Experimental Demonstration of All-Optical 8-Gbit/s Secure Free-Space Chaotic Communications over 8.2-meter Link Based on Unidirectional Injection-Locking Chaos Synchronization

Yiqun Zhang[1,2,6], Mingfeng Xu[1,3], Qiang Chen[1,4], Mengjie Zhou[5], Shuangcheng Chen[5], Mingbo Pu[1,3,4], Ning Jiang[2], Kun Qiu[2], Martin P. J. Lavery[6], Hasan T. Abbas[6], and Xiangang Luo[1,4,*]

[1] *State Key Laboratory of Optical Technologies on Nano-Fabrication and Micro-Engineering, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China*

[2] *School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China*

[3] *Research Center on Vector Optical Fields, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China*

[4] *School of Optoelectronics, University of Chinese Academy of Sciences, Beijing 100049, China*

[5] *Tianfu Xinglong Lake Laboratory, Chengdu 610299, China*

[6] *James Watt School of Engineering, University of Glasgow, Glasgow G128LT, UK*

* *Corresponding authors: lxg@ioe.ac.cn*

Abstract: We first experimentally demonstrate an 8-Gbit/s free-space secure chaotic optical communications link over 8.2 meters in a long corridor with satisfactory BER performance by achieving one-way injection locking chaos synchronization. © 2022 The Author(s)

1. Introduction

Free-space optical (FSO) communication has gained extensive investigations since it provides flexibility, high data capacity, high directivity, and unlicensed spectrum compared to conventional microwave systems [1,2]. With the growing demand for large-capacity communication systems, the security of optical systems is becoming increasingly important. Although free-space channels offer a higher level of security than other mediums, the large laser beam diameter at the receiving terminal still leads to a risk of information leakage, especially over long distances [3]. Chaotic cryptography has been widely studied and plenty of breakthroughs have been achieved since the first successful verification of chaotic synchronization in 1990 [4]. However, most experimental optical systems reported so far are transmitted through optical fiber links [5-7]. Although Rultov presented a self-synchronizing chaotic communication over a 5 km FSO link with the BER of 1.92×10^{-2} in 2002, the data rate is only about 60 Kb/s and the chaotic signal is generated in the electrical circuit [8]. The experimental study of the issues related to all-optical chaotic encryption that employs broadband chaos as the optical carrier and high-quality chaos synchronization under atmospheric turbulence for real high-speed, fully optical modulated FSO secure systems has not been reported, up to the authors' best knowledge.

In this paper, we first experimentally demonstrate an 8.2-meter 8-Gbit/s FSO secure communications link using optical chaotic modulation. A 1.9-meter hot air convection atmospheric turbulence simulator is placed between the transmitter (Alice) and receiver (Bob), and the natural atmospheric environment is simulated by setting parameters such as temperature difference T between the upper and lower parallel plates, wind speed, and transmission distance. The experimental results show that high-quality chaos synchronization can be achieved, even under strong turbulent conditions. Based on the broadband chaotic carrier induced with high bias current, a high-security FSO data transmission system with a bit rate over Gb/s and satisfactory BER below the forward error correction (FEC) limit of 3.8×10^{-3} is achieved.

2. Experimental setup

Figure 1 shows the experimental setup of the all-optical secure FSO chaotic communication system. A conventional external-cavity semiconductor laser (ECSL) with optical feedback is used as the chaotic optical carrier source, which consists of a drive laser (DL), a polarization controller (PC1), a 50:50 fiber coupler (FC1), a variable optical attenuator (VOA) and a fiber mirror (M). After passing through an optical isolator (ISO1), the chaotic optical carrier is modulated with the message through an intensity modulator (IM) with a 3-dB bandwidth of 10 GHz. An erbium-doped fiber amplifier (EDFA) is utilized to amplify the chaotic encrypted signal to pre-compensate the attenuation caused by atmospheric turbulence and adjust the power injected into the slave laser (SL) to achieve unidirectional injection-locking chaos synchronization. Afterward, the amplified signal is sent to a collimator (COL.1) and a beam telescope with 5 times magnification, which emits a collimated Gaussian beam with a beam waist of 18.75 mm. After 8.2-meter FSO transmission, the beam is collected through a beam reduction telescope and then coupled into

single-mode fiber (SMF). The encrypted signal is then split into two parts through a 2×2 FC2. One part with the state of polarization adjusted by PC2 is unidirectionally injected into SL for chaos synchronization, and the synchronized chaotic signal is detected by a photodetector (PD1). The other part is detected by PD2 after passing through the delay line, which minimizes the time delay difference between the two signals. The recovered message is decrypted by subtracting the synchronized chaos from the encrypted transmitted signal and then filtered by a low-pass four order Butterworth filter with a cut-off frequency of 0.8R, where R is the transmission bit rate. In our experiment, the bias current of the lasers can be flexibly adjusted by the integrated low-noise driver. The operation wavelengths of lasers are 1549.6 nm and the feedback strength is fixed at -10 dBm. The output power at the transmitter is adjusted by EDFA from 10 dBm to 20 dBm. The wind speed and the transmission distance in the turbulence simulator are set as 2.5 m/s and 10 km, respectively. The bandwidths of both PDs are 20 GHz. A high-speed digital oscilloscope collects the two signals detected by PDs with the sampling rate of 100 GS/s and four 59-GHz bandwidth channels.

