Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

A perfect secure optical-network with an anti-correlated noise

Il-Pyeong Hwang [a], Chang-Hee Lee [a,b,*]

[a] School of Electrical Engineering, KAIST—Korea Advanced Institute of Science and Technology, Daejeon 34141, Republic of Korea
[b] Liangjian International College, CQUT—Chongqing University of Technology, Chongqing 401135, P.R. China

ARTICLE INFO

Keywords:
Optical secure network
Perfect secrecy
Anti-correlated noise
Wiretap channel

ABSTRACT

We propose a perfect secrecy optical communication with an anti-correlated noise between wavelength-division-multiplexed (WDM) channels. The anti-correlated noise carries confidential information. By sending the different WDM channels to different communication paths in optical communication networks (wired and/or wireless), the achievable signal-to-noise ratio for eavesdroppers can be restricted to much less than that of a target receiver. We demonstrate a perfect secrecy optical network with a three-channel anti-correlated noise generated by using a Fabry–Perot laser diode and a broadband light source. The secure data-rate of 3.95-Gb/s was achieved against an eavesdropper on a single path. We also investigate a secrecy capacity as a function of the number of eavesdropped paths. Finally, security enhancement methods for the proposed system are introduced.

1. Introduction

The secure information exchange has been one of the most important requirements for communication networks. Recently, the secure communication has been received considerable attention due to emergence of super-computing machines including quantum computers. Since the computing machine can decipher any enciphered data using current mathematical encryption algorithms such as Riverst Sharmir Adleman (RSA), Data Encryption Standard (DES), and Advanced Encryption Standard (AES) within limited time, it is expected to cause social unrest [1,2]. To protect information against enemies who have the computing power, it is mandatory to care not only higher communication layers, but also the physical layer, and then cut off the information flow to them.

There are many strategies to keep the secure communication in physical layer, including signal concealing (steganography), enciphering/deciphering (cryptography, or coding), channel monitoring, and using channel capacity difference. The steganography is a technology that conceals the confidential information into legacy communication data or transmission [3–5]. For example, concealing the confidential information into amplified-spontaneous emission (ASE) noise of a legacy communication channel was proposed [6]. This strategy is efficient for an enemy who does not recognize the trick [7,8]. For the cryptography, optical code-division multiple access (Optical CDMA) can be an example [9]. In this method, communicators use a pre-shared code for encoding/decoding of the confidential information. Particularly, in physical layer secure communication, physical parameters can be the part of code such as path delay of channels, dispersion, wavelength, and etc [10,11]. This strategy is computationally secure related with complexity of the pre-shared code [12]. For the channel monitoring, quantum key distribution (QKD) is well known approach [13–15]. Based on the quantum mechanics, existence of an eavesdropper can be detected by monitoring the transmitted quantum state. Then, secure keys can be shared, when the channel is safe. Currently, there are many researches to overcome practical challenges of QKD for applications [16], including rate-distance limit [17–19], and cost-efficiency [20].

Meanwhile, to limit information to an eavesdropper, the wire-tap channel theory has been intensively considered, which uses channel capacity difference between a target communication receiver and an eavesdropper [21]. When the target receiver has a better signal-to-noise ratio (SNR) (or channel capacity = maximum mutual information) than that of an eavesdropper, we can achieve secrecy in communication with a secrecy capacity. When the positive secrecy capacity is maintained during the entire communications process, the communicators can keep the secrecy of the exchanged information against any eavesdropper. And then this secure state on the information is represented as perfect secrecy [21,22].

However, in most case, the eavesdropper can obtain a higher SNR than the target receiver, as this entity is in between the communicator's channel, and then less affected by channel impairment. In addition, the eavesdropper may also have higher performance devices. Fortunately, we can degrade the eavesdropper's channel capacity by transmitting artificial noise to some places where an eavesdropper is expected [23,24]. Nevertheless, the system cannot guarantee the communication security, because it is not always possible to predict the eavesdropper's location.

[*] Corresponding author at: School of Electrical Engineering, KAIST—Korea Advanced Institute of Science and Technology, Daejeon 34141, Republic of Korea.
E-mail addresses: jpsqlove@kaist.ac.kr (I.-P. Hwang), changheelee@kaist.edu (C.-H. Lee).

https://doi.org/10.1016/j.optcom.2020.125649
Received 20 January 2020; Received in revised form 27 February 2020; Accepted 28 February 2020
Available online 3 March 2020

To be sure the perfect secrecy regardless of the eavesdropper's location, an anti-correlated noise based secure communications were proposed [25,26]. The confidential information is imposed on 'M'-channel anti-correlated noise and is distributed on multiple paths in a communication network (wired and/or wireless). It should be noted that a lower SNR to any eavesdropper who has signals from less than 'M' channels is assured because of the characteristics of the anti-correlated noise, while the target receiver has a high SNR than the eavesdropper. Thus, we can achieve perfect secrecy in the communication [21,22].

This paper is extended investigation of the proposed method [25,26]. The secrecy capacity was theoretically investigated as a function of the number of eavesdropped paths, for the first time. We also experimentally demonstrate a perfect secrecy optical-network with a 'three'-channel anti-correlated noise from a Fabry–Perot laser diode (F–P LD) that spontaneous emission sources are injected into. The system is realized with commercial components, including a Fabry–Perot laser diode and a broadband light source. The secrecy capacity of 3.95 Gb/s is achieved against a single eavesdropper. In addition, a security enhancement method using bidirectional communication is proposed. We show that the bidirectional communication can provide additional secrecy capacity with the same number of channels. When an eavesdropper has all signals from the 'M' channels, the proposed method is computationally secure. To improve the security in this case, some signal encryption methods using physical phenomena can be adopted, such as path delay, phase modulation, intensity modulation, and optical nonlinear effects. In this paper, we analyze the path delay and phase modulation effects on the computational complexity. Based on our analysis, we expect that the computational complexity of 2^{281} can be achievable with our proposed method.

2. Operation principle

2.1. Theoretical background – Secrecy capacity and perfect secrecy

When Alice wants to send information to Bob, the channel capacity C_{AB} between Alice and Bob (using a polarized signal) is given by [27]

$$C_{AB} = \frac{1}{2}\log_2\left\{1 + SNR_{AB}\right\} \qquad \text{(bits/symbol)} \tag{1}$$

where SNR_{AB} denotes SNR of the Bob's signal. Similarly, when Eve eavesdrops the information during the communication, the channel capacity of Eve is represented as $\mathrm{C_{AE}}$ with SNR of the Eve's signal (SNR_{AE}).

Based on Wyner's wire-tap channel theory, an information theoretic secrecy capacity (C_{Secure}) is defined as the capacity difference between the eavesdropper Eve (C_{AE}) and the target receiver Bob (C_{AB}) [21].

$$C_{Secure} = C_{AB} - C_{AE} \qquad \text{(bits/symbol)} \tag{2}$$

To have a positive secrecy capacity, the SNR of Bob should be greater than that of Eve. In other words, the mutual information between Alice and Bob must be greater than the maximum mutual information (or channel capacity) between Alice and Eve.

We can use the secrecy capacity by adopting a modulation format carrying multiple bits per a symbol (bits/symbol) and a coding for the wire-tap channel [21]. For example, when Alice and Bob use a modulation format carrying more bits/symbol than the channel capacity C_{AE}, Eve gets higher bit error rate (BER) compared to it of Bob. Thus, when the communicators use the wire-tap channel coding for sharing maximum C_{Secure} information, Eve cannot retrieve any confidential information from the eavesdropping channel due to the high BER. In other words, the communicators can keep the secrecy of the exchanged information of maximum C_{Secure} against any eavesdropper. And then this secure state on the information is represented as perfect secrecy [21,22].

It should be noted that the modulation format must be selected within $C_{AE} < C_{format} \leq C_{AB}$ to achieved secrecy capacity. C_{format} is carrying bits per symbol of the modulation format, which should be lower than the channel capacity C_{AB}, to achieve an error-free communication. Then, we can express the secrecy capacity of a secure communication that uses a modulation format carried C_{format} bits/symbol as

$$C_{secure} = C_{format} - C_{AE}. \qquad \text{(bits/symbol)} \tag{3}$$

Then, the corresponding secure communication speed is expressed as

$$Secure\ Communication\ Speed = C_{secure} \times \text{Baudrate}. \qquad \text{(bits/second)} \tag{4}$$

The speed is proportional to baud-rate (or symbol rate) of the transmission and the secrecy capacity.

