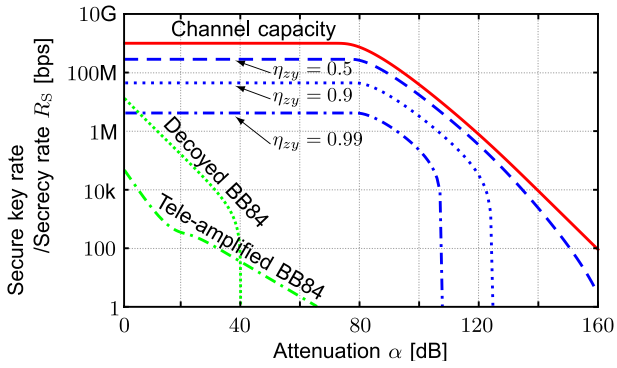
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Numerical Study on Secrecy Capacity and Code Length Dependence of the Performances in Optical Wiretap Channels

Volume 7, Number 5, October 2015

H. Endo
T. S. Han, Life Fellow, IEEE
T. Aoki
M. Sasaki



DOI: 10.1109/JPHOT.2015.2472281
1943-0655 © 2015 IEEE

IEEE photonics SOCIETY

IEEE

Numerical Study on Secrecy Capacity and Code Length Dependence of the Performances in Optical Wiretap Channels

H. Endo,[1,2] T. S. Han,[1] *Life Fellow, IEEE*, T. Aoki,[2] and M. 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

DOI: 10.1109/JPHOT.2015.2472281

Manuscript received July 1, 2015; revised August 18, 2015; accepted August 20, 2015. Date of publication August 24, 2015; date of current version September 3, 2015. This work was supported by the Council for Science, Technology, and Innovation (Cabinet Office, Government of Japan) through the ImPACT Program. Corresponding author: M. Sasaki (e-mail: psasaki@nict.go.jp).

Abstract: Secrecy issues of free-space optical links realizing information theoretically secure communications and high transmission rates are discussed. We numerically study secrecy communication rates of optical wiretap channel based on on–off keying (OOK) modulation under typical conditions met in satellite-ground links. It is shown that, under reasonable degraded conditions on a wiretapper, information theoretically secure communications should be possible in a much wider distance range than a range limit of quantum key distribution, enabling secure optical links between geostationary Earth orbit satellites and ground stations with currently available technologies. We also provide the upper bounds on the decoding error probability and the leaked information to estimate a necessary code length for given required levels of performances. This result ensures that a reasonable length of wiretap channel code for our proposed scheme must exist.

Index Terms: Physical layer security, free space optical communication, secrecy capacity, finite-length analysis.

1. Introduction

Free-space optical (FSO) communication is a promising technology for high-data-rate wireless networks, such as data links between satellites and ground stations [1]–[4], ad hoc trunk link not bounded by fiber networks [5], and the “last mile” link from the fiber backbone to the client premises [6].

The high directionality of laser beam can make FSO communications more secure than RF ones. However, it has been shown in [7] and [8] that FSO communications can still suffer from optical tapping risks, especially when the main lobe of laser beam is considerably wider than the receiver size, which is the case for optical links between moving terminals, and also between satellites and ground stations. To establish the secrecy of confidential data communications, symmetric key cryptography is often used with a preshared secret key or a key exchanged via public key cryptosystems. These crypto-schemes are based on mathematical problems that are practically impossible to solve using current computer resources. Its security is often referred to as computational security.

Recently, an approach based on physical layer security attracts much attention as an alternative mechanism. This is based on an appropriate coding technique designed by considering physical properties of the channels, i.e., the main channel between the sender (Alice) and the legitimate receiver (Bob), and the wiretapper channel from Alice to an eavesdropper (Eve). This coding is particularly called the wiretap channel coding [9], [10], and realizes the two functions at the same time in the physical layer; the reliability for Bob and the secrecy against Eve. The secrecy ensured by this paradigm is referred to as information theoretic security (ITS), which can be everlasting, in the sense that it can be proved that Eve cannot obtain meaningful information even by unforeseen mathematical insights or by off-line attacks with future advanced computers.

