Free-space optical channel estimation for physical layer security

Hiroyuki Endo,[1,2] Mikio Fujiwara,[1] Mitsuo Kitamura,[1] Toshiyuki Ito,[1] Morio Toyoshima,[3] Yoshihisa Takayama,[3,4] Hideki Takenaka,[3] Ryosuke Shimizu,[5] Nicola Laurenti,[6] Giuseppe Vallone,[6] Paolo Villoresi,[6] Takao Aoki,[2] and Masahide Sasaki[1,*]

[1] *Quantum ICT Laboratory, National Institute of Information and Communications Technology, Koganei, 184-8795, Japan*
[2] *Department of Applied Physics, Waseda University, Shinjuku, 169-8050, Japan*
[3] *Space Communication Systems Laboratory, National Institute of Information and Communications Technology, Koganei, 184-8795, Japan*
[4] *Current affiliation: School of information and Telecommunication Engineering, Tokai University, Takanawa, Minato, 108-8619, Japan*
[5] *Center for Frontier Science and Engineering, the University of Electro-Communications, Chofu, 182-8585, Japan*
[6] *Department of Information Engineering, University of Padova, via Gradenigo 6/B, 35131 Padova, Italy*

[*] *psasaki@nict.go.jp*

Abstract: We present experimental data on message transmission in a free-space optical (FSO) link at an eye-safe wavelength, using a testbed consisting of one sender and two receiver terminals, where the latter two are a legitimate receiver and an eavesdropper. The testbed allows us to emulate a typical scenario of physical-layer (PHY) security such as satellite-to-ground laser communications. We estimate information-theoretic metrics including secrecy rate, secrecy outage probability, and expected code lengths for given secrecy criteria based on observed channel statistics. We then discuss operation principles of secure message transmission under realistic fading conditions, and provide a guideline on a multi-layer security architecture by combining PHY security and upper-layer (algorithmic) security.

OCIS codes: (060.0060) Fiber optics and optical communications; (060.2605) Free-space optical communication.

References and links

1. V. W. S. Chan, "Free-space optical communications," J. Lightwave Technol. **24**(12), 4750–4762 (2006).
2. M. Toyoshima, "Trends in satellite communications and the role of optical free-space communications [Invited]," J. Opt. Netw. **4**(6), 300–311 (2005).
3. S. S. Muhammad, T. Plank, E. Leitgeb, A. Friedl, K. Zettl, T. Javornik, and N. Schmitt, "Challenges in establishing free space optical communications between flying vehicles," in *Proceedings of 6th International Symposium on Communication Systems, Networks and Digital Signal Processing* (2008), pp. 82–86.
4. F. Fidler, M. Knapek, J. Horwath, and W. R. Leeb, "Optical communications for High-Altitude Platforms," IEEE J. Sel. Top. Quantum Electron. **16**(5), 1058–1070 (2010).
5. Facebook, "Connecting the world from the sky," Tech. Rep., Facebook (2014).
6. D. Kedar and S. Arnon, "Urban optical wireless communication networks: the main challenges and possible solutions," IEEE Commun. Mag. **42**(5), S2–S7 (2004).
7. J. C. Juarez, A. Dwivedi, A. R. Hammons, S. D. Jones, V. Weerackody, and R. A. Nichols, "Free-space optical communications for next-generation military networks," IEEE Commun. Mag. **44**(11), 46–51 (2006).

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

8. W. S. Rabinovich, C. I. Moore, R. Mahon, P. G. Goetz, H. R. Burris, M. S. Ferraro, J. L. Murphy, L. M. Thomas, G. C. Gilbreath, M. Vilcheck, and M. R. Suite, "Free-space optical communications research and demonstrations at the U.S. Naval Research Laboratory," Appl. Opt. **54**(31), F189–F200 (2015).
9. M. Agaskar and V. W. S. Chan, "Nulling strategies for preventing interference and interception of free space optical communication," in *Proceedings of IEEE International Conference on Communications* (IEEE, 2013), pp. 3927–3932.
10. A. Puryear and V. W. S. Chan, "Using spatial diversity to improve the confidentiality of atmospheric free space optical communication," in *Proceedings of IEEE Global Communications Conference* (IEEE, 2011), pp. 1–6.
11. M. Eghbal and J. Abouei, "Security enhancement in free-space optics using acousto-optic deflectors," IEEE J. Opt. Commun. Netw. **6**(8), 684–694 (2014).
12. F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," IEEE Photon. J. **7**(2), 7901014 (2015).
13. M. Bloch and J. Barros, *Physical Layer Security: From Information Theory to Security Engineering* (Cambridge University, 2011).
14. X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications* (CRC, 2013).
15. M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," Proc. IEEE **103**(10), 1725–1746 (2015).
16. A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J. **54**(8), 1355–1387 (1975).
17. I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory **24**(3), 339–348 (1978).
18. R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. secret sharing," IEEE Trans. Inf. Theory **39**(4), 1121–1132 (1993).
19. U. M. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory **39**(3), 733–742 (1993).
20. F. Oggier and B. Hassibi, "A perspective on the MIMO wiretap channel," Proc. IEEE **103**(10), 1874–1882 (2015).
21. S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," IEEE Trans. Wireless Commun. **7**(6), 2180–2189 (2008).
22. A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: the MISOME wiretap channel," IEEE Trans. Inf. Theory **56**(7), 3088–3104 (2010).
23. F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," IEEE Trans. Inf. Theory **57**(8), 4961–4972 (2011).
24. N. Wang, X. Song, J. Cheng, and V. C. M. Leung, "Enhancing the security of free-space optical communications with secret sharing and key agreement," J. Opt. Commun. Netw. **6**(12), 1072–1081 (2014).
25. H. Endo, T. S. Han, T. Aoki, and M. Sasaki, "Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels," IEEE Photon. J. **7**(5), 7903418 (2015).
26. X. Sun and I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," IEEE Photon. J. **8**(1), 7901110 (2016).
27. H. Endo, M. Fujiwara, M. Kitamura, T. Ito, M. Toyoshima, H. Takenaka, R. Shimizu, T. Aoki, and M. Sasaki, "Physical layer security in free-space optical communications," IEICE Tech. Rep. **115**(448), 11–15 (2016).
28. G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, and P. Villoresi, "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels," Phys. Rev. A **91**, 042320 (2015).
29. I. Capraro, A. Tomaello, A. Dall'Arche, F. Gerlin, R. Ursin, G. Vallone, and P. Villoresi, "Impact of turbulence in long range quantum and classical communications," Phys. Rev. Lett. **109**, 200502 (2012).
30. J. Proakis and M. Salehi, *Digital Communications*, 5th ed. (McGraw-Hill, 2007).
31. I. I. Kim, B. McArthur, and E. Korevaar, "Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications," in Proc. SPIE **4214**, (2001).
32. W. S. Rabinovich, R. Mahon, H. R. Burris, G. C. Gilbreath, P. G. Goetz, C. I. Moore, M. F. Stell, M. J. Vilcheck, J. L. Witkowsky, L. Swingen, M. R. Suite, E. Oh, and J. Koplow, "Free-space optical communications link at 1550 nm using multiple-quantum-well modulating retroreflectors in a marine environment," Opt. Eng. **44**(5), 056001 (2005).
33. L. C. Andrews, R. L. Phillips, and C. Y. Hopen, *Laser Beam Scintillation with Applications* (SPIE, 2001).
34. P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory **54**(10), 4687–4698 (2008).
35. S. Arisa, Y. Takayama, H. Endo, M. Fujiwara, M. Sasaki, and R. Shimizu, "Coupling efficiency of laser beam to multimode fiber for free space optical communication," in *Proceedings of International Conference on Space Optics* (2014).
36. T. S. Han, H. Endo, and M. Sasaki, "Reliability and secrecy functions of the wiretap channel under cost constraint," IEEE Trans. Inf. Theory **60**(11), 6819–6843 (2014).
37. I. Csiszár, "Almost independence and secrecy capacity," Probl. Peredachi Inf. **32**(1), 48–57 (1996).
38. M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," IEEE Trans. Inf. Theory **57**(6), 3989–4001 (2011).