2.2. Anti-correlated noise

Obviously, random signals introduced by power splitting of a random source have perfectly positive correlation each other (corresponding correlation coefficient is '1'). In other words, the signals of the split sources are identical. In opposite way, when the correlation coefficient is negative, i.e., a split signal increase implies decrease of the other split signals, we defined it as anti-correlation. It should be noted that the sum of the perfectly anti-correlated two signals is constant, since the fluctuations of the two signals are compensated each other. In addition, we can have a set of anti-correlated signals for which the sum of all elements (or signals, $N_1, N_2, \ldots, N_M$) is constant as

$$\sum_{i=1}^{M} N_i(t) = Constant. \qquad \text{(M: total number of elements or signals)} \tag{5}$$

For the correlation coefficient between the two signals N_i and N_j, it depends on the total number of elements 'M'; the element can be a signal, carrier, channel, and etc., as followed applications. When we have only two elements ('M' = 2), the correlation coefficient is '−1', because the fluctuations are in opposite direction to each other. Then, the coefficient is reduced with an increase of 'M' as '$-1/(M-1)$'.

Practically, the anti-correlated signals can be generated for any physical quantities of an optical field, such as an intensity, phase, or electric field. In this paper, we introduce a noise set on optical intensities, which is followed above relation. Then, we define the set as an anti-correlated noise, and we can express the total intensity $I_{tot}(t)$ as

$$I_{tot}(t) = \sum_{i=1}^{M} I_i(t) = \sum_{i=1}^{M} \left\{S_i(t) + N_i(t)\right\}. \tag{6}$$

Here $I_i(t)$, $S_i(t)$, and $N_i(t)$ are the intensity, the signal, and the anti-correlated noise element of the 'i'th channel, respectively. To simplify the analysis, we assume that the sum of all anti-correlated noise elements is zero, then the total intensity $I_{tot}(t)$ equals to $\sum_{i=1}^{M} S_i(t)$. It implies that every single intensity $I_i(t)$ has lower signal-to-noise ratio (SNR) compared to the total intensity $I_{tot}(t)$. In addition, we can introduce high SNR difference (or channel capacity difference) between them by introducing very high noise on each single channel.

2.3. A perfect secrecy optical network

A conceptual diagram of the proposed perfect secrecy optical network is shown in Fig. 1. Node 'A' (transmitter) transmits confidential information to node 'B' (target receiver) using a modulated anti-correlated noise through multiple paths (three paths in this example). The anti-correlated noise is generated within 'M' optical carriers or optical channels. Then, each element of the modulated anti-correlated noise is transmitted through different path. In this case, any eavesdropper (Eve) on one of the paths obtains severely low SNR or low channel capacity due to the very high noise of the single element. It should be noted that the noise is in the communication carrier, and then it is independent of the quality of the receiver. In other words, the best SNR of Eve is limited by the carrier noise although Eve's receiver does not introduce any type of noises.

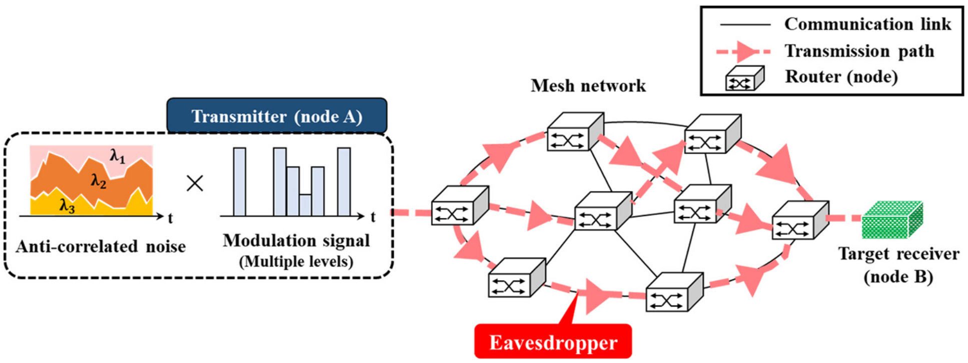

Fig. 1. A conceptual diagram of an anti-correlated noise based perfect secrecy optical network.

While the target receiver with all correlated channels (three elements in this case) can achieve high SNR obtained by retrieving the correlation between all elements properly. It is understandable that the correlations between the carriers (or channels) were broken at the target receiver, since the anti-correlated noise has a finite correlation time and each element experiences a different transmission path. Therefore, node 'A' and 'B' should share secretly the transmission path information or characteristics of the transmission paths to retrieve the correlation. As a result, the target receiver has the higher SNR or the channel capacity than Eve, which eventually ensure the perfect secrecy against Eve on a single path. The secrecy can be extended for less than 'M' channels eavesdropping (in this example up to two channels), since the Eve's SNR (or the channel capacity) is remained as lower than that of the target receiver.

The secrecy capacity C_{Secure} with an 'M'-channel anti-correlated noise can be represented as a function of the number of eavesdropped channels 'k' (or paths). To induce it, we define SNR of the received signal with the 'k' channels as

$$SNR_{\mathrm{k}} = \frac{\left\langle A_{signal,k}(\mathrm{t})\right\rangle^2}{\left\langle A_{noise,k}(\mathrm{t})\right\rangle^2}. \tag{7}$$

$A_{signal,k}(\mathrm{t})$ and $A_{noise,k}(\mathrm{t})$ stand for the converted photo-currents of the intensity $\sum_{i=1}^{k} I_i(t)$ with the 'k' channels. For distribution of the anti-correlated noise elements to each channel, we assume that the signal power is equally distributed to each channel. In addition, each carrier has the same noise power due to the carrier noise. Then, statistically, the noise power $\left\langle A_{noise,k}(\mathrm{t})\right\rangle^2$ can be expressed as

$$\left\langle A_{noise,k}(\mathrm{t})\right\rangle^2 = \sum_{i}^{k} \sigma_i^2 + \sum_{i,j}^{k} \rho_{i,j}\cdot\sigma_i\sigma_j = \mathrm{k}\cdot\sigma_i^2 + 2\cdot {}_k\mathrm{C}_2\cdot\rho\cdot\sigma_i^2. \tag{8}$$

σ_i^2 is noise power of the channel 'i', and $\rho_{i,j}$ is correlation coefficient between the noise elements in channel 'i' and 'j'. In ideal case of the anti-correlated noise, the correlation coefficient ρ between every two channels is equal to each other. In addition, when we have all channels (k = M), the noise power $\left\langle A_{noise,M}(\mathrm{t})\right\rangle^2$ is zero. Therefore, the correlation coefficient ρ can be induced from Eq. (8) in the condition of (k = M) as

$$\rho = \frac{-1}{M-1}. \tag{9}$$

Meanwhile, the signal power $\left\langle A_{signal,k}(\mathrm{t})\right\rangle^2$ is proportional to 'k^2' (the square of the number of obtained channels). Then, we can represent SNR_{k} as a function of 'k' and SNR_1 as Eq. (10). The denominator of this equation is induced by Eq. (8).

$$SNR_k = \frac{k^2\cdot\left\langle A_{signal,1}(\mathrm{t})\right\rangle^2}{k\cdot\left(M-k/M-1\right)\cdot\left\langle A_{noise,1}(\mathrm{t})\right\rangle^2} = \frac{k\cdot(M-1)}{M-k}\cdot SNR_1 \tag{10}$$

Based on this equation, we can have the infinite SNR when we have all channels (k = M). However, the SNR_M is finite in reality, so Eq. (10) is valid within (k < M).

Using the equations, the secrecy capacity (C_{secure}) for the 'M'-channel anti-correlated noise also can be represented as a function of the amount of the eavesdropped channels 'k' (k < M) as

$$C_{secure}(k) = \frac{1}{2}\log_2\left(1+SNR_M\right) - \frac{1}{2}\log_2\left(1+\frac{k\cdot(M-1)}{M-k}\cdot SNR_1\right). \tag{11}$$

Based on above analysis, we calculate the secrecy capacity of the proposed method and compare it with that of the previous multipath routing methods in Fig. 2.