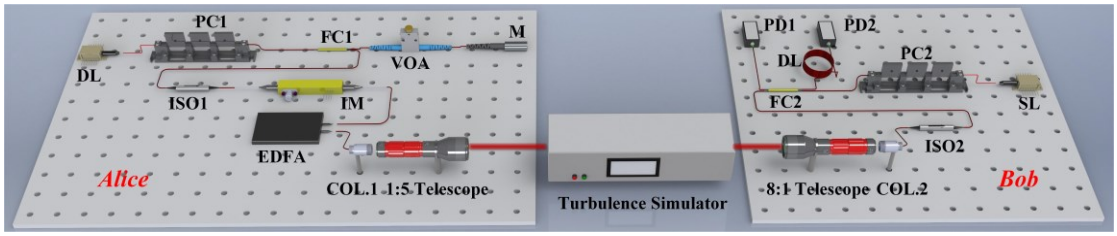

Fig. 1. Experimental setup of the proposed secure FSO communication system; DL, drive laser; SL, slave laser; PC, polarization controller; FC, fiber coupler; VOA, variable optical attenuator; M, mirror; ISO, optical isolator; IM, intensity modulator; EDFA, erbium-doped fiber amplifier; COL, collimator; DL, delay line; PD, photodetector.

3. Experimental Results and Discussion

Figure 2 shows the experimental results in terms of the chaos waveforms and power spectra for the chaotic carrier signal (first row) and the synchronized signal (second row) generated by DL and SL, respectively, at a bias current of 30 mA and without turbulence effects, as well as the correlation plot between them. Here, the cross-correlation coefficient (CC) defined in [9] is used to quantify the synchronization quality. It is observed that there is little difference between the two chaos waveforms (Fig. 2(a) and 2(b)). The effective bandwidths of the chaotic carrier signal and synchronized signal, defined as the span between the direct current component and the frequency where 80% of energy is contained in the RF spectrum [10], are about 8.5 GHz (Fig. 2(c) and 2(d)). In addition, the CC value between them is 0.94, and the correlation plot exhibits a 45-degree line as expected (Fig. 2(e)), which indicates that high-quality synchronization is achieved after being transmitted through an 8.2-meter corridor.

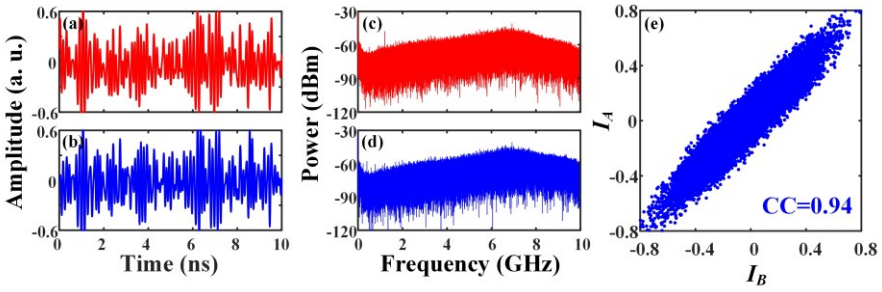

Fig. 2. Temporal intensity waveforms (first column), power spectra (second column) and the correlation plot of the two output chaotic signals.

To illustrate the atmospheric effects on synchronization performance, Fig. 3(a) presents the CC evolution between DL and SL with 20 mA bias current as a function of transmitter power under different input temperatures of the turbulence simulator. The Fried parameter r_0 can be deployed to characterize the atmospheric turbulence strength. In our experiments, r_0 can be adjusted by controlling the temperature T. As T is raised from 30 ℃ to 120 ℃, r_0 decreases from 4 cm to 1.1 cm, corresponding to the refractive index structure parameter C_n^2 of 10^{-15} to 10^{-13} (moderately strong turbulence). When the transmitter power is low, the turbulence significantly affects the quality of the injection-locked synchronization of the chaotic signal after free-space transmission, while when the transmitter power is increased above 15.5 dBm, the turbulence effect has almost no impact on the synchronization performance. The high-power laser can pierce the simulated atmospheric environment and enhance the signal-to-noise ratio of the system. Fig. 3(b) shows the CC curves between two chaotic signals under different bias currents cases. Similar to the

results obtained in Fig. 3(a), high-quality chaos synchronization is achieved for two lasers at all three bias currents when the transmitter power is increased over 15.5 dBm