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

39. I. Csiszár and J. Körner, *Information Theory: Coding Theorem for Discrete Memoryless Systems*, (2nd ed.) (Cambridge University, 2011).

1. Introduction

Free-space optical (FSO) communication is a promising technology for enhancing the connectivity of wireless networks [1], thanks to the features such as wide band width in an unregulated spectrum, ultra-low inter-channel interference, and power-efficient transmission. Potential applications of FSO communication include satellite laser communications [2], a network system comprised of unmanned aerial vehicles, high-altitude platforms or drones [3–5], the last one mile link from the fiber backbone to the clients premises [6] and military applications [7, 8].

As FSO communication becomes more and more important in these applications, the security requirements also become more demanding. Although high directionality of laser beam makes FSO communication inherently more secure than RF counterparts, FSO communication can still suffer from optical tapping risks, especially when the main lobe of laser beam footprint is considerably wider than the receiver size [9–11]. These risks would be pronounced in urban communications where an eavesdropper would hide in the top of the same building as the legitimate receiver [12], or in satellite-to-ground laser communications in which the beam footprint would be a scale of km. Therefore, secure communication over FSO links still remains a challenging task.

Traditionally, security has been highly dependent on the upper layer protocols such as conventional encryption techniques with a pre-shared secret key or a key exchanged via public key cryptosystems. The security of these protocols is proved with algorithmic means. Then, it will be weakened as computer technologies and decryption algorithms are advancing. Moreover, with the rapid growth of the number of communication nodes, the key distribution and management are becoming increasingly difficult, and are introducing larger overhead and latency to the system. During the past few years, however, physical layer (PHY) security [13, 14] has been gaining research attentions as a means to complement conventional encryption techniques. Its security is provided in information theoretical manners based on the particular coding techniques [15–19] or the careful signal designs [20–23]. Different from conventional encryption techniques, no computational assumptions are placed on the eavesdropper. Practically, the existing security system can be enhanced by introducing PHY security as a first line of defense against eavesdropping.

The fundamental theoretical frameworks of PHY security was laid by Wyner [16], and Csiszár and Körner [17] based on secure message transmission over a wiretap channel, and by Ahlswede and Csiszár [18], and Maurer [19] based on secret key agreement from common randomness. In the wiretap channel model, its security is provided by an appropriate channel code guaranteeing both the reliability for the legitimate receiver and the secrecy against the eavesdropper. If the channel from the sender to the eavesdropper is a degraded version of that from the sender to the legitimate receiver, a non-zero secrecy rate can be achieved by sacrificing a fraction of the message rate. While such a degraded condition seems not to be realistic in wired communications, it is more reasonable in FSO communications built up between parties with a direct line-of-sight (LoS). Specifically, in LoS links, surveillance cameras will be able to detect any suspicious activity which makes it harder for an eavesdropper to intercept the main lobe of laser beam. On the perspective of this scenario, there have been theoretical studies [12, 24–26] on the potential of PHY security in FSO communications.

In spite of these remarkable theoretical studies, realization of PHY security is still a challenging issue. In FSO links, the intensity of the transmitted beam and the statistics of the received signals vary in a time scale of ms due to atmospheric turbulences. This kind of fading effect makes it difficult to implement an efficient coding scheme which can ensure PHY security un-

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

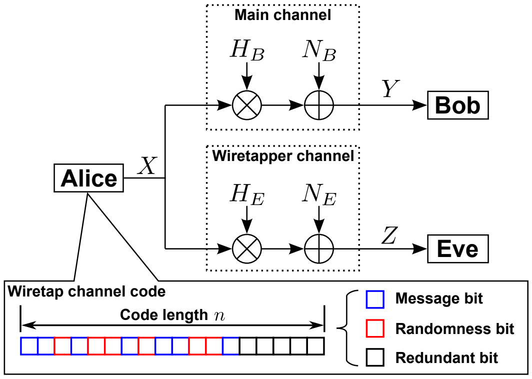

Fig. 1. Schematic diagram of the wireless wiretap channel model and wiretap channel coding [27].

der various conditions. Some approaches to mitigate the effect of atmospheric turbulences have been investigated such as the adaptive real time selection technique [28] in a horizontal quantum communication link of 143 km between La Palma and Tenerife Islands [29]. However, experimental data and analyses on FSO fading links from the viewpoint of PHY security are still overwhelmingly lacking.

This motivates us to collect transmission data in an FSO wiretap channel and analyze them in terms of fundamental metrics of PHY security. To this end, we have constructed a metropolitan terrestrial FSO link testbed (Tokyo FSO Testbed). This testbed consists of one sender terminal and two receiver terminals, one for the legitimate receiver and the other for the eavesdropper. Each of the two is 7.8 km distance apart from the sender terminal. The purposes of the testbed are (1) to examine PHY security techniques (e.g., secure message transmission and secret key agreement) in real-field FSO links, (2) to emulate typical FSO communication scenarios such as satellite-to-ground laser communications, and (3) to accumulate transmission data under several real-field conditions and utilize them for practical system design. In this paper, we focus on secure message transmission and analyze the characteristics of the FSO wiretap channel by transmitting a pseudorandom binary sequence based on on-off keying modulation. Using the output signal statistics, we estimate secrecy rates and related security metrics. We then discuss how the legitimate party can set a guideline for operating secure message transmission based on the observed data with pilot signals and the data accumulated from the past.

2. Wiretap channel and performance metric

Throughout the paper, we consider secure message transmission via a wireless wiretap channel system illustrated in Fig. 1. The sender (Alice) encodes a confidential message into a code word random variable (RV) X^n for transmission over the wiretap channel, where n is the code length. We assume that Alice uses on-off keying modulation, thus RV X takes a value with 0 or the peak power of the transmission laser. Moreover, we also assume that the laser power and the input probability distribution P_X over X are fixed irrespective of the channel state.

The legitimate receiver (Bob) observes the output via a discrete-time quasi-static fading channel (the main channel) given by

$$Y = H_B X + N_B, \tag{1}$$

being H_B the channel gain RV and N_B the additive white Gaussian noise (AWGN) RV. The eavesdropper (Eve) is also capable to observe Alice's transmission from the output via a

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

discrete-time quasi-static fading channel (the wiretapper channel) given by

$$Z = H_E X + N_E, \tag{2}$$

being H_E the channel gain RV and N_E the AWGN RV. Here, upper case letters X, Y, Z, H_B, H_E are all positive real RVs since we modulate intensity of light. For later convenience, we shall use lower case letters x, y, z, h_B, h_E to denote realizations of X, Y, Z, H_B, H_E, respectively.

In order to transmit m bits of confidential information reliably and securely through the wiretap channel, Alice introduces some redundancy to perform error correction and some random dummy information as the cost of additional secrecy. This entails adding redundant bits and l random dummy bits to the code word and hence increasing its length to n as shown in the lower panel of Fig. 1. This scheme is particularly referred to as wiretap channel coding. To design a wiretap channel code of length n, we shall specify two rates, the message rate $R_B = m/n$ and the randomness rate $R_E = l/n$ in bits/letter.