For the simplest case, we can think of equally distributed information to 'M' channels without any encryption (or multipath routing without encryption). Then, information to Eve is proportional to the number of eavesdropped channels 'k'. In this case, secrecy capacity is linearly decreased along with the number of the eavesdropped channels as the yellow 'x' marked line.

However, if we use key sharing algorithm such as Shamir's (T, M) algorithm and Blakley's algorithm, only a person who has at least 'T' keys (or 'T' channels) from total 'M' keys (or 'M' channels) can have the information [28–30]. Thus, the information security is fully maintained without any leaked information until that Eve has all channels (when T = M) as black solid line.

Meanwhile, in the proposed method with ideal case ($SNR_M \to \infty$), we can have the information security fully maintained with almost no leaked information until that Eve has all channels (when k = M), as shown in Fig. 2 green dashed–dotted line (overlapped with black solid line). For realization, the secrecy capacity will be limited by SNR_1 (it was 6.4 dB considered our experimental results) and SNR_M, as red circle-marked line (20 dB suppression) and blue diamond-marked line (30 dB suppression), which depends on the performance of the noise suppression. When Eve achieves all three channels, the perfect secrecy is not guaranteed, ether. For this case, we introduce computationally secure system as discussed later.

3. Experimental demonstration of a perfect secrecy optical network

3.1. The anti-correlated noise generation

For introducing the anti-correlation relation between intensities of optical wavelength channels, a gain saturation effect can be used. There are many examples of using the gain saturation effect on a single channel for a noise suppression [31–33]. It should be noted that we could achieve anti-correlation relation among the multiple channels input. This is because the fluctuation of the total input is suppressed by the gain saturation, on the other hand, the fluctuations of each channel is still remained.

To induce the anti-correlation relation on the optical intensity, we operate a highly multi-mode Fabry–Perot laser diode (F–P LD) in deep saturation region with injection seeding, as shown in Fig. 3(a).

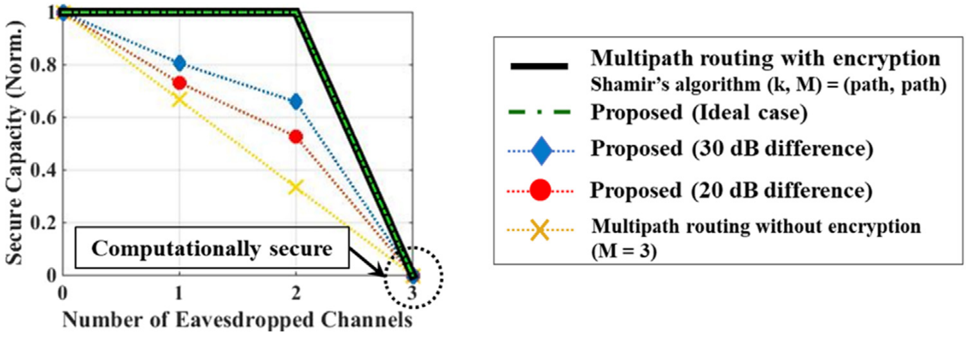

Fig. 2. The normalized secrecy capacity along with the number of eavesdropped channels.

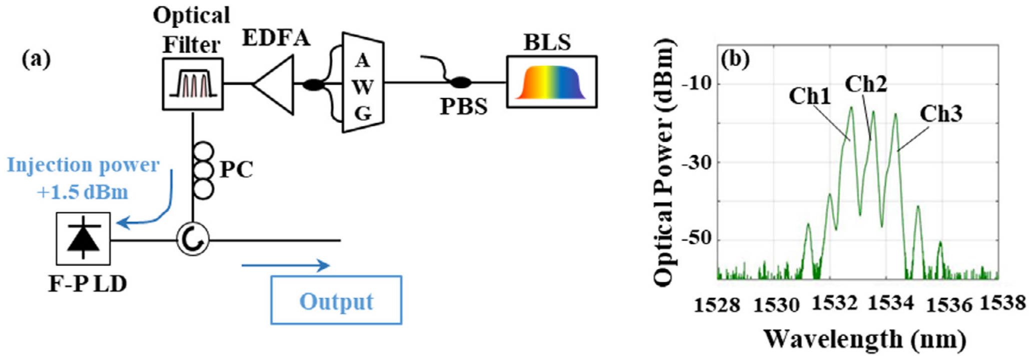

Fig. 3. (a) Anti-correlated noise generator (BLS: broadband light source, PBS: Polarization beam splitter, AWG: Arrayed waveguide grating, EDFA: Erbium doped fiber amplifier, PC: Polarization controller), and (b) optical spectrum of the output.

For getting noise sources, the polarized broadband light which is an amplified spontaneous emission from a broadband light source (BLS) was filtered by an arrayed waveguide grating (AWG, 50 GHz channel spacing, 35 GHz 3-dB channel bandwidth, flat-top type), then three-channel outputs are combined by 4 × 1 coupler. The channel spacing of 100 GHz between adjacent channels was selected to match with the mode spacing of the F–P LD of 100 GHz. To have high injection power, an erbium doped fiber amplifier (EDFA) was used. After that, the polarization of the amplified output was controlled by a polarization controller (PC) to match the polarization of the mode inside the F–P LD. Then, it was injected into a Fabry–Perot Laser Diode (F–P LD) with injection power of +1.5 dBm, which brings the laser in deep saturation region. This induces a strong gain saturation in the F–P LD. Because of the high-power injection with the mode-matched seeds, we had a three-channel output from the highly multi-mode F–P LD, as shown in Fig. 3(b) of the optical spectrum of the F–P LD [26].

To investigate the properties of the generated optical intensity, we measured relative intensity noise (RIN) of the output within 50 MHz ~4 GHz frequency region, as shown in Fig. 4(a).

The measured average RIN of each single channel (or each single mode of the F–P LD output) and total three-channel (or the total three modes of the F–P LD) were −102.46 dB/Hz (blue line in Fig. 4(a)) and −120.80 dB/Hz (red line in Fig. 4(a)), respectively. The noise difference is around 18 dB. It is considerable noise suppression compared to the uncorrelated input channels, which have average RIN of −104.00 dB/Hz and −108.77 dB/Hz for each single channel and the total three-channel, respectively; the uncorrelated input case has only 4.77 dB difference. It implies that the total three-channel output experienced the strong noise suppression, whereas each fluctuation of the channels is remained; an increase of the average RIN of each single channel from −104.0 dB/Hz (before injection) to −102.46 dB/Hz (after injection) was introduced by filtering of the injected light by a mode profile of the F–P LD. When we measure the average RIN with only two channels (see Fig. 4(a) green line), it still has very high RIN as −106.98 dB/Hz, which is only 4.5 dB less compared to the single channel case.

For estimation of SNR of each case, the RIN-SNR relation can be used as

$$\mathrm{SNR} = \frac{1}{RIN_{linear} \times Bandwidth}. \tag{12}$$

Then, corresponding SNRs of single channel, two channels, and the total tree-channel case are 6.4 dB, 11.1 dB, and 24.8 dB, respectively.

To understand the correlation between channels, we measured the cross-correlation as shown in Fig. 4(b). The cross-correlations between adjacent channels (channel 1 and 2, channel 2 and 3) were approximately −0.5 matched with the theoretical value ($-1/(M-1) = -0.5$) as followed Eq. (9), while that of the channels 1 and 3 was −0.23. This can be explained differences in the output power as shown in Fig. 3(b). Average correlation time of the three cases in Fig. 4(b) was about 115 ps (bandwidth of the anti-correlated noise was about 9 GHz). It should be noted that the anti-correlated noise generator was realized by using commercial off-the-shelf devices.

