DC-bias Added Symmetrical 1-D Constellation Mapped Time-Domain Hybrid PAM System Using Simple Phase Encryption for Secure Visible-band Free-Space Optical Communication

Ayumu Kariya[(1)], Tomoya Ishikawa[(1)], Hodaka Amano[(1)], Fumiya Kobori[(1)], Keita Tanaka[(1)], Keiji Shimada[(1)], Reika Suketomo[(1)], Yuika Mori[(1)], Takahiro Kodama[(1)]

[(1)]Faculty of Engineering and Design, Kagawa University, 2217-20 Hayashi-cho, Takamatsu, 761-0396, Japan, kodama.takahiro@kagawa-u.ac.jp

Abstract *This experiment is the first to demonstrate the application of secure visible light band free-space optical communication to a hardware-effective no-excessive power penalty phase-encryption scheme. This scheme is applied to a flexible time-domain hybrid PAM signal with a fixed data symbol-to-encryption key bit ratio. ©2023 The Authors*

Introduction

Free-space optical (FSO) communication, capable of large-capacity transmission, has attracted attention as one of the 6th generation wireless communication standards [1–3]. In FSO communication, the wavelength band selected by the laser diode (LD) differs depending on the communication environment such as ground-to-satellite or underwater communication [4]. Visible-band FSO communication propagates in free space under conditions that allow human visual observation and eavesdropping; therefore, higher confidentiality is required compared to invisible-band FSO communication and wired communication [5]. Quantum key distribution (QKD) technology has been reported for highly secure FSO communication between two points [6–9]. By safely sharing the secret key between two points via QKD, selecting a simple algorithm for combining the data encryption keys is possible. For communication using terminals that have difficulty in supplying power, such as underwater terminals, a simple algorithm is preferable to a one with a large processing load, such as the current standard encryption algorithm. Recently, symbol-based encryption has been studied instead of bit-based encryption. Further, a simple phase shift method is as effective because it is easily implementable when the key interception is brutal [10–12].

Single-carrier [13] and multicarrier [14] schemes have been studied for variable-capacitance intensity modulation/direct detection transceivers in FSO communication. Although increasing the symbol rate per carrier is the basis for large-capacity transmissions, several encryption schemes have been reported [15,16]. In contrast, time-domain hybrid pulse amplitude modulation (TDHP) can realize variable capacity using the single-carrier method [17,18]. TDHP signals with a fixed symbol rate operation that is advantageous in environments where the frequency characteristics are static within the radio frequency (RF) band. The only necessity here is designing a fixed equalizer that compensates for the specified frequency characteristics of high-frequency devices. To the best of our knowledge, the application of symbol encryption to adaptive bit-rate single-carrier schemes in FSO systems has not been reported.

In this paper, we propose a direct current (DC) bias-added symmetric TDHP signal by applying symbol encryption using the phase-shift method for a secure visible band FSO system. Moreover, theoretical formulations and principal verification experiments were performed for the proposed system. This system can encrypt data while maintaining the number of data symbols and key bits by changing the generation ratio of the two modulation schemes under a fixed symbol rate in a TDHP signal composed of PAM2 and PAM4.

Principle of Phase Shift Encryption for DC-bias Added Symmetric TDHP Signals

As shown in Fig. 1(a), the DC-bias-added asymmetric TDHP signal consisting of PAM2 and PAM4 generates a transient response over multiple symbols at the boundary of different modulation schemes because the DC component is removed via C-coupling in a standard avalanche photodiode (APD). Figs 1(b,c) show the experimental time waveforms around the boundary symbols transitioning from PAM2 to PAM4 and vice versa. To prevent the occurrence of a transient response, a symmetrical TDHP signal with DC bias that does not generate a transient reaction after DC removal post-reception was used by adding a DC component to the low-multilevel PAM signal in advance. The theoretical formulas for bit error ratio (BER) versus signal-to-noise ratio (SNR) for a symmetric TDHP signal with a DC bias are as follows:

Fig. 1: (a) Transient response at the modulation scheme boundary in DC-bias added asymmetric TDHP signals, (b) experimental time waveform from PAM2 to PAM4, and (c) experimental time waveform from PAM4 to PAM2.