We assume that the channel gains H_B and H_E remain constants h_B and h_E, respectively, during specific interval (coherence interval). In each coherence interval with channel realizations h_B and h_E, one has to satisfy $R_B + R_E \leq I(P_X, P_{Y|X,H_B})$ to establish a reliable communication, where $I(P_X, W)$ is the mutual information with the input probability distribution P_X and the transition probability distribution W, and $P_{Y|X,H_B}$ denotes the transition probability distribution of the main channel. On the other hand, $R_E \geq I(P_X, P_{Z|X,H_E})$ should be satisfied for confidentiality, where $P_{Z|X,H_E}$ denotes the transition probability distribution of the wiretapper channel. Hence, the message rate R_B must satisfy the following relation in each coherence interval,

$$R_B \leq R_{\mathrm{S,i}}(h_B, h_E) \equiv \max[0, I(P_X, P_{Y|X,H_B}) - I(P_X, P_{Z|X,H_E})]. \tag{3}$$

We shall call $R_{\mathrm{S,i}}(h_B, h_E)$ the instantaneous secrecy rate given h_B and h_E. When there is no ambiguity, we will drop the dependence on (h_B, h_E).

In this paper, Bob is assumed to use hard-decision decoding where the value of individual bits are quantized to either $y = 0$ or $y = 1$ based on the threshold y_{th}. Thus, the mutual information $I(P_X, P_{Y|X,H_B})$ is calculated as

$$I(P_X, P_{Y|X,H_B}) = \sum_{x \in \{0,1\}} \sum_{y \in \{0,1\}} P_X(x) P_{Y|X,H_B}(y|x, h_B) \log_2 \left[\frac{P_{Y|X,H_B}(y|x, h_B)}{\sum_{x'} P_X(x') P_{Y|X,H_B}(y|x', h_B)} \right]. \tag{4}$$

In the above equation, the transition probability functions for $y = 1$ and $y = 0$ given by $x \in \{0, 1\}$ are defined as

$$P_{Y|X,H_B}(1|x, h_B) = \frac{N(y \geq y_{\mathrm{th}}|x, h_B)}{N(x)}, \quad P_{Y|X,H_B}(0|x, h_B) = \frac{N(y \leq y_{\mathrm{th}}|x, h_B)}{N(x)}, \tag{5}$$

where $N(x)$ is the number of an input $x \in \{0, 1\}$ transmitted by Alice, and $N(y \geq y_{\mathrm{th}}|x, h_B)$ and $N(y \leq y_{\mathrm{th}}|x, h_B)$ are the numbers of events of $y \geq y_{\mathrm{th}}$ and $y \leq y_{\mathrm{th}}$ conditioned by an input $x \in \{0, 1\}$ in the coherence interval with the channel realization h_B, respectively. The threshold y_{th} should be numerically optimized such that the mutual information $I(P_X, P_{Y|X,H_B})$ is maximized.

On the other hand, Eve is assumed to use soft-decision decoding which uses a whole range of output values to make decisions. This is the reasonable in secure communication, since the mutual information based on soft-decision decoding is slightly larger than that based on hard-decision decoding [30]. In this decoding, considering the finite size of samples (see Appendix A), we quantize the experimental data into K bins with an identical width Δ. Thus, the transition probability function $P_{Z|X,H_E}(z^{(i)}|x, h_E)$ is calculated as follows:

$$P_{Z|X,H_E}(z^{(i)}|x, h_E) = \frac{N(z^{(i)}|x, h_E)}{N(x)}, \tag{6}$$

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

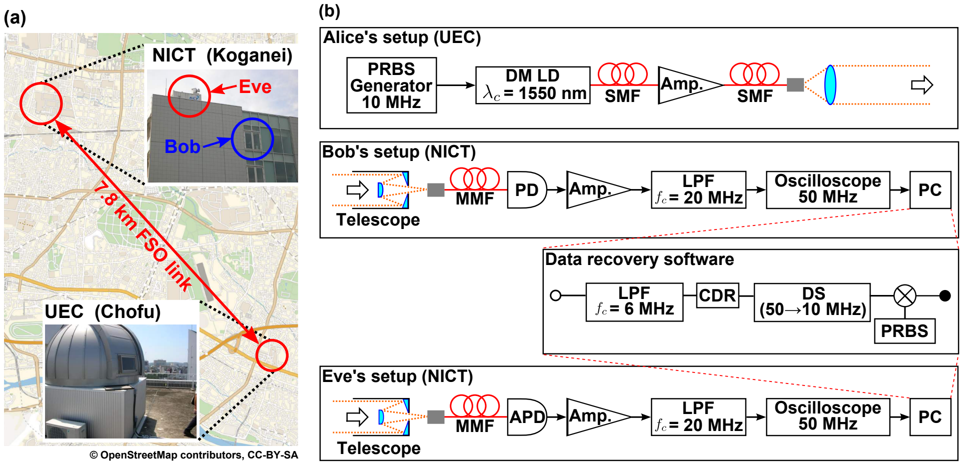

Fig. 2. (a) Overview of Tokyo FSO Testbed. Alice's terminal is installed on a building roof at UEC. Bob's and Eve's terminals are located on a building at NICT. ©OpenStreetMap contributors, CC-BY-SA. (b) Schematic layout of experimental setup of Alice's, Bob's, and Eve's terminals [27].

being $N(z^{(i)}|x,h_E)$ the number of events that z is in i-th bin conditioned by an input $x \in \{0,1\}$ in the coherence interval with the channel realization h_E. The mutual information $I(P_X, P_{Z|X,H_E})$ is calculated as

$$I(P_X, P_{Z|X,H_E}) = \sum_{x\in\{0,1\}} \sum_{i=1}^{K} P_X(x) P_{Z|X,H_E}(z^{(i)}|x,h_E) \log_2 \left[\frac{P_{Z|X,H_E}(z^{(i)}|x,h_E)}{\sum_{x'} P_X(x') P_{Z|X,H_E}(z^{(i)}|x',h_E)} \right]. \quad (7)$$

3. Overview of the experimental setup

The ideal technological goal is to evaluate the instantaneous secrecy rate $R_{\mathrm{S,i}}$ by monitoring the channel state information (CSI), namely, the channel gains of both the main and wiretapper channels, in various conditions depending on weather, temperature, and instruments. However, due to the effect of atmospheric turbulences, the gains H_B and H_E are always fluctuating and hardly predicted. This kind of fading effect makes it difficult to implement an efficient wiretap channel coding scheme under various conditions. This motivates us to collect transmission data in an FSO wiretap channel by using Tokyo FSO Testbed introduced in this section. The testbed and its experimental data allow us not only to analyze the secrecy performance of secure message transmission based on the information-theoretic metrics, but also to determine whether secure message transmission can be established or not under a given condition.

A schematic layout of Tokyo FSO Testbed is shown in Fig. 2(a). We set Alice in an all-weather telescope dome on the rooftop of a building in the University of Electro-Communications (UEC) at Chofu of Japan (35°39′28.8″N, 139°32′39.5″E). In the National Institute of Information and Communications Technology (NICT) at Koganei (35°42′24.2″N, 139°29′19.3″E), we set Bob's receiver in the sixth floor of a building. All optical components are located on a high-precision motorized gimbal. On the rooftop of the building which is just above the sixth floor, we set a container type terminal which takes the role of Eve. This terminal consists of an all-weather scanner on the top of the container. Receiver optics and electronics are located on an optical breadboard inside of the container. These facilities form an FSO link with a straight-line distance of 7.8 km.