3.2. Demonstration of the perfect secrecy optical network

The experimental setup for demonstration of the proposed perfect secrecy optical network is shown in Fig. 5. The anti-correlated noise generator was identical to that in Section 3.1. The network consists of three different paths; a wired link with length of 5 km and two wireless links with length of 3 m and 7 m. At the transmitter, the modulation format was selected by considering the channel capacity of each single channel and the total channel, as followed Eq. (3). Since the channel capacities of each single channel (SNR: 6.4 dB) and the total channel (24.8 dB) are 1.21 bits/symbol and 4.12 bits/symbol, respectively, for a 4-pulse amplitude modulation (4-PAM, $C_{format} = 2.0$ bits/symbol). The modulation signal with 5 Gbaud-rate was generated by combined two outputs of a pulse-pattern generator (PPG). After the modulation at the Mach–Zehnder modulator (MZM), the optical signal is experienced a physical encryption with a dispersion compensating fiber (DCF), which will be explained later. The amount of dispersion for the DCF was

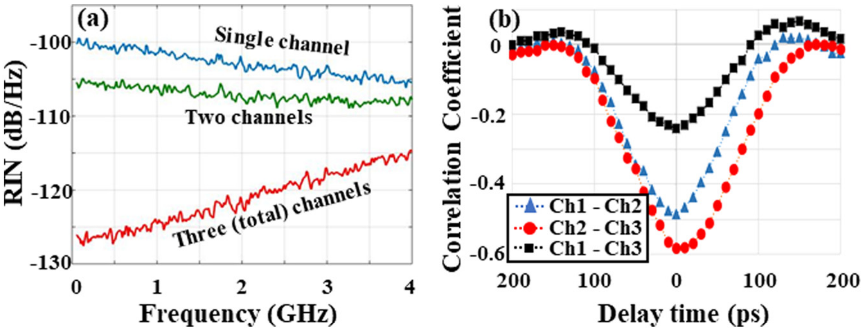

Fig. 4. (a) RIN of the anti-correlated noise source, (b) correlation coefficient between the two modes.. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

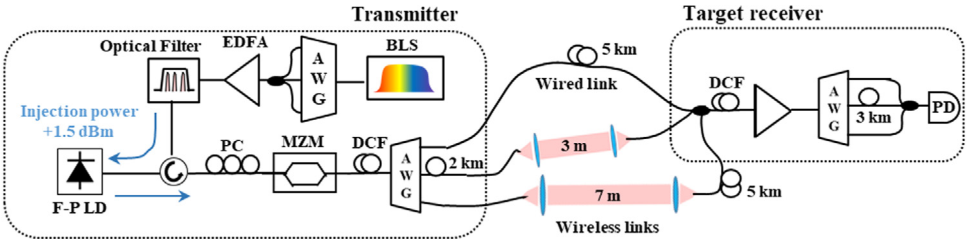

Fig. 5. A demonstration of the perfect secrecy optical network.

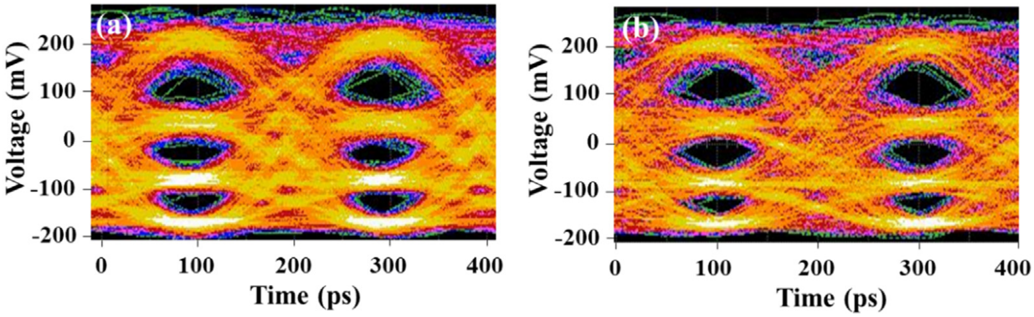

Fig. 6. The eye diagrams of (a) after modulation (at the transmitter side) and (b) at the target receiver.

1360 ps^2. Then, the three channels of the modulated anti-correlated noise were filtered out, and coupled into different transmission paths. We added a fiber spool (2 km fiber, in this example) for a physical encryption (assigned difference in the delay time) before coupling into the transmission paths. The transmitted signals were combined at the target receiver and decrypted (matching the delay time within the correlation time and compensating the dispersion) for the recovery of the transmitted data. It should be noted that optical power of each channel was monitored, and matched with each other. Then, the optical signals were received by 4 GHz bandwidth PIN PD based receiver.

The eye diagrams in Fig. 6 show (a) the modulated anti-correlated noise after the modulator, and Fig. 6(b) the recovered signal at the target receiver. We can see clear four-level eye diagrams in both cases. Then, bit error rate (BER) was measured for each case, as in Fig. 7. The forward error correction (FEC) limit of 10^{-3} was satisfied at received power of −19.5 dBm before transmission. After transmission, we observed 1.5 dB penalty. This penalty can be explained as mismatch in delay time (correlation) and dispersion. It should be noted that we have error floor, since the BER was limited by the RIN of the transmitted signal (not by the receiver noise).

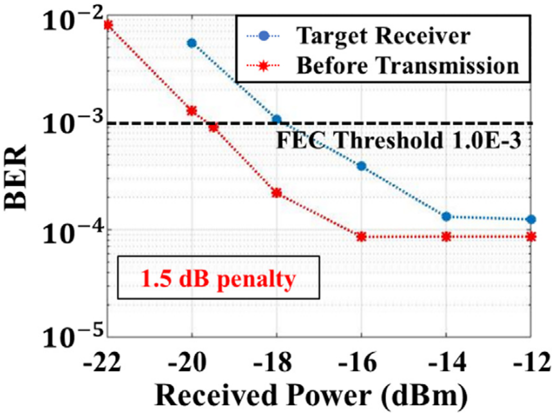

Fig. 7. Bit error rate (BER) measurement results.

The quality of an eavesdropped signal was measured as in Fig. 8. In this measurement, we assumed that Eve can have the signals from links without distortion or limitation on coupling efficiency. When Eve has a signal in a single path, it is impossible to recognize modulation feature since the eye-diagram shows severe distortion (due to the very low SNR) as seen in Fig. 8(a). Furthermore, when Eve has more signals without delay matching, the correlation is not retrieved and thus, the information cannot be recovered as shown in Fig. 8(b) and Fig. 8(c) for two and tree mismatched signals, respectively. However, when Eve has