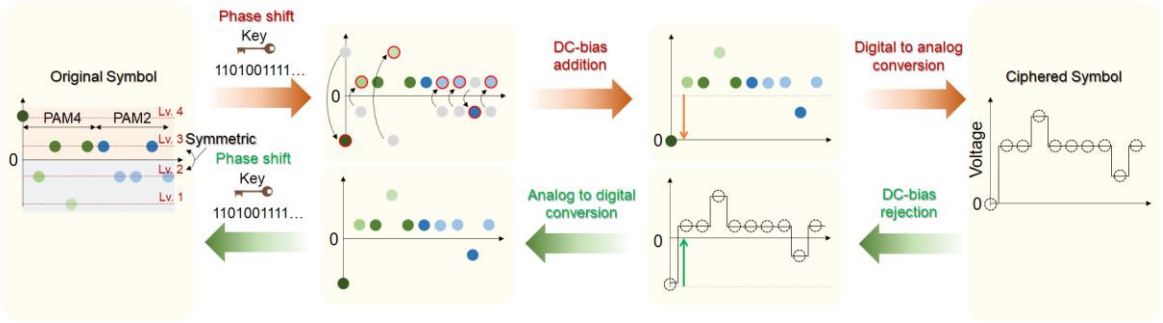

Fig. 2: Principle of phase shift encryption/decryption for DC-bias added symmetric TDHP signals.

$$\mathrm{BER}_{\mathrm{PAM2}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{1}{10}\mathrm{SNR}\frac{1-q}{2\{(1-p)(1-q)+p(1+q)\}}}\right) \quad (1)$$

$$\mathrm{BER}_{\mathrm{PAM4}} = \frac{3}{8}\mathrm{erfc}\left(\sqrt{\frac{1}{14}\mathrm{SNR}\frac{1+q}{2\{(1-p)(1-q)+p(1+q)\}}}\right) \quad (2)$$

$$\mathrm{BER}_{\mathrm{TDHP}} = \frac{2p}{1+p}\times\mathrm{BER}_{\mathrm{PAM4}} + \frac{1-p}{1+p}\times\mathrm{BER}_{\mathrm{PAM2}} \quad (3)$$

where p is the ratio of PAM4 to all the symbols, and q corresponds to the average power for transition from PAM2 to PAM4 when the average powers of PAM2 and PAM4 are equal. Optimum BER performance is obtained for any p when q = 0.17.

Figure 2 shows the phase-shift encryption/decryption principle for DC-bias-added symmetric TDHP signals. On the transmitter side, the data symbol stream of the original TDHP signal is phase-shifted according to the encryption key-bit stream. When the encryption key bit is one, the polarity of the data symbol is reversed, and when the encryption key bit is 0, the polarity of the data symbol is maintained while the encryption key bit is zero. Next, after adding DC bias to ensure that the lowest level of the PAM4 signal was 0, a DC-bias-added symmetric TDHP signal encrypted by the digital-to-analog converter was generated. On the receiver side, the signal was converted into a digital signal using an analog-to-digital converter after DC removal by the APD. The digitized symmetric TDHP signal was restored to the original TDHP signal by phase shifting using the same rule and cryptographic key on the transmitter side.

Experimental Setup

Figure 3 shows the experimental system setup of the 312.5 Msymbol/s symmetric TDHP signal with phase-shift encryption. On the transmitter side, the mapper generates a symbol stream of the TDHP signal from the data stream via offline digital signal processing (DSP). The masking component generates an encrypted symbol stream from the original symbol stream based on a 256-bit repeated encryption key bit stream. After outputting a symmetrical TDHP signal (p = 0.1 to 0.9) from an arbitrary waveform generator (AWG) with a sampling rate of 1.25 Gsample/s and a 250 MHz bandwidth limit, a DC-added symmetrical TDHP signal is input to a 450-nm blue LD with a bias T.