In Fig. 2(b), we show an overview of the optical and electrical components in our testbed. The light source is a narrow linewidth direct-modulated laser diode (DM LD, Sense Light Semiconductors DL-BF10-CLS101B-S1550: band width less than 50 kHz at CW operation mode) with a central wavelength λ_c of 1550 nm. This wavelength is selected since it suffers from less free-space attenuation [31] and meets the eye-safety regulations [32]. A signal is in the format of a 10 MHz pseudorandom binary sequence (PRBS) with length of $2^{15}-1$, and the modulation scheme is Non-Return-to-Zero on-off keying. The signal light is coupled into a fiber collimator (aperture diameter of 10 mm and divergence angle of 1.0 mrad) via a single mode fiber (SMF) and expanded into an approximately 5.5 mm beam. The laser is driven by direct modulation mode, and the average output power is set to be 100 mW. The collimator is mounted on a motorized gimbal driven by a high-resolution stepper motor.

At Bob's terminal, a fraction of the signal beam spot whose diameter is approximately 8 m is coupled into a Cassegrain telescope (aperture diameter of 111 mm and focal length of 800 mm) which collimates the beam down into 10 mm in diameter. Then, the beam is focused into a 200 μm multimode fiber (MMF) and finally sent to a photodiode detector (PD, Terahelz Technology Inc. TIA-525 optical receiver) whose noise equivalent power (NEP) is 3.0 pW/$\sqrt{\text{Hz}}$. The total optical loss of Bob's system, including the attenuation due to the window glass, is estimated to be -14dB. At Eve's terminal, the signal beam is tapped with a Cassegrain telescope (aperture diameter of 100 mm and focal length of 2000 mm). The intensity of the beam is measured by an avalanche photodiode detector (APD, Laser Components A-CUBE-I200-10) with higher sensitivity (NEP is 160 fW/$\sqrt{\text{Hz}}$) than Bob's detector. The total optical loss of Eve's system was measured to be -9dB. The comparison of the NEPs of the detectors and the total optical losses between the terminals corroborates that Eve's receiver system is much more sensitive than Bob's one. This fact allows us to emulate a reasonable situation where Eve's receiver is much better than Bob's one. In addition, we can emulate more various wiretap channel conditions by directing Alice's beam to several positions between Bob and Eve.

At both terminals, the photodetector signal is amplified by a preamplifier (Hamamatsu C6438) and then sent to a USB oscilloscope (sampling rate of 50 MHz and bandwidth limit of 20 MHz by a low-pass filter (LPF)) for A/D conversion. Digitized data are then sent to a computer. In order to identify the transmitted signal from the received data, Bob and Eve independently perform an off-line PC-based data recovery process of which the flow chart is shown in the middle panel of Fig. 2(b). First, high frequency noise is filtered out by a LPF (cutoff frequency f_c of 6 MHz) from the input sequence. Then, an accompanying clock signal is generated via a clock data recovery (CDR) process, and the data are down sampled (DS) into 10 MHz of repetition rate by referencing the clock data. Finally, to perform the frame synchronization, cross-correlation between the down sampled data and the original PRBS sequence is calculated. In the experiment, the above-mentioned flow is implemented via LabVIEW.

4. Results and analysis

4.1. Configuration of the experiment

Figure 3 shows our experimental configuration of FSO transmission campaign held on 17 November 2015 under cloudy Tokyo skies. During the experiment, the beam centroid is put in a position closer to Bob's terminal than Eve's one as shown by red circle, such that the received power at Eve would be slightly degraded compared to that at Bob. This geometrical configuration allows us to emulate typical wiretap channel model for satellite-to-ground laser communications where Eve attempts to tap the lobe of the beam footprint. Although our horizontal link cannot precisely emulate the realistic fading-induced scintillation in the vertical link of satellite-to-ground laser communications (the former is in one atmospheric layer while the latter is affected by several atmospheric layers with different scintillation effects), we can derive

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

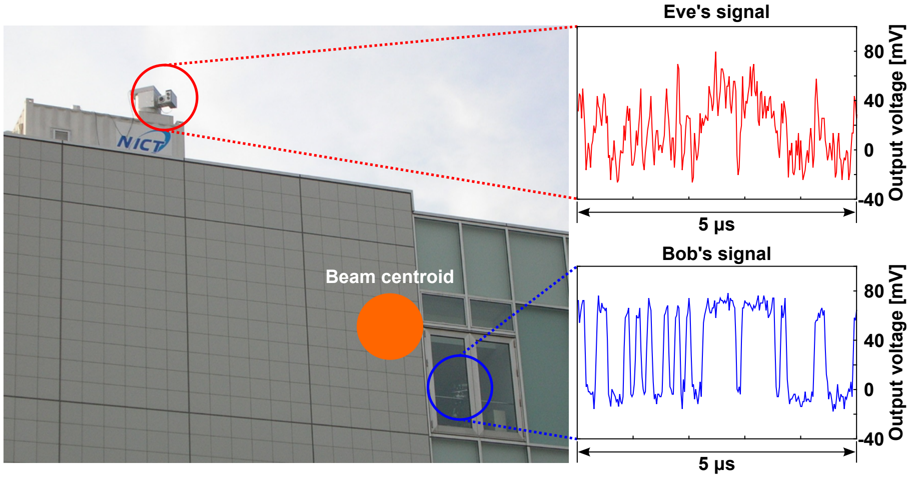

Fig. 3. Experimental configuration of FSO transmission campaign held on 17 November 2015, and typical waveforms received by Eve (upper) and Bob (lower) over 5 μs. The data are taken at 14:43:00 JST. In the figure, we subtracted the DC offset of a detector from the received signal.

the basic principles of the channel estimation and the design of secure message transmission systems for a generic FSO link.

We conducted the experiments in 5 time periods, namely, 14:43 - 14:46, 15:57 - 16:00, 16:33 - 16:36, 17:37 - 17:40, and 18:10 - 18:13 in JST. We note that 16:33 JST was the sunset time on the day. In each time period, we made 10 times of transmission and 2×10^6 bits of the PRBS are transmitted in each transmission with 200 ms duration. To characterize the instantaneous secrecy rate $R_{\mathrm{S,i}}$, we divide the duration of each 200 ms transmission into 50 of the 4 ms slot which includes 2×10^5 samples corresponding to 4×10^4 bits. In this time slot, the channel realizations h_B and h_E seem to be roughly constant hence the coherence time of the fading channels is in the order of ms. Moreover, samples of statistically sufficient size are included in the duration. The effect of atmospheric turbulence is nicely captured as the variation of the instantaneous secrecy rate at each time slot.

In this transmission campaign, we observed a pointing deviation of the received peak power, which can be compensated by rearranging the angles of the receiver telescopes every hour. We observed a typical deviation rate of 0.2 mrad/hour, which may be attributed to the refraction effect due to the varying and nonuniform air temperature and to the thermal expansion of the building in which the two receivers are located. In the time scale of each transmission (a few minutes), the FSO link stays in the same condition.