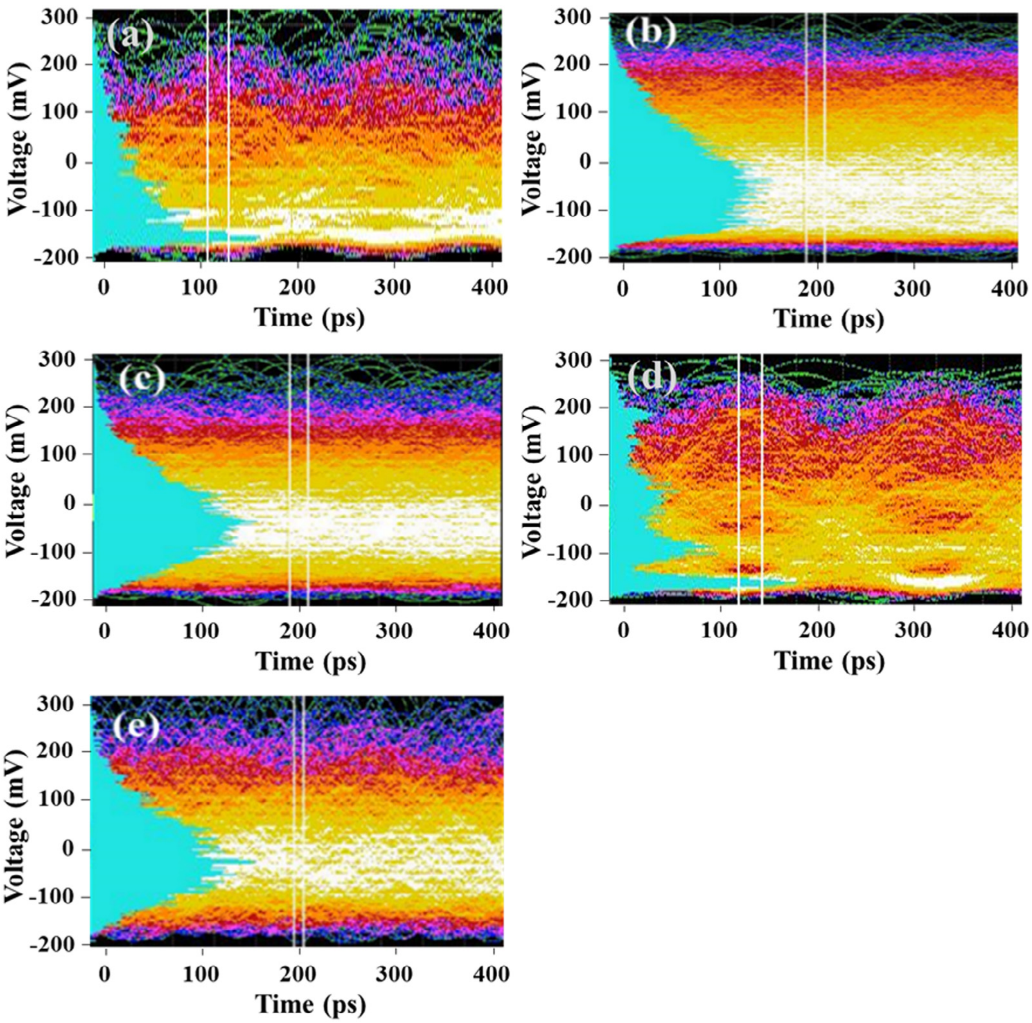

Fig. 8. The eye diagrams of Eve who achieves (a) a signal, (b) two mismatched signals, (c) three mismatched signals, (d) two matched signals, and (e) two matched signals and one mismatched signal (total three signals); dispersion effect was not applied in these results.

the two channels with matched delay, the adversary can get improved eye-diagram as shown in Fig. 8(d). Even this case, it was still hard to measure BER due to the low SNR (BER was over 1.5×10^{-1}). When we add the other signal without matching the delay (to Fig. 8(d)), the eye diagram becomes worse again as shown in Fig. 8(e).

Then, the realized secrecy capacity was estimated for each case. The carrying bits per a symbol of the 4-PAM modulation format is 2.0 bits/symbol. For any case of Eve on a single path, the secrecy capacity is 0.79 bits/symbol, since the channel capacity of Eve is 1.21 bits/symbol (SNR: 6.4 dB). Then, the corresponding secure communication speed is 3.95 Gb/s (as followed Eq. (4)), by considering the symbol rate of 5 Gbaud-rate. For Eve who has the two channels with delay matching condition as shown in Fig. 8(d), the channel capacity for Eve is 1.88 bits/symbol (SNR: 11.1 dB). In this case, the secrecy capacity becomes 0.12 bits/symbol (the secure communication speed is 0.6 Gb/s). The secure communication speed can be improved by using a modulation format with higher a bits/symbol rate, such as 8-PAM (3 bits/symbol), or 16-PAM (4 bits/symbol).

It is clear that when Eve has signals from all channels, the adversary can have the transmitted signal as shown in Fig. 6(b), by retrieving the correlation between the channels. To make it difficult, the encryptions (break of the correlation) can be imposed at the transmitter and transmission paths. Dispersion is one of the correlation break methods between the signals. To apply this encryption, we used a DCF in this experiment, as shown in Fig. 5. The measured effects of the correlation break due to dispersion are shown in Fig. 9(a) and (b) for two signals and three signals, respectively. It should be noted that the delay time between paths were fully matched. It is clear that we cannot recognize any modulation feature, and the eye-diagram was worse than Eve who has the two channels with correlation recovery. Since the correlation can be recovered by signal processing method (dispersion compensation for this case), the proposed method is computationally secure for Eve who has signals from all paths.

4. Improvement of the security

4.1. Improvement of the secrecy capacity with a bidirectional transmission

We have demonstrated one-way secure transmission with the anti-correlated noise. The secrecy capacity can be improved by adding a backward secure transmission, i.e., a bidirectional secure communication. Conceptual diagrams of the proposed bidirectional secure communication are shown in Fig. 10. Node ‘A’ wants to send confidential information to node ‘B’ in secret against any Eve. Prior to transmission of the information, node ‘A’ receives an encryption key (true random key) for one-time pad [22] from node ‘B’, as shown in Fig. 10(a). The key is transmitted by using the proposed perfect secrecy optical network from node ‘B’. Node ‘A’ then encrypts the information with the received encryption key. The modulated anti-correlated noise by this encrypted information is transmitted to node ‘B’ as shown in Fig. 10(b). It should be noted that transmission paths from node ‘A’ to node ‘B’ can be selected differently from transmission paths of node

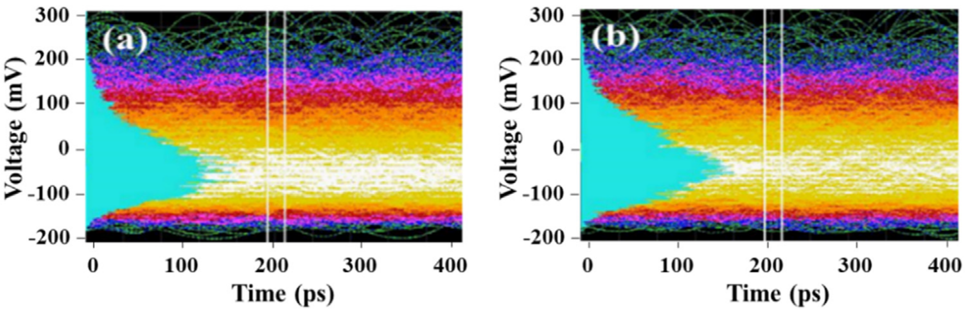

Fig. 9. The eye-diagrams of (a) two delay matched signals, and (b) three delay matched signals without dispersion compensation.

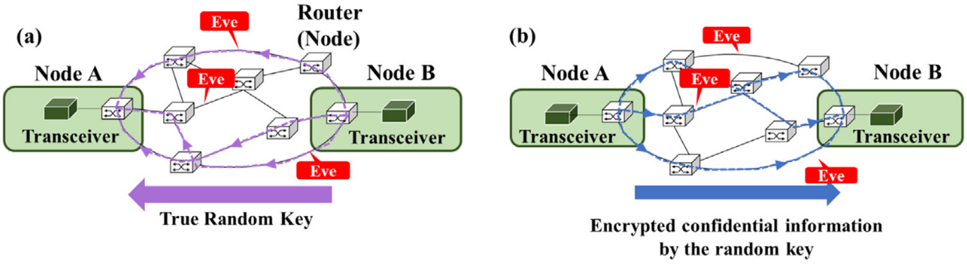

Fig. 10. Proposed bidirectional perfect secrecy network for improved security: (a) the exchange of a one-time encryption (true random) key through multiple paths, and (b) transmission of the encrypted confidential information through different paths.

'B' to node 'A'. Finally, node 'B' decrypts the received information (the encrypted confidential information) using the transmitted encryption key.

In this scenario, the secrecy capacity can be improved substantially, as a full eavesdropping on the unidirectional case does not provide any information to the eavesdropper. The adversary then needs information from both directions for achieving the confidential information. In other words, the channel capacity of Eve is limited by the smaller number of eavesdropped channels between two directions. We can express the obtainable secrecy capacity against Eve as $C_{secure}(\min\{k_1, k_2\})$ (see Eq. (11)), for which $\min\{k_1, k_2\}$ indicates the smaller number between 'k_1' and 'k_2'. The two numbers 'k_1' and 'k_2' indicate the number of eavesdropped channels from each direction (k_1 is for node 'A' → node 'B', and k_2 is for node 'B' → node 'A').

To verify the secrecy capacity improvement, we compare the secrecy capacity of the unidirectional communication with that of the bidirectional case, with the same number of channels '2M' for each case. Then, the unidirectional case uses '2M'-channel anti-correlated noise, while the bidirectional case uses 'M'-channel anti-correlated noise in both directions. First, the secrecy capacity as a function of the number of eavesdropped channels of the bidirectional case was calculated based on Eq. (11), as shown in Fig. 11(a) for 'M = 3' case. We used the experimental result of the maximum secrecy capacity (4.12 bits/symbol with no eavesdropping) for the normalization of the maximum mutual information (z-axis). Each secrecy capacity bar in Fig. 11(a) represents the minimum secrecy capacity of a given '$k = k_1 + k_2$'. Then, we compared the result to the unidirectional case of '2M = 6' case, as shown in Fig. 11(b), which was calculated based on Eq. (11) ether. The unidirectional case and the bidirectional case are displayed with blue and red lines, respectively. Since the secrecy capacity of the bidirectional case (red line) is greater than it of the unidirectional case in whole 'k', the green shaded region, for which an area is in between the two lines, represents the amount of the secrecy capacity improvement. Therefore, for the enhancement of the secrecy capacity, the bidirectional communication method is more efficient than unidirectional method with increasing the number of anti-correlated noise channels.