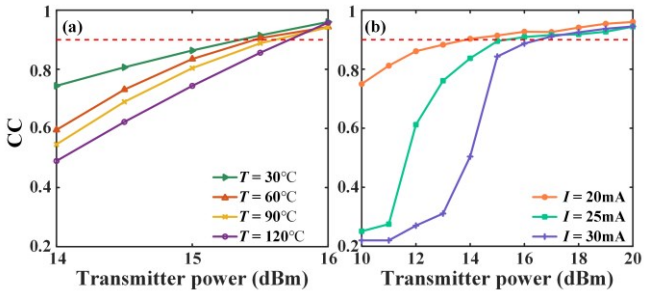

Fig. 3. Influence of transmitter power on the cross-correlation between DL and SL under (a) different turbulence strengths and (b) different bias currents. The red dashed line denotes the threshold of high-quality chaos synchronization with CC = 0.9.

Figure 4 demonstrates the transmission performance of the designed all-optical secure FSO chaotic communication system for the case of no turbulence effect. The original data with a bit rate of 6 Gbit/s is directly collected by the oscilloscope, as shown in the black line of Fig. 4(a). The recovered data is displayed in the red line. The comparison between the original and recovered signals indicates that the information is correctly retrieved. The eye diagram of the recovered data shown in Fig. 4(c) further confirms the excellent decryption performance. The corresponding encrypted signal illustrated in Fig. 4(b), where the temporal waveform exhibits a noise-like characteristic with randomly oscillating intensity, indicates that the original data is sufficiently hidden in the chaotic carrier, and the eye diagram shown in Fig. 4(d) is completely closed. Fig. 4(e) illustrates the BER performances of the encrypted and decrypted data versus the transmission bit rate for different laser bias currents. Here, 2×10^9 bits are used to calculate the BER by comparing the recovered data with the original one. For the legally recovered data under I = 30 mA case, the BER is always below 3.8×10^{-3} when R⩽8Gb/s, which is the hard decision forward error correction (HD-FEC) threshold. The results revealed that further increasing the laser bias current makes it possible to achieve secure FSO chaotic communications with a bit rate over 10 Gbit/s. In comparison, the BER of encrypted data is much higher than that of legally recovered one, and the information cannot be retrieved at BERs above 0.4.

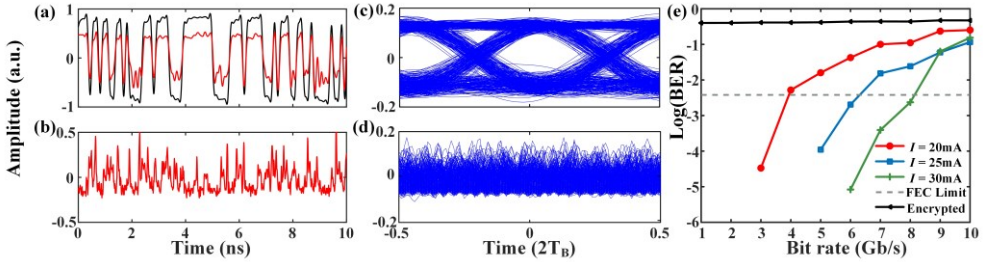

Fig. 4. Temporal intensity waveforms of (a) original message (black) and the recovered message (red), (b) encrypted message. The eye diagrams of (c) the recovered message and (d) the encrypted message. (e) BER performances of the encrypted message (black), the recovered message with I = 20mA (red), I = 25 mA (blue), and I = 30 mA (green). The gray dashed line denotes the threshold of HD-FEC.

4. Conclusion

We first experimentally demonstrated an all-optical secure FSO chaotic communication based on the unidirectional injection-locking synchronization mechanism. The chaos synchronization performance was analyzed under moderately strong turbulence strength induced by a hot air convection atmospheric turbulence simulator. The results indicate that high-quality synchronization with a large CC value of 0.94 can be obtained. The communication performance is investigated in different bias current cases, which reveal that the data information can be sufficiently hidden and correctly recovered at the receiver. It confirms the security enhancement of future FSO communications and the feasibility of chaotic laser application in the free-space environment.

5. References

[1] R. Zhang, et al., Nat. Photonics **15**, 743-750 (2021).
[2] V. Chan, J. Light. Technol. **24**, 4750-4762 (2006).
[3] M. Li, et al., Opt. Express **26**, 2954-2964 (2018).
[4] M. Pecora, et al., Phys. Rev. Lett. **64**, 821-825 (1990).
[5] A. Argyris, et al., Nature **438**, 343-346 (2005).
[6] R. Lavrov, et al., IEEE J. Quantum Electron. **46**, 1430-1435 (2010).
[7] A. Zhao, et al., J. Lightw. Technol. **39**, 2288-2295 (2021).
[8] N. Rulkov, et al., Phys. Rev. Lett. **89**, 277905 (2002).
[9] S. Xiang, et al., Opt. Lett. **47**, 2818-2821 (2022).
[10] A. Zhao, et al., Opto-Electron. Adv. **5**, 200026 (2022).