4.2. Temporal variation of instantaneous secrecy rate

In Fig. 4, we show the temporal variation of the instantaneous secrecy rate $R_{\mathrm{S,i}}$ (solid line) and the average output voltage (dotted line) for the typical 200 ms FSO transmission at 17:37:00 JST, in the late evening time about an hour after the sunset. This time period is a typical case where the fading-induced scintillation is not so heavy. Actually, the highest rate (8.30 Mbits/second (Mbps), from 12 ms to 16 ms) and the lowest rate (5.25 Mbps, from 76 ms to 80 ms) are not so far different (Taking into account the 10 MHz repetition rate of the input, Bob would gain 10 Mbps of information if Eve was absent.). Moreover, the fluctuation of the average output voltage at Bob (dotted line) seems not to have a direct correlation with the instantaneous

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

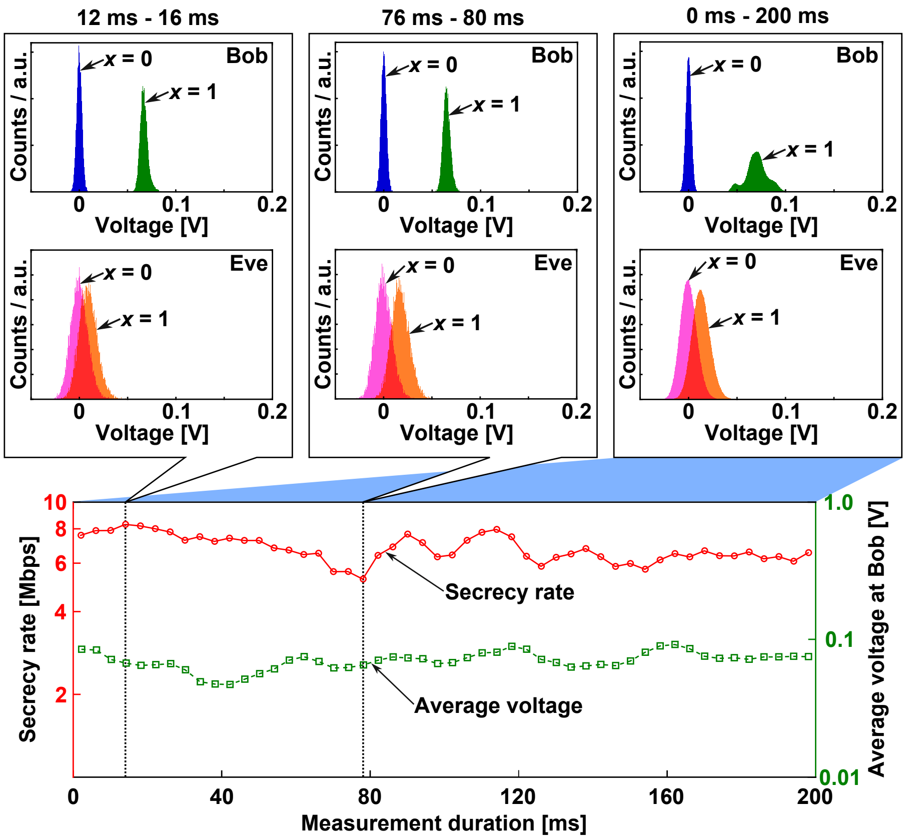

Fig. 4. Temporal variation of instantaneous secrecy rate $R_{S,i}$ (solid line) and the average output voltage (dotted line) for the experimental data at 17:37:00 JST, the late evening time about an hour after the sunset, on 17 November 2015. In each time slot, the measurement duration is 4 ms and 4×10^4 bits are contained. Two upper left insets are the histograms of the output voltage for the best case (between 12 ms and 16 ms) and the worst case (between 76 ms and 80 ms). The upper rightmost inset is the output voltage histogram for the whole period of the 200 ms transmission. Width of histogram bins are 0.3 mV both for Bob's and Eve's data (see Appendix A). In the histogram, we subtracted the DC offset of the detector from the received signal.

secrecy rate $R_{S,i}$ (solid line).

In the two left upper insets of Fig. 4, we show the histograms of the output voltage of the detectors for the best and worst cases. Clearly, the two peaks in Eve's received power histograms overlap with each other while the peaks in Bob's one are perfectly separated in both insets. It turns out that under the condition of this time period, we can potentially transmit at most 5.25 Mbps of information with perfect secrecy. We also show the histograms of the output voltage for the whole period of 200 ms transmission in the upper rightmost inset of Fig. 4. The spectra of these histograms are not so broader even compared to those of 4 ms time slot. In general, the stronger the light fluctuation is, the broader the spectrum of the intensity distribution becomes [33], but Fig. 4 is not the case.

Figure 5 shows the temporal variation of the instantaneous secrecy rate $R_{S,i}$ (solid line) and the average output voltage (dotted line) for the typical 200 ms FSO transmission at 16:34:20

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

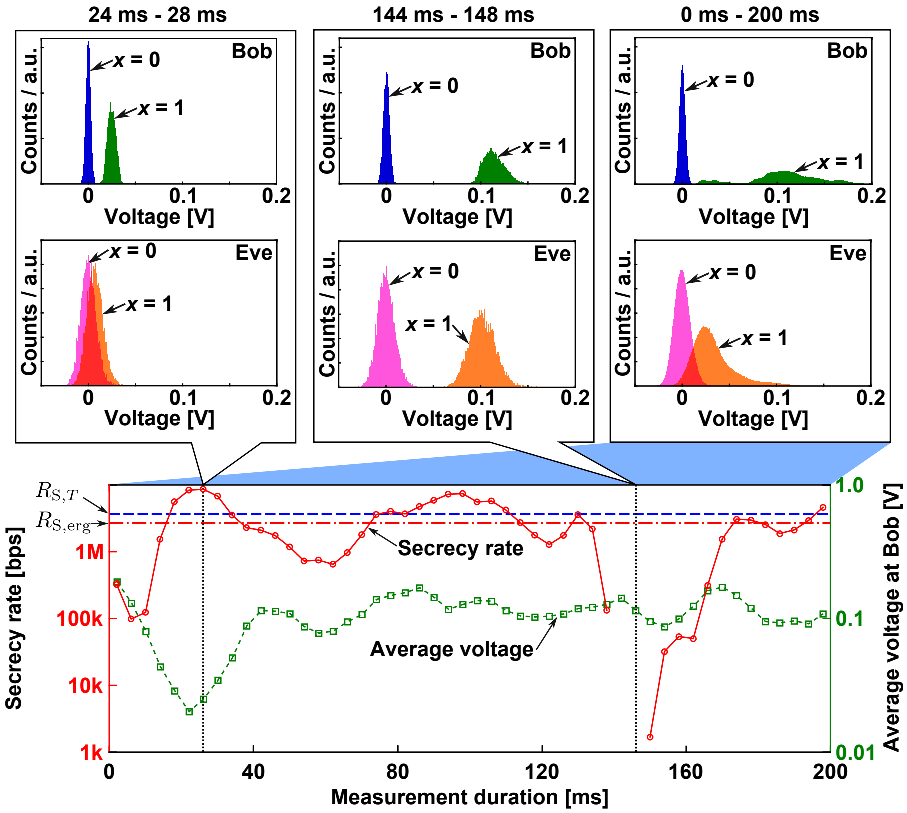

Fig. 5. Temporal variation of instantaneous secrecy rate $R_{\mathrm{S,i}}$ (solid line) and the average output voltage (dotted line) for the experimental data at 16:34:20 JST, just one minute after the sunset time, on 17 November 2015. In each time slot, the measurement duration is 4 ms and 4×10^4 bits are contained. For comparison, the ergodic secrecy rate $R_{\mathrm{S,erg}}$ (chain line) and the long span secrecy rate $R_{\mathrm{S,T}}$ (dashed line) are also shown. Two upper left insets are the histograms of the output voltage of the detectors for the best case (between 24 ms and 28) and the worst case (between 144 ms and 148 ms). The upper rightmost inset is the output voltage histogram for the whole period of the 200 ms transmission. Width of histogram bins are 0.3 mV both for Bob's and Eve's data. In the histogram, we subtracted the DC offset of the detector from the received signal.