4.2. *Analysis of computational complexity*

An eavesdropper (Eve) who has all channels from the network is able to retrieve the transmitted data. In this case, the proposed method is computationally secure against the eavesdropper. To improve security, we propose to impose encryption of the channels on top of the time delay, including phase modulations. Then, we investigate the effects of these encryptions on the security. Finally, the computational complexity of the proposed method is analyzed.

4.2.1. *Encryption on the phase of the signals including fiber dispersion*

It is well known that a chromatic dispersion induces a phase shift on signals as square of the frequency deviation from the carrier. As a result, the intensity profile can be changed, and then the correlation relation between the anti-correlated noise channels can be broken. Thus, the eavesdropper must compensate dispersion and match the delay time to retrieve the transmitted information. Before we discuss the effects of dispersions, we consider a simple case with a constant phase shift within a given bandwidth to given channels. We matched the center of the phase shift region to the center of the signal spectrum. Even though the time delay was exactly matched, the average RIN of the total channel was degraded as a function of bandwidth of the phase shift region as shown in Fig. 12(a). For this result, the phase shift was π radian.

In the shaded region written as secure region, we can have positive secrecy capacity (see Eq. (2)), because of the SNR difference between target receiver's signal (with the phase shift compensation) and the eavesdropped signal (without the compensation). The minimum value of the average RIN for the secure region is −107.8 dB/Hz (channel capacity is 2.0 bits/symbol for 4-PAM modulated signal). The minimum phase shift bandwidth for achieving the secure region is 840 MHz (blue solid line). As increase of the bandwidth, the average RIN is increase until bandwidth of 3.1 GHz. After that the average RIN start to reduce (degradation become less). This is from the reduction of the effective phase distortion within the signal bandwidth. The maximum bandwidth for achieving the secure region is 6.2 GHz. When we apply the phase shift to all three channels, the bandwidth range for secure region becomes 250 MHz– 9.5 GHz (red dotted line).

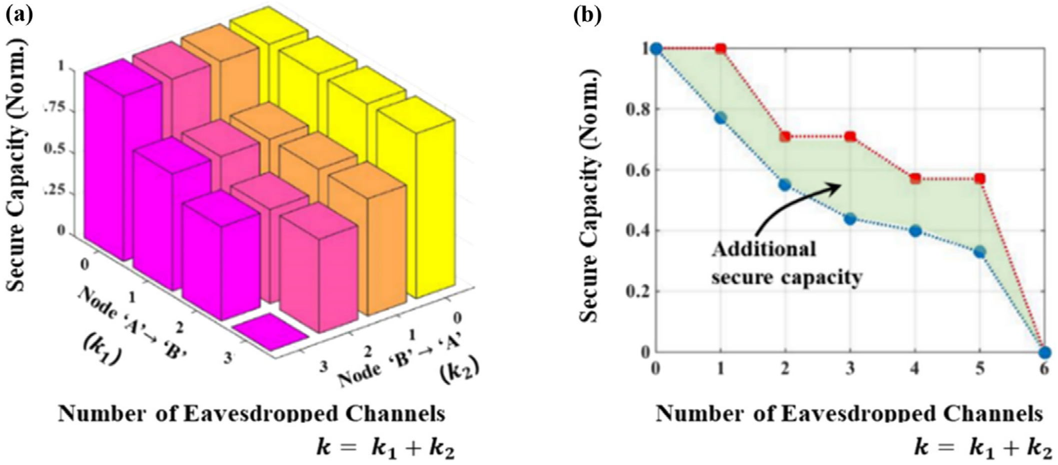

Fig. 11. (a) Secrecy capacity with the amount of the pilfered signals in each direction, and (b) secrecy capacity comparison between the bidirectional and unidirectional systems. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

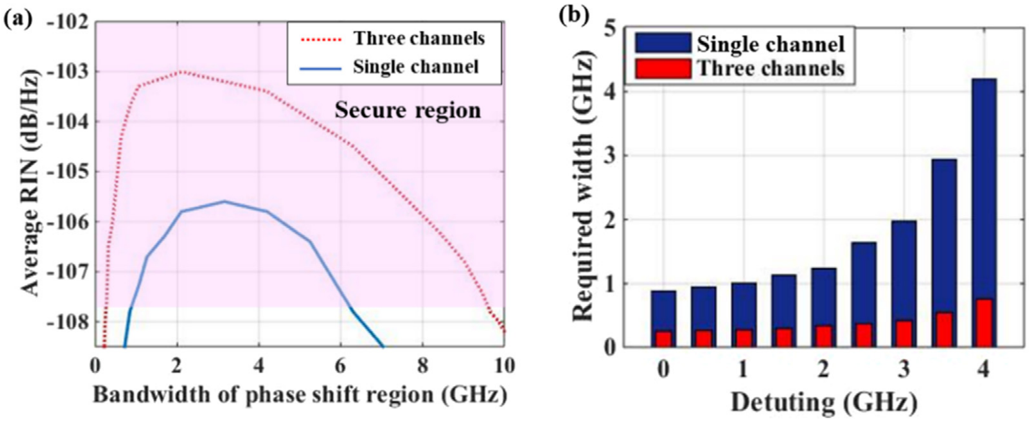

Fig. 12. (Simulation) (a) Decorrelation along with the phase modulation, and (b) required modulation width for reaching the secure region with phase shift of π along with detuning.. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

We also investigate influence of detuning of the center of the phase shift region from the center of the signal spectrum. The required bandwidth to reach the secure region is shown as a function of the detuning frequency in Fig. 12(b). The blue bar is for the phase shift on a single channel. As expected, the required bandwidth increases with increase of the detuning. It is also clear that the required bandwidth for a given detuning is decreased when we apply the phase shift to all three channels (Fig. 12(b) red bar).

It is possible to induce a complex phase changes with a phase mask in spectral domain. For analysis, we modeled simple phase masks and applied them to all three channels. Total bandwidth of each phase mask was 9 GHz (same with spectral width of the signal), and the spectrum was divided into nine sections (bandwidth of each section was 1 GHz). Then, the center of each phase mask was tuned to the center of each channel spectrum.

Then, we analyzed the required phase shift to reach the secure region as a function of the number of phase shift sections. The phase shift sections of each phase mask were allocated symmetrically from center of the phase mask to outward direction. In addition, we put the phase shift sections in between unchanged sections. For example, the corresponding phase mask patterns for the number of phase shift sections of '2', '3', '4' and '5' are '000101000', '001010100', '010101010', and '101010101', respectively; in each pattern, '1' and '0' indicate the normalized phase shift of the section and unchanged section, respectively. When we applied the same amount of phase shift to each section, the required phase shift was converged to 0.26π as shown in Fig. 13.

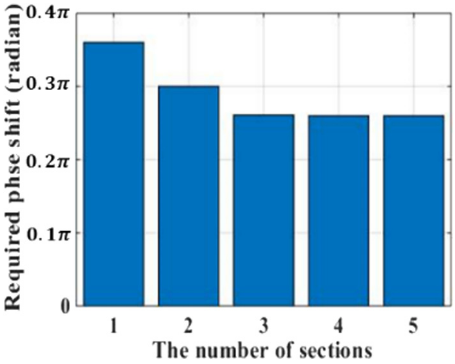

Fig. 13. Reduction of required phase shift as increase of the number of phase change sections.