On the receiver side, the light collected by the condenser lens is input into the APD. The digital signal is sampled and quantized using a digital storage oscilloscope (DSO) with a sampling rate of 2.5 Gsample/s and bandwidth limit of 300 MHz at the output. At the offline DSP on the receiver, the band limitation of the RF device is compensated for by a 10-tap time-domain equalizer (TDE) based on the least-mean-square and 25-tap frequency-domain equalizer (FDE). After decoding the symbols based on the encrypted symbol stream in the demasking part, the original data stream is regenerated via hard decision processing. The BER characteristics are measured while changing the received power by cutting the beam cross-section with a beam shutter at the transmitter side.

Experimental Results

Figures 4 show the received power versus BER characteristics while changing p from 0.1 to 0.9 in steps of 0.1 under the following three conditions:

(Case 1) With a legitimate receiver for standard unencrypted TDHP signals
(Case 2) With a legitimate receiver that can correctly decode encrypted TDHP signals for cryptographic key sharing
(Case 3) With an eavesdropping receiver that

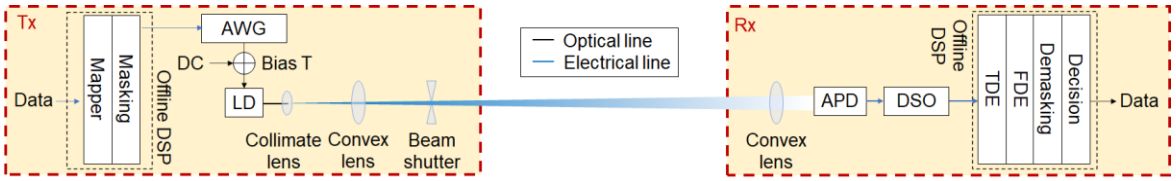

Fig. 3: Experimental setup.