Studies so far on physical layer security in wireless channels and system architecture issues are nicely reviewed in [11]. An information-theoretically secure key exchange protocol over quasi-static wireless channels was proposed with a near-optimal LDPC (low density parity check)-based reconciliation method over a wide range of signal-to-noise ratios (SNRs) [12]. Physical layer security of FSO communications has been discussed in [13], proposing a secret key agreement over fading channels with reciprocity, and clarifying dominating factors on the secret key rate. In [14], analysis was made on likely wiretap scenarios and influences to secure FSO communication performances, in terms of the outage probability of non-zero secrecy capacity. Mostafa and Lampe studied physical layer security for indoor visible light communications [15], and showed that secrecy rates can be increased by utilizing Eve's channel state information (CSI) via null-steering, or by adding artificial noises when Eve's CSI is not available.

An extreme example of physical layer security has been already realized in quantum key distribution (QKD) [16]–[18], which has been extensively studied and now becomes practical in a metropolitan area fiber network [19], [20]. QKD ensures the unconditional security in the sense that Eve can have unlimited physical abilities and computational power. For FSO channels that are basically line-of-sight (LoS) communications, however, this assumption is sometimes too much. The LoS condition can naturally relax the assumption for Eve. In fact, expected key rates of QKD in satellite-to-ground links are impractically poor if one insists on assuming that Eve can be everywhere in the universe and can do anything. Instead, one should exploit more practical schemes that can attain higher key rate for LoS FSO channels under sensible assumptions case by case.

Design theory for wiretap channel coding should hopefully be able to evaluate the reliability for Bob and the secrecy against Eve. Practically, the cost constraint at Alice's side, such as the power and bandwidth constraint, is an important factor to be cared. In fact, transmission power should be carefully regulated so as not to increase wiretap risks. Furthermore, the performances should eventually be characterized in finite length coding for practical use. These issues have been partly dealt with in literatures [21], [22], but insights into unified theory and numerically expected performances have not been accumulated sufficiently yet, even in the idealistic setting of fading free channels.

In this paper, we study the optical wiretap channels with linear attenuation and background noises based on the on-off keying (OOK) modulation. From the practical viewpoint, we impose the power constraint on Alice's available transmission power. We numerically study the achievable secrecy rates and the secrecy capacity as a function of channel attenuation. We compare them with the secure key rate for QKD to show how the performance can be increased by compromising the assumption on Eve. According to the calculation, even if Eve can obtain 99% as much power as Bob, FSO links with ITS would be possible between geostationary earth orbit (GEO) satellites and ground stations with currently available technologies. A functional meaning of auxiliary random variable originally introduced by Csiszár and Körner [10] to establish the rate region of the general wiretap channel is clarified as a booster mechanism of the distance limit due to the auxiliary noises. We then apply a recent theory on the error and secrecy exponents by some of authors [21] to finite length analysis on the optical wiretap channels. We show how the code length to reach the given required levels of reliability and secrecy is estimated via the finite length analysis.

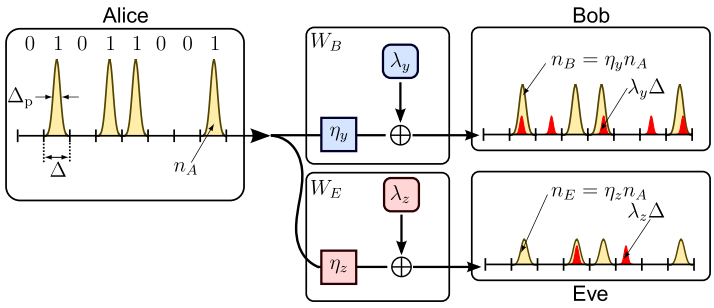


Fig. 1. Wiretap channel based on on-off keying (OOK) modulation.

The paper is organized as follows. In Section 2, we give the model and formulate the problems. In Section 3, we present numerical results of an achievability rate (lower bound to the secrecy capacity) and the structure