Instead of the phase mask, a chromatic dispersion in an optical fiber induces a continuous phase shift across the signal spectrum. We measured experimentally average RIN of the total channel as a function of dispersion as in Fig. 14(a). For this experiment, we used a dispersion compensating fiber (DCF). Once again, we matched the delay time of all three channels. The average RIN degrades as we increase the dispersion, and we reach the secure region when the dispersion is more than 935 ps^2 (corresponding length of single mode fiber is 55 km). The average RIN also degrades with a higher order dispersion. For reference, we

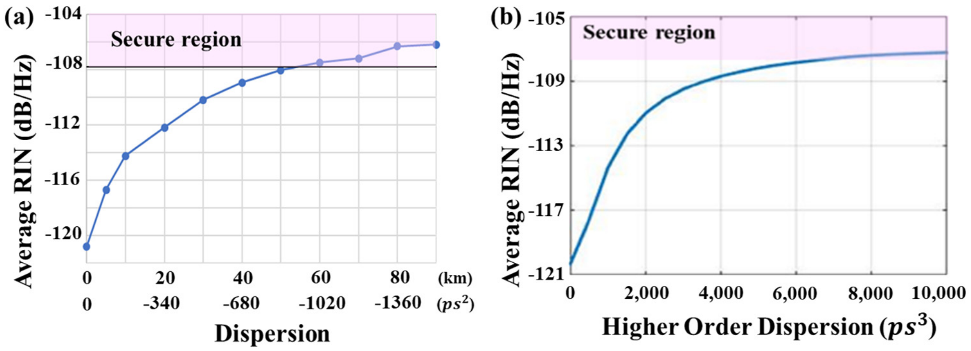

Fig. 14. Decorrelation along with (a) the chromatic dispersion (measurement) and (b) Higher order dispersion (simulation).

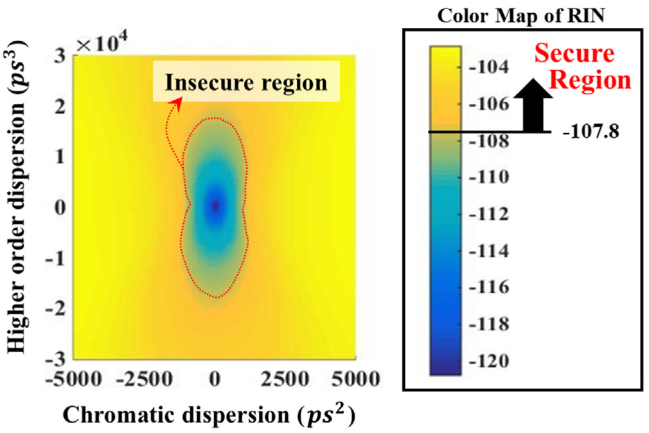

Fig. 15. Secure and insecure region along with the amount of chromatic and higher order dispersions (simulation results).. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

simulated the degradation as a function of the higher dispersion as shown in Fig. 14(b). We have the secure region when the higher order dispersion is above 6000 ps^3. For this calculation, we assumed zero chromatic dispersion.

By combining these two dispersion effects, we draw two-dimensional contour for the secure region in Fig. 15. The color becomes bluer as decrease of the average RIN. The average RIN of the inside the red contour in Fig. 15 is lower than −107.8 dB/Hz, then we represented that area as insecure region. The area looks the dumbbell shape, since the two dispersion effects on half of the spectrum compensate each other due to the different symmetry. (The chromatic dispersion has an axial symmetry, while the third order dispersion the origin symmetry in frequency domain. Thus, the directions of the phase shift of the two dispersion on one-half of the spectrum are always opposite each other.) When the two effects are applied simultaneously, the average RIN degradation is slower than the case with only chromatic dispersion effect. In addition, the average RIN degradation is slowest when only third order dispersion is applied, because it is less effective than chromatic dispersion.

4.2.2. *Estimation of computational complexity*

Since an eavesdropper (Eve) achieving all channels is able to recover transmitted information, we estimate a computational complexity by assuming that Eve will retrieve the information by using digital signal processing methods. We also assume that Eve can convert all received signals into digital data without distortion or adding noise.

For the investigation, we considered an optical network that carriers 64 wavelength division multiplexed (WDM) channels over a single fiber, which is length of 80 km (400 μs delay time). Then, we assumed that a three-channel anti-correlated noise (as in the experiment) was within the WDM channels instead of three different paths. In addition, the physical encryptions using the fiber delay, the chromatic dispersion within ±25 000 ps^2, the third order dispersion within ±300 000 ps^3, and the phase masking were considered. We believe that these dispersions can be achievable with chirped fiber brag gratings (FBGs). For the case of the phase modulation, we assumed the phase shift of each region is different with each other, and it is in between $\pm\pi$.

To retrieve the confidential information, Eve has to match the delay time of the three channels within the correlation time of the anti-correlation. It is also clear that the adversary must decrypt the encrypted information by the dispersions and the phase modulation. Since Eve does not have any information on these processes, the adversary must do all process with help of signal processing technologies.

First, Eve has to find out three channels that carry the confidential information among 64 channels. Then, Eve has the complexity of $n_{ch} = {}_{64}C_3$. After that, Eve will try to match delay time among the channels. A well-known that calculation of the cross-correlation using the Fast Fourier Transform Cross-correlation method algorithm [34] has a complexity of $O(n\log_2 n)$ in big-O notation where 'n' stands for the number of samples in FFT. Then, the time delay 'τ' between two signals can be estimated by a frequency dependent phase as $e^{i2\pi f\tau}$. Because the delay time accuracy must be less than half of the correlation time (58 ps = 115 ps/2), 'n' is approximately 6.90×10^6 (= maximum delay/half of the correlation time = 400 us/58 ps), when we assume the maximum delay time difference as 400 us (80 km fiber delay).

For the encrypted signal with the chromatic dispersion, the decryption process needs multiplications of the inverse function as below.

$$\mathrm{U}(\omega) = \exp\left\{\pm i\frac{1}{2}\beta_2\Delta\omega^2 L\right\}. \tag{13}$$

β_2 is the chromatic dispersion coefficient, and $\Delta\omega$ is angular frequency difference. By changing transmission length 'L', we can change the amount of compensating dispersion. Based on the measurement result in Fig. 14(a), the resolution of the compensation should be at most half of the amount of dispersion for secure region (467.5 ps^2 = 935 ps^2/2). Therefore, the number of cases for decryption of the chromatic dispersion approximately equals to $n_{2\mathrm{nd}}^2 = 1.1\times10^4 (= \{(2\times\text{maximum dispersion})/resolution\}^2)$; because the amount of the applied dispersion can be different for two paths, the square operation was taken. In the similar manner, the complexity induced by the third order dispersion was calculated as $n_{3\mathrm{rd}}^2 = 1.0\times10^4$ $(=\{2\times(3.0\times10^5)/(6.0\times10^3)\}^2)$.

For the worst-case scenario, even we assume that Eve knows the existence of an encryption phase mask, Eve should guess amount of the phase shift and the bandwidth of phase shift section to decrypt the phase modulation. Then, we investigated effects of detuning on the decryption phase mask from the center of the encryption phase mask to estimate the bandwidth of the phase shift section; the encryption and decryption masks should have inverse relation each other. As shown in Fig. 16, the average RIN increases with increment of the detuning.

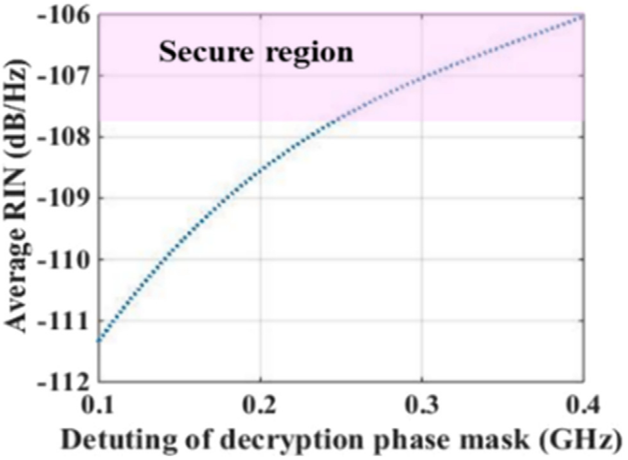

Fig. 16. Average RIN degradation as increase of detuning of decryption phase mask from the encryption phase mask.