JST, just one minute after the sunset time. Contrary to Fig. 4, the difference between the best case (8.75 Mbps, from 24 ms to 28 ms) and the worst case (0 bps, from 144 ms to 148 ms) is much more distinct. For the best case, the signal via the main channel is quite distinguishable while that via the wiretapper channel is hardly distinguished as seen in the upper left inset. On the other hand, around the time slot of the worst case, the instantaneous secrecy rate decreases suddenly. This is because the wiretapper channel is error-free and hence Eve can establish a reliable channel from Alice. It is estimated that the beam centroid should have suddenly been gotten closer to Eve's one. The output voltage histograms for the whole period of the 200 ms transmission are shown in the upper-right inset of Fig. 5. Compared to the one in Fig. 4, their shapes are much broader or heavy-tailed. This means that the atmospheric turbulences in this time period are much more pronounced than that in the late evening time. Similar to Fig. 4, the variations of Bob's average output voltage (dotted line) seem not to have a direct correlation

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

with the instantaneous secrecy rate $R_{\mathrm{S,i}}$ (solid line). Therefore, even in the present receiver configuration, based on the Eve-near-Bob scenario in [12], the possible spatial correlation between Eve's and Bob's channels does not show a significant impact on the secrecy rate.

Figures 4 and 5 indicate that Alice and Bob should find good atmospheric conditions so as to avoid a sudden fatal information leakage. If there is a good correlation between Bob's and Eve's observations on some straightforward measure, such as the average output voltages, then Alice and Bob could roughly infer an attainable secrecy rate (or its lower bound) by looking only at output voltage of Bob's detector. Unfortunately, however, no good correlation between the secrecy rate and Bob's average output voltage was seen in Figs. 4 and 5. One way is to use Bob's output voltage histograms which are measured for a longer time (e.g., 200 ms like as in Figs. 4 and 5) than a fading time scale as the partial CSI. If the histogram is broader, the secrecy rate varies and the fatal information leakage would occur, implying that Alice and Bob should avoid from such durations. Thus Alice and Bob can use appropriate pilot signals, compare the histogram with accumulated data, and opportunistically choose good time durations like Fig. 4.

4.3. Code word over a longer time span

Even in the larger fading case like Fig. 5, if a fast feed-forward mechanism could be employed, one might be able to use an appropriate wiretap channel code, adapting changes of the channel states due to fading-induced scintillation. This is, however, technically challenging.

Another possibility is to find a good code appropriately designed for the observations over a longer time span, just as shown in the upper rightmost inset in Fig. 5. To distinguish these long span transition probabilities from instantaneous ones, we shall call the former the long span transition probabilities, and denote them as $\mathrm{E}[P_{Y|X,H_B}]$ and $\mathrm{E}[P_{Z|X,H_E}]$ for Bob's and Eve's channels, respectively. They are actually statistical mixtures of the instantaneous channel transition probabilities of Eq. (6) and have much wider spread in distribution.

We can then calculate the secrecy rate for these long span transition probabilities as

$$R_{\mathrm{S,T}} \equiv I(P_X, \mathrm{E}[P_{Y|X,H_B}]) - I(P_X, \mathrm{E}[P_{Z|X,H_E}]), \tag{8}$$

which we call the long span secrecy rate. The value of $R_{\mathrm{S,T}}$ (3.71 Mbps) is shown as the dashed line in Fig. 5. As seen, the long span secrecy rate $R_{\mathrm{S,T}}$ itself remains reasonably high, even though there appear fatal decreases of the instantaneous secrecy rates in the observed time span. In such fatal regions, Eve's channel remains error-free as shown in the upper middle inset. The result of the long span secrecy rate implies that there exists a good code to deceive Eve even in such a situation provided that the channel states remain as they are in Fig. 5 for an even longer period such that the channel can be used many times with such a good code. For example, one may spread a message onto a code word over the long spanned observation with sufficient randomization, and attain the secrecy even under the fading like in Fig. 5.

Interestingly, under the assumption that both the input probability distribution P_X and the input power are fixed over the whole time period and the main channel is almost error-free, the long span secrecy rate $R_{\mathrm{S,T}}$ is slightly larger than the ergodic secrecy rate $R_{\mathrm{S,erg}}$ (see Appendix B) which is just defined as the average of the instantaneous secrecy rates

$$R_{\mathrm{S,erg}} \equiv \mathrm{E}[R_{\mathrm{S,i}}(h_B, h_E)], \tag{9}$$

and is often used to see an overall throughput in fading channels [34]. The value of $R_{\mathrm{S,erg}}$ (2.77 Mbps) is shown as the chain line in Fig. 5 and corroborates the above point. In order to achieve the ergodic secrecy rate $R_{\mathrm{S,erg}}$, one should employ a fast feed-forward mechanism to adapt changes in a fading channel, which is technically challenging, as stated above. Thus the transmission of a code word over a longer time span would be more attractive as fading-resistant techniques.

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

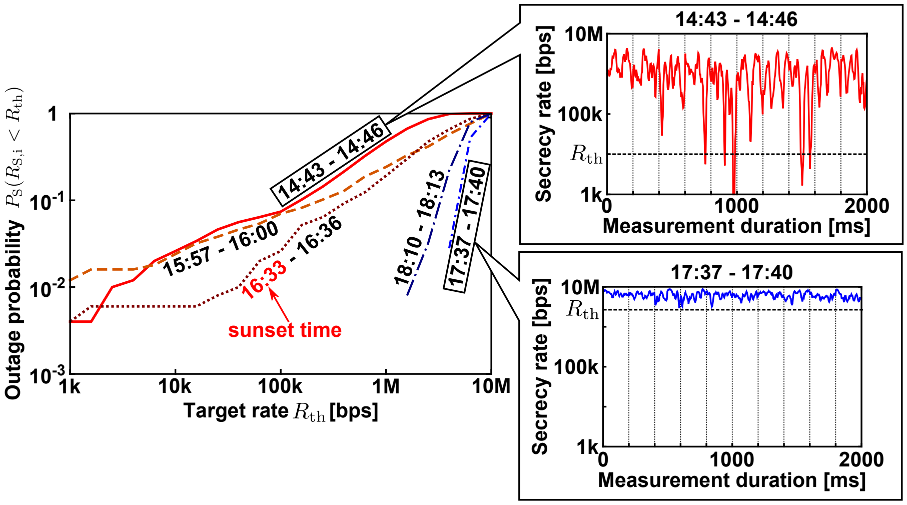

Fig. 6. Secrecy outage probability $P_S(R_{S,i} < R_{th})$ as a function of target rate R_{th} for 5 campaign periods on 17 November 2015. In each time period, 10 independent 200 ms FSO transmissions (totally 20 Mbits), namely, 500 of 4 ms FSO transmission is contained.

Table 1. Mean values of the scintillation index σ_I^2 and refractive-index structure constant C_n^2 for each campaign period[a].

Campaign period	Mean σ_I^2	Mean C_n^2 $[\mathrm{m}^{-2/3}]$
14:43 - 14:46	0.076	2.17×10^{-16}
15:57 - 16:00	0.408	1.16×10^{-15}
16:33 - 16:36 (sunset time)	0.168	4.79×10^{-16}
17:37 - 17:40	0.034	9.69×10^{-17}
18:10 - 18:13	0.044	1.26×10^{-16}

[a] To calculate σ_I^2 and C_n^2 in this table of each 200 ms transmission, we selected the event where the light source is on.