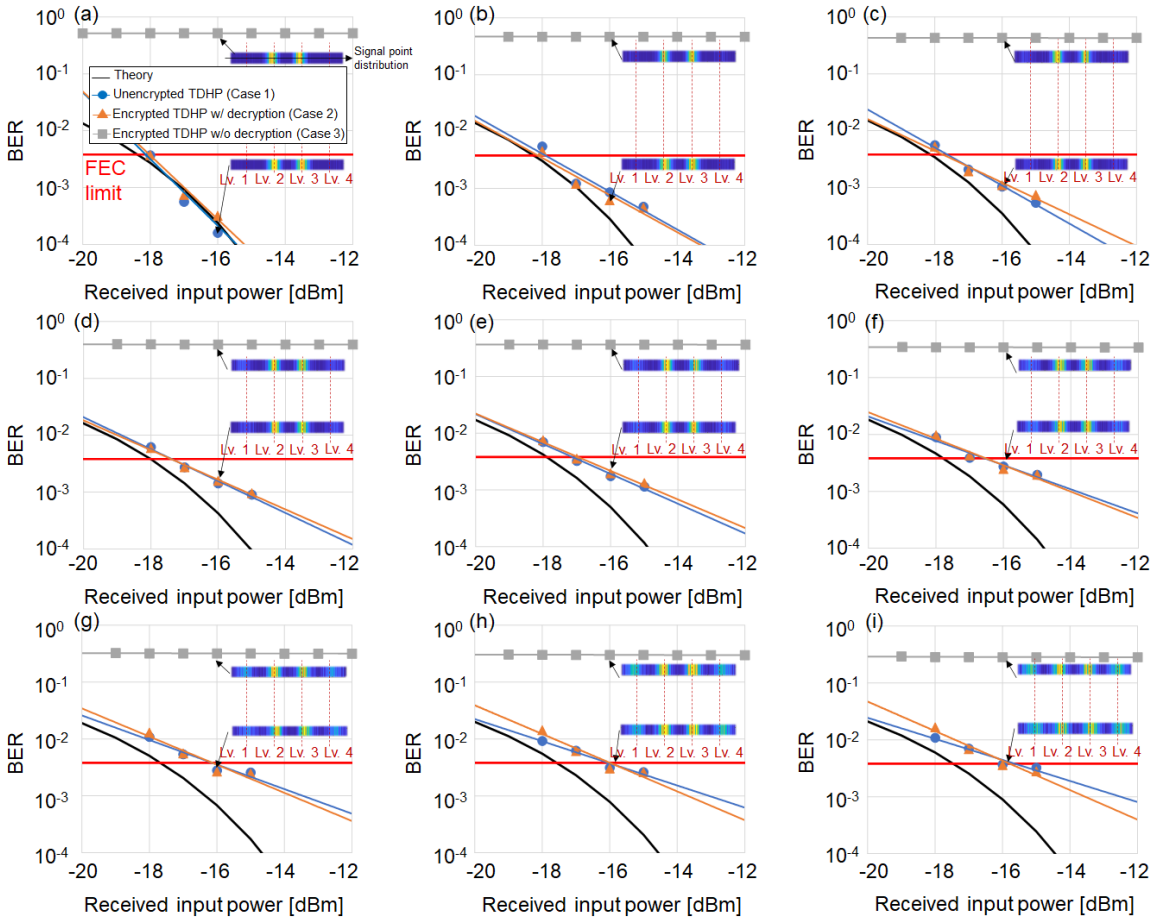

Fig. 4: (a-i) Theoretical and experimental BERs changing the *p* parameter from 0.1 to 0.9 by 0.1.

cannot decrypt encrypted TDHP signals due to non-shared encryption keys

Since the signal characteristics for cases 1 and 2 are constant for any *p*, encryption does not generate a power penalty. In addition, since the signals of cases 1 and 3 have similar signal distribution under the same received power conditions for any *p*, no features appear in the signal points, regardless of the success of decoding. At the received power of -16 dBm, which achieves the forward error correction (FEC) limit for any *p*, the noise distribution near the signal point is almost the same, so the effect of shot noise is small. The signal in case 3 cannot reach the FEC limit even at a high received power. The signal characteristics for cases 1 and 2 have a maximum penalty of 2 dB against theoretical characteristics owing to the influence of signal distortion received by PAM4 at $p = 0.9$. Here, the theoretical characteristics only consider thermal noise. As *p* increases, the number of PAM4 errors decreases; thus, the characteristics of case 3 improve slightly. This improvement is because the phase cipher for PAM4 is only valid for 1 bit out of 2 bits.

Conclusions

In a proof-of-principle experiment, phase-shift cryptography was applied to a symmetric TDHP signal with a DC offset for easy and reasonably secure visible-band FSO communication. We confirmed that the phase-shift cipher does not cause excessive power penalties for legitimate receivers with the encryption key, and that an eavesdropper without the key cannot reach the FEC limit under any received power condition.

Acknowledgements

This work was supported by JSPS KAKENHI Grant Number JP22K04105.

References

[1] A. Bekkali, H. Fujita, and M. Hattori, "Free-space optical communication systems for B5G/6G networks," *Proc. OptoElectronics and Communications Conference (OECC)*, W1A.1. 2021. DOI: 10.1364/OECC.2021.W1A.1

[2] L. J. S. Kumar, P. Krishnan, B. Shreya, and S. M. S, "Performance enhancement of FSO communication system using machine learning for 5G/6G and IoT applications," *Optik*, vol. 252, Feb. 2022. DOI: 10.1016/j.ijleo.2021.168430

[3] R. Harada, N. Shibata, S. Kaneko, T. Imai, J. Kani, and T. Yoshida, "Adaptive beam divergence for expanding range of link distance in FSO with moving nodes toward 6G," *IEEE Photonics Technology Letters*, vol. 34, no. 20, pp. 1061-1064, Oct. 2022. DOI: 10.1109/LPT.2022.3199789

[4] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Societh*, vol. 1, pp. 957-975, July 2020. DOI: 10.1109/OJCOMS.2020.3010270

[5] F. J. L. Martinez, G. Gomez, J. M. G. Balsells, "Physical-layer security in free-space optical communications," *IEEE Photonics Journal*, vol. 7, no. 2, Apr. 2015. DOI: 10.1109/JPHOT.2015.2402158

[6] E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *NPJ Quantum Information*, vol. 2, no. 16025, 2016.