To recover the information, the detuning must be less than 250 MHz. Then, the decryption resolution of Eve must be less than 250 MHz for the detuning, and 0.26π for the phase shift (from the result of Fig. 13).

Thus, the number of cases 'n_{phase}' for undo the phase modulation is approximately

$$n_{phase} \sim \left(\frac{2\pi}{decryption\ resolution\ of\ phase\ shift}\right)^{\left(\frac{spectral\ width}{resolution\ of\ bandwidth}\right)}. \tag{14}$$

Because the spectral width of our experiment is about 9 GHz, the index can be about 36 (= 9 GHz/250 MHz). Thus, the computational complexity for compensating the phase modulations on two signals is $n_{phase}^2 \approx 2^{212} \left(\approx \left\{(2\pi/0.26\pi)^{36}\right\}^2\right)$.

Finally, the total computational complexity including the delay, the dispersions, and the phase modulation is

$$\text{Operation} = \left\{\left(n \log_2 n\right) \times n_{ch} n_{\text{2nd}}^2 n_{\text{3rd}}^2 n_{phase}^2\right\}. \tag{15}$$

For our experimental, we may achieve the total computational complexity of 2^{281}. This complexity is considerably higher than current encryption algorithm with 128 bits.

5. Conclusion

We proposed a perfect secrecy optical network based on an anti-correlated noise. The anti-correlated noise was generated by using an ASE-injected F–P LD. Then, the individual channel of the modulated anti-correlated noise was transmitted to different 'M' paths within an optical communication network for the secure communication. Any eavesdropper on a single path experienced significantly lower SNR than that of the target receiver. This holds even when an eavesdropper can receive the signal without distortion and adding noise. Thus, the perfect secrecy is guaranteed based on Wyner's theory. This secrecy can be extended even for any eavesdroppers who have less than 'M' channels (from the perfect secrecy optical network with the 'M' channels anti-correlated noise).

Experimentally, we demonstrated the proposed method with the three-channel anti-correlated noise. The demonstrated secrecy capacity was 0.79 bits/symbol, which was estimated from measured SNRs of Eve and the target receiver. The corresponding secure communication speed was 3.95 Gb/s using 4-PAM with symbol rate of 5 Gbaud-rate. The transmission penalty was 1.5 dB with sensitivity of −19.5 dBm for BER of 10^{-3}. This secrecy capacity reduced to 0.12 bits/symbol (corresponding secure communications speed: 0.6 Gb/s) against an eavesdropper who has two channels with the correlation recovery.

We proposed secrecy capacity enhancement method using the bidirectional communication. In that case, an eavesdropper cannot have any confidential information on a single direction, even though the adversary has all channels in that direction.

Against an eavesdropper who has all channels, we estimated computational complexity of the proposed method. For the encrypted data with time delay, chromatic dispersion, high order dispersion, and phase shift, we can achieve the computational complexity of $\sim 2^{281}$. This is much higher than current 128 bits encryption algorithms.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This project was partly supported by project WQ20165000357 (Recruitment Program of Global Experts).

We thank Dr. Pallab Kumar Choudhury, KAIST, for his valuable comments.

References

[1] C. Landwehr, D. Boneh, J.C. Mitchell, S.M. Bellovin, S. Landau, M.E. Lesk, Privacy and cybersecurity: The next 100 years, Proc. IEEE 100 (Special Centennial Issue) (2012) 1659–1673.
[2] Daniel Gottesman, Hoi-Kwong Lo, From quantum cheating to quantum security, 2001, arXiv preprint-ph/0111100.
[3] N. Provos, P. Honeyman, Hide and seek: an introduction to steganography, IEEE Secur. Priv. 1 (3) (2003) 32–44.
[4] D. Artz, Digital steganography: hiding data within data, IEEE Internet Comput. 5 (3) (2001) 75–80.
[5] Der-Chyuan Lou, jian-Lung Liu, Steganographic method for secure communications, Comput. Secur. 21 (5) (2002) 449–460.
[6] B. Wu, Z. Wang, Y. Tian, M.P. Fok, B.J. Shastri, D.R. Kanoff, P.R. Prucnal, Optical Steganography Based on amplified spontaneous emission noise, Opt. Express 21 (2) (2013) 2065–2071.
[7] Haripriya Rout, Brojo Kishore Mishra, Pros and Cons of Cryptography, Steganography and Perturbation techniques, IOSR J. Electron. Commun. Eng. (2014) 76–81.
[8] Rina Mishra, Praveen Bhanodiya, A review on steganography and cryptography, in: 2015 International Conference on Advances in Computer Engineering and Applications, IEEE, 2015, pp. 119–122.
[9] Andrew Stok, Edward H. Sargent, The role of optical CDMA in Access networks, IEEE Commun. Mag. 40 (9) (2002) 83–87.
[10] Tomas H. Shake, Security performance of optical CDMA against eavesdropping, J. Lightwave Technol. 23 (2) (2005) 655–670.
[11] Tomas H. Shake, Spectral-phase-encoded optical CDMA, J. Light Wave Technol. 23 (4) (2005) 1652–1663.
[12] T. Yeteng, et al., Study on the effect of system parameters on physical-layer security of optical CDMA systems, in: 2019 18th International Conference on Optical Communications and Networks, ICOCN, IEEE, 2019.
[13] C.H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984, pp. 175–179.
[14] Artur K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. 67 (6) (1991) 661–663.
[15] Peter W. Shor, John Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. 85 (2) (2010) 441–444.
[16] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, Zhiliang Yuan, Practical challenges in quantum key distribution, npj Quantum Inf. 2 (2016) 16025.
[17] L. Marco, et al., Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature 557 (7705) (2018) 400–403.
[18] L. Sheng-Kai, et al., Satellite-to-ground quantum key distribution, Nature 549 (7670) (2017) 43–47.
[19] W. Tao, et al., High key rate continuous-variable quantum key distribution with a real local oscillator, Opt. Express 26 (3) (2018) 2794–2806.
[20] V. Raju, et al., A cost-effective measurement-device-independent quantum key distribution system for quantum networks, Quantum Sci. Technol. 2 (4) (2017) 04LT01.
[21] Aaron D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.

[22] C.E. Shannon, Communication theory of secrecy systems, Bell Labs Tech. J. 28 (4) (1949) 656–715.

[23] Satashu Goel, Rohit Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun. 7 (6) (2008) 2180–2189.

[24] Z. Xiangyun, M.R. McKay, Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation, IEEE Trans. Veh. Technol. 59 (8) (2010) 3831–3842.

[25] Il-Pyeong Hwang, Chang-Hee Lee, Secure communication using anti-correlated noise, in: Asia Communications and Photonics Conference 2017, ACP 2017, Su1L.1, 2017.

[26] Il-Pyeong Hwang, Myeonggyun Kye, Chang-Hee Lee, Secure communication using anti-correlated noise from ASE-injected F-P LD, in: 2018 23rd Opto-Electronics and Communications Conference, OECC, 5D1-2, 2018.

[27] C.E. Shannon, Communication in the presence of noise, Proc. IRE 37 (1) (1949) 10–21.

[28] Adi Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.

[29] Lou Wenjing, Yuguang Fang, A multipath routing approach for secure data delivery, in: IEEE 2001 MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No. 01CH37277), Vol. 2, 2001.

[30] G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, Vol. 48, 1979, pp. 313–317.

[31] Anoma D. McCoy, Peter Horak, benn C. Thomsen, Morten Ibsen, David J. Richardson, Noise suppression of incoherent light using a gain-saturated SOA: Implications for spectrum-sliced WDM systems, J. Lightwave Technol. 23 (8) (2005) 2399–2409.

[32] Joon-Young Kim, Sang-Rok Moon, Sang-Hwa Yoo, Chang-Hee Lee, DWDM-PON at 25 GHz channel spacing based on ASE injection seeding, Opt. Express 20 (26) (2012) B45–B51.

[33] Hyun Deok Kim, Seung-Goo Kang, Chang-Hee Lee, A low-cost WDM source with an ASE injected Fabry–Perot semiconductor laser, IEEE Photonics Technol. Lett. 12 (8) (2000) 1067–1069.

[34] G.D. Bergland, A guided tour of the fast fourier transform, IEEE Spectrum 6 (7) (1969) 41–52.