4.4. *Secrecy outage probability*

In the previous subsection, we observed that the received signal statistics of the long term transmission serves as a partial CSI of the wiretap channel. Alice and Bob can utilize this to determine whether they conduct secure message transmission or not. However, they may dare to perform secure message transmission even with compromising the confidentiality. In such a situation, a natural question arisen is then how is the trade-off relation between the throughput and the risk of information leakage. In this case, the secrecy outage probability provides a quantitative metric.

The secrecy outage probability $P_S(R_{S,i} < R_{th})$ is defined as the cumulative probability that an instantaneous secrecy rate $R_{S,i}$ is smaller than a given target rate R_{th}. This outage probability quantifies how often fatal information leakage occurs when the wiretap channel code is employed at constant rate R_{th}. Obviously, the secrecy outage probability is a monotone increase function of target rate R_{th}, which indicates the trade-off relation between security and throughput.

Figure 6 depicts the outage probability $P_S(R_{S,i} < R_{th})$ for 5 campaign periods. In each time period, 10 independent 200 ms transmissions (totally 20 Mbits) are contained. The instanta-

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

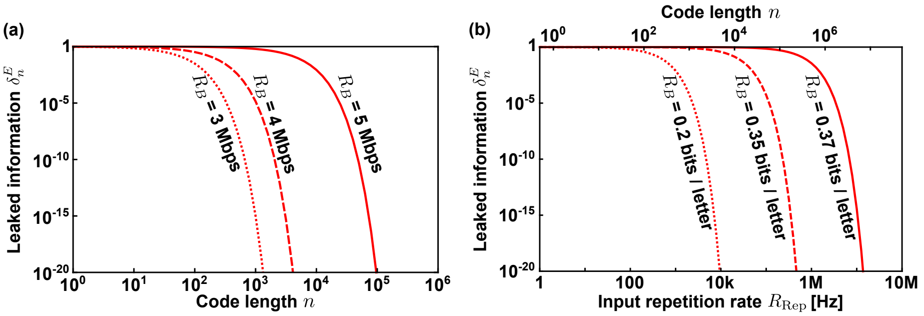

Fig. 7. (a) Code length dependence of leaked information measure δ_n^E between 76 ms and 80 ms in Fig. 4. (b) Repetition rate dependence of leaked information measure δ_n^E over the whole observation time of 200 ms in Fig. 5.

neous rate $R_{\mathrm{S,i}}$ is calculated in the duration of 4 ms. The time variations of the instantaneous secrecy rate are illustrated in right panels for 14:43 - 14:46 JST and 17:37 - 17:40 JST.

The behavior of the outage probability shown in Fig. 6 is well reflected in the behaviors of the scintillation index σ_I^2 and the refractive-index structure constant C_n^2 [33] shown in Table 1. For example, before the sunset time, C_n^2 indicates a larger value over 10^{-16}. On the other hand, one hour after the sunset time (17:37 - 17:40), C_n^2 becomes the smaller value below 10^{-16}, and C_n^2 turns to be a slightly larger value after further 30 minutes later (18:10 - 18:13). Such a temporal suppression of fading-induced scintillation one hour after the sunset time has already been observed in the past experiment held in NICT [35].

As shown in Fig. 6, the secrecy outage probability is almost negligible even when the target rate is set to be more than 1 Mbps in the late evening time (17:37 - 17:40), meaning that the perfect secure transmission at high throughput is possible. On the other hand, before the sunset time (14:43 - 14:46), the outage probability still remains to be 0.01 even if the target rate decreases to 10 kbps. Such kind of larger outage probability alerts that the perfect secrecy cannot be guaranteed solely by the wiretap channel code with $R_{\mathrm{th}} = 10$ kbps. It advices that some backup encryption schemes in the upper layers should be activated to prepare for the worst case scenario.

4.5. *Finite length analysis*

Although the secrecy rate is regarded as a reasonable benchmark of the system, it concerns only the asymptotic limit at code length $n \to \infty$. Practically, in the bounded-code-length scenario, the message rate R_B cannot be arbitrarily close to the secrecy rate as well as the information leakage cannot be completely diminished. Thus, in order to design a practical code with the perfect secrecy, the message rate R_B should be chosen much lower than the secrecy rate and the necessary code length n for the required secrecy criteria should be known. This motivates researchers [36–38] to introduce the secrecy exponent $H_{\mathrm{sec}}(R_E)$ (see Appendix C), which is a stronger characterization showing how fast the leaked information decreases. Actually, in [25], through the upper bound on the leaked information measure $\delta_n^E \le e^{-nH_{\mathrm{sec}}(R_E)}$, where the leaked information measure δ_n^E is measured by a statistical distance between distributions [25, 36], the code length dependence of δ_n^E has been investigated in the idealistic fading free model, or constant channel gain model. In what follows, we consider the application of $H_{\mathrm{sec}}(R_E)$ on atmospheric fading channels.

First, we consider the case with the weaker fading case, such as in Fig. 4. In this case, the

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

fluctuation of the instantaneous secrecy rate is also weak. We may select the worst time slot, design a code for it, and apply it for the whole interval such as 200 ms in Fig. 4. Now, our purpose is to investigate what code length is required in this time slot. In Fig. 7(a), we show the code length dependence of the leaked information criteria δ_n^E on the time slot of the worst case (from 76 ms to 80 ms) in Fig. 4. Clearly, as R_B decreases (or the randomness rate R_E increases, since we assume that sum of the rates $R_B + R_E$ is fixed), δ_n^E decreases faster, attaining a given criterion δ_n^E with a shorter code length. When Alice and Bob set R_B to be 3 Mbps (the dotted line in Fig. 7(a)), $\delta_n^E < 10^{-20}$ can be obtained by a code with $n = 10^3$. Since this value serves as the upper bound over the whole time period, Alice and Bob reasonably achieve the secure message transmission with fixing the message rate $R_B = 3$ Mbps and the code length $n = 10^3$. For the curve of $R_B = 4$ Mbps (dashed line), the required code length for $\delta_n^E < 10^{-20}$ is $n = 10^4$ and still reasonable. On the other hand, as we raise the rate up to $R_B = 5$ Mbps (solid line), which is close to the instantaneous secrecy rate $R_{\mathrm{S,i}} = 5.25$ Mbps (see Fig. 4), $n = 10^5$ of code word is required for $\delta_n^E = 10^{-20}$. However, considering that the repetition rate is 10 MHz and the time slot duration is 4 ms, this code length is out of a consistent design.

Next and finally, we discuss finite length analysis in the larger fading case like in Fig. 5. In Subsection 4.3, we have already discussed a fading resistant technique based on a code word over a longer time span, i.e., the whole observation time of 200 ms. The input repetition rate was set as 10 MHz. This means that there are 2×10^6 symbols in the whole span, and the code length is also 2×10^6. This length is however, considerably long, and readily causes large coding complexity. To reduce such complexity, one must set a lower repetition rate R_{rep} for a fixed observation time T_{O}, where the code length n is determined as $n = R_{\mathrm{rep}} T_{\mathrm{O}}$. Figure 7(b) shows how fast the leaked information criteria δ_n^E decreases as the repetition rate R_{rep} for a given message rate $R_B = m/n$. As easily imaged, if the larger message rate is required, the repetition rate must be higher for attaining a given level of secrecy, and hence the code length should also be longer according to $n = R_{\mathrm{rep}} T_{\mathrm{O}}$. Suppose that we set the secrecy criteria as $\delta_n^E < 10^{-20}$. Then for a message rate $R_B = 0.2$ bits/letter, the repetition rate and the code length must be set roughly as $R_{\mathrm{rep}} = 10$ kHz and $n = 2 \times 10^3$, respectively, which realizes the secure message transmission at 2 kbps. For a higher message rate $R_B = 0.37$ bits/letter, the repetition rate and the code length should be $R_{\mathrm{rep}} = 13.8$ MHz and $n = 2.77 \times 10^6$, respectively, realizing the 5.13 Mbps secure message transmission.

5. Concluding remarks

In this paper, we have discussed the feasibility of PHY security in real-field FSO links. Using Tokyo FSO Testbed, we could gather the experimental data for various atmospheric conditions which will meet satellite-to-ground laser communications. We exploited three information theoretical quantities as performance measures, the secrecy rates, the secrecy outage probability and the expected code lengths for given secrecy criteria. We observed that the real conditions influence the temporal variation of the instantaneous secrecy rate; the temporal variation is stable in the late evening time, whereas it is much stronger before the sunset time. When the variation of secrecy rate is stable, Alice and Bob can establish the secure message transmission with reasonable code lengths. On the other hand, when the variation of secrecy rate is much heavier, Alice and Bob can assess the possibility of secure message transmission using a good and longer code designed based on the long span statistics of the channel. Quantitatively, they can calculate the probability of the fatal information leakage via the secrecy outage probability. Combining the PHY security with upper-layer cryptographic schemes, they may be able to establish secure communication even in the heavy fading condition.

In this paper, we mainly focused on the secure message transmission via the wiretap channel. As was stated, the opportunistic transmission may be impractical in the configuration of this

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

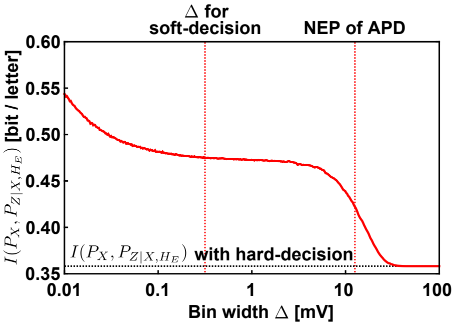

Fig. 8. Bin width dependence of the mutual information $I(P_X, P_{Z|X,H_E})$ for the time slot from 76 ms to 80 ms in Fig. 4.

paper since a fast adaptive optimization over input probability distribution, input power, and message rate is required. However, in the delay tolerant communication such as secret key agreement [18, 19] using public channels, this opportunistic approach will work effectively. In secret key agreement, Alice and Bob can opportunistically select appropriate time slots after sharing initial randomness, and apply information reconciliation and privacy amplification to the data in these time slots. Moreover, the secrecy rate gives a lower bound for the achievable secret key rate. The experimental result gathered via Tokyo FSO Testbed campaign tells us that the implementation of secret key agreement scheme in this testbed is straightforward. Thus, the feasibility study of this scheme in real field FSO communications will be a next target of this campaign.

With a direct analysis, this study provides quantitative assessment of the key rate reduction from the eavesdropper in real channel conditions. This is a strong support for the further study of this effect with a mobile attack, as for instance in the case of Eve on a drone. Moreover, although our results were obtained in horizontal terrestrial propagation, we believe that our feasibility study is a first step towards a realization for large-scale deployment of PHY security in FSO communication. PHY security in FSO communication will open a new paradigm for the basis of high-capacity and high-altitude secure communications exploiting satellites, air planes and drones.

Appendix A: Bin width Δ for evaluating $I(P_X, P_{Z|X,H_E})$ with soft-decision decoding

In this appendix, we discuss the bin width Δ for evaluating the mutual information $I(P_X, P_{Z|X,H_E})$ based on soft-decision decoding. The bin width for Bob's output voltage histogram (Figs. 4 and 5) was also determined by the same procedure.

Ideally, one should make the bin width Δ as finely as possible. In practice, however, the finite sample size of experimental data sets the lower bound on allowed values of Δ. To determine such a lower bound, we investigate the bin width dependence of the mutual information $I(P_X, P_{Z|X,H_E})$ in Fig. 8. For large Δ, $I(P_X, P_{Z|X,H_E})$ stays at a constant value which corresponds to the value for hard-decision decoding. On the other hand, as Δ decreases, the curve starts climbing steadily at 20 mV, and then reaches a plateau around at $I(P_X, P_{Z|X,H_E}) = 0.475$ bit per letter, the value for soft-decision decoding. Note that the noise equivalent power (NEP) of Eve's APD, 12 mV, is located in the slope of this increase. As Δ decreases further, $I(P_X, P_{Z|X,H_E})$ turns to increase again at around 0.3 mV. This is due to the lack of sample size, namely, one can artificially construct non-overlap distributions for the input signals 0 and 1, which is of course a fake. Hence, we adopt 0.3 mV as the bin width Δ which is neither too large not to underestimate $I(P_X, P_{Z|X,H_E})$ nor too small to mitigate the effect of limited sample size.

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016

Appendix B: Superiority of $R_{\mathrm{S,T}}$ over $R_{\mathrm{S,erg}}$

In this appendix, we show that under the condition that both the input probability P_X and input power are fixed over all coherence interval, and the main channel is almost error free, the long span secrecy rate $R_{\mathrm{S},T}$ outperforms the ergodic secrecy rate $R_{\mathrm{S,erg}}$.

As is well known [39], the mutual information $I(P,W)$ is a convex function of transition probability W with the fixed input probability distribution P. Thus, the following inequality holds from the Jensen's inequality [39];

$$\mathrm{E}[I(P,W)] \geq I(P,\mathrm{E}[W]). \tag{10}$$

Using this inequality, we have

$$\begin{aligned} R_{\mathrm{S,erg}} &= \mathrm{E}[I(P_X, P_{Y|X,H_B}) - I(P_X, P_{Z|X,H_E})] && (11)\\ &\leq I(P_X, \mathrm{E}[P_{Y|X,H_B}]) - I(P_X, \mathrm{E}[P_{Z|X,H_E}]) && (12)\\ &= R_{\mathrm{S,T}}, && (13) \end{aligned}$$

where Eq. (12) follows from the assumption that Bob's channel is almost error-free and applying Eq. (10) on $I(P_X, P_{Z|X,H_E})$.

Appendix C: Definition of secrecy exponent

In this appendix, we give the definition of the secrecy exponent $H_{\mathrm{sec}}(R_E)$. The secrecy exponent $H_{\mathrm{sec}}(R_E)$ is defined as

$$H_{\mathrm{sec}}(R_E) \equiv \max_{0\leq\rho<1} \left(\phi(-\rho|P_{Z|X,H_E}, P_X) + \rho R_E \ln 2\right), \tag{14}$$

where

$$\phi(-\rho|P_{Z|X,H_E}, P_X) \equiv -\ln \sum_{i=1}^{K} \left(\sum_{x=\{0,1\}} P_X(x) P_{Z|X,H_E}(z^{(i)}|x,h_E)^{\frac{1}{1-\rho}} \right)^{1-\rho}, \tag{15}$$

with $0 \leq \rho < 1$.

The secrecy exponent $H_{\mathrm{sec}}(R_E)$ is monotone strictly positive increasing in $R_E > I(P_X, P_{Z|X,H_E})$ and becomes 0 for $R_E \leq I(P_X, P_{Z|X,H_E})$. This is the manifestation of the tradeoff relation between information rate and secrecy [36]: namely, for more secure communication, one should increase R_E for the price of sacrificing the information rate R_B.

Acknowledgment

This work was funded by ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan). The authors gratefully acknowledge inspiring discussions with Prof. Ryutaroh Matsumoto and Dr. Masahiro Takeoka.

#259736 Received 24 Feb 2016; revised 1 Apr 2016; accepted 3 Apr 2016; published 14 Apr 2016