-km standard SMF transmission, the recovered constellations at Bob and the eavesdropper (Eve) are present in Fig. 2(c) and (d) for a 20-Gbaud QPSK and 8-PSK signal, respectively. When the temporal delay and spectral phase between the signal and LO are both matched (Bob has both keys), the signal can be detected and properly recovered. Even if Eve has the temporal delay information, without correctly matching the spectral phase, data recovery is still impossible. Bob achieves bit error rate (BER) of 1.2×10^{-5} and 9.8×10^{-4} for QPSK and 8-PSK signal, respectively. A dispersion compensating fiber (DCF) is used to compensate the chromatic dispersion (CD) of the 43-km SMF.

Figure 3(a) and (b) shows the system performance of both QPSK and 8-PSK signals after 43-km SMF transmission when the temporal delay is matched and only the Rx dispersion is scanned for different amount of dispersion applied at Tx. It can be observed that a small mismatch in dispersion significantly degrades the performance, which confirms that the spectral phase coding is beneficial in enhancing the security. To analyze the performance differences between the three matched points (A, B and C in Fig. 3(a) and (b)). We measured the BERs for various amount of dispersion applied and matched at the Tx and Rx, see Fig. 3(c). We attribute this performance degradation to the diffraction effects from the WSSes, whose impact increases as applied dispersion gets larger. Alternatively, fiber Bragg gratings and integrated micro-ring resonators can be applied to provide large amount of dispersion for encryption without introducing any diffraction artifacts so the system performance can be improved.

5. Conclusion

We experimentally demonstrated a two-level optical encryption scheme and realized 20-Gbaud QPSK and 8-PSK transmission over 43-km SMF. Without matching either the temporal delay or the spectral phase, electrical signal cannot be detected. Low-coherence matched detection supports high-capacity transmission employing advanced modulation formats so can be an alternative cost-efficient scheme to enhance the security of optical networks.

This work was supported in part by the National Natural Science Foundation of China (Project No. 61420106011, 61635006, 61601277, 61601279) and the Science and Technology Commission of Shanghai Municipality (Project No. 17010500400, 18511103400).

References

1. K. Shaneman, S. Gray, "Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection and prevention," in *IEEE Military Communications Conference*, 711-716, 2004.
2. N. Gisin, R. Thew, "Quantum communications," in *Nat. Photonics* **1**, 165-171, 2007.
3. A. Argyris, et.al., "Chaos-based communications at high bit rates using commercial fibre-optic links," in *Nature* **438**, 343-346, 2005.
4. Z. Jiang, et.al., "Experimental Investigation of Security Issues in O-CDMA," in *J. Lightwave Technol.* **24**, 4228-4234, 2006.
5. Z. Si, et.al., "Code extraction from encoded signal in time-spreading optical code division multiple access," in *Opt. Lett.* **35**, 229-231, 2010.
6. X. Wang, et.al., "Bit-by-bit optical code scrambling technique for secure optical communication," in *Opt. Express* **19**, 3503-3512, 2011.
7. M. Peil, et.al., "Synchronization of Chaotic Semiconductor Laser Systems: A Vectorial Coupling-Dependent Scenario," in *Phys. Rev. Lett.* **88**, 2002.
8. B. Wu, et.al., "Optical steganography based on amplified spontaneous emission noise," in *Opt. Express* **21**, 2065-2071, 2013.
9. H. Chen, et.al., "Optical Crosstalk Reduction using Amplified Spontaneous Emission (ASE)," in *Optical Fiber Communication Conference*, p.M4G.5, 2018.
10. Z. Wang, C. Xie, "Automatic optical polarization demultiplexing for polarization division multiplexed signals," in *Opt. Express* **17**, 3183-3189, 2009.