[7] S. Arnon, J. R. Barry, G. K. Karagiannidis, R. Schober, and M. Uysal, eds., Advanced Optical Wireless Communication System. Cambridge Uni. Press., 2012.

[8] Z. Qu and I. B. Djordjevic, "Approaching Gb/s secret key rates in a free-space optical CV-QKD system affected by atmospheric turbulence," *Proc. European Conference on Optical Communication (ECOC)*, P2.SC6.32, 2017. DOI: 10.1109/ECOC.2017.8345986

[9] C. Erven, C. Couteau, R. Laflamme, and G. Weihs, "Entangled quantum key distribution over two free-space optical link," *Optics Express*, vol. 16, no. 21, pp. 16840-16853, 2008. DOI: 10.1364/OE.16.016840

[10] F. Huo and G. Gong, "XOR encryption versus phase encryption, an in-depth analysis," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 4, pp. 903-911, Aug. 2015. DOI: 10.1109/TEMC.2015.2390229

[11] D. L. Hoang, T. H. Tran, Y. Nakashima, "Performance evaluation of 802.11ah physical layer phase encryption for IoT applications," *Proc. International Conference on Advanced Technologies for Communications (ATC)*, pp. 84-88, Oct. 2018. DOI: 10.1109/ATC.2018.8587437

[12] T. Kodama and T. Miyazaki "Demonstration of hardware-effective phase shift-based symbol-masking for secure coherent QPSK system," *Proc. Asia Communications and Photonics Conference (ACP)*, Su2A.92, Nov. 2018. DOI: 10.1109/ACP.2018.8596137

[13] M. A. Khalighi, and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2231-2258, Forthquarter 2014. DOI: 10.1109/COMST.2014.2329501

[14] R. Chen, K. H. Park, C. Shen, T. K. Ng, B. S. Ooi, and M. S. Alouini, "Visible light communication using DC-biased optical filter bank multi-carrier modulation," *Proc. Global LiFi Congress (GLC)*, pp. 1-6, Feb. 2018. DOI: 10.23919/GLC.2018.8319094

[15] H. Wang, B. Liu, Z. Guo, Y. Wan, S. Zhou, Z. Ding, and J. Ren, "High-security OFDM-OAM optical transmission scheme based on quad-wing ultra-chaotic encryption," *IEEE Photonics Journal*, vol. 15, no. 2, Apr. 2023. DOI: 10.1109/JPHOT.2023.3239612

[16] H. Huang, J. Chen, H. Chen, Y. Huang, Y. Li, Y. Song, N. K. Fontaine, R. Ryf, and M. Wang, "Secure free-space optical communication via amplified spontaneous emission (ASE)," *Proc. Optical Fiber Communications Conference and Exhibition (OFC)*, Th1K.3, Mar. 2020. DOI: 10.1364/OFC.2020.Th1K.3

[17] T. Kodama, M. A. B. A. Sanusi, F. Kobori, T. Kimura, Y. Inoue, and M. Jinno, "Comprehensive Analysis of Time-Domain Hybrid PAM for Data-Rate and Distance Adaptive UWOC System," *IEEE Access*, vol. 9, pp. 57064-57074, 2021. DOI: 10.1109/ACCESS.2021.3071467

[18] X. You, J. Chen, Y. Zhong, S. Chen, and C. Yu, "Efficient dimming control with time domain hybrid modulation in indoor hybrid visible light/infrared communication systems," *in Proc. 24th OptoElectronics and Communications Conference (OECC) and 2019 International Conference on Photonics in Switching and Computing (PSC)*, Fukuoka, Japan, pp. 1-3, 2019. DOI: 10.23919/PS.2019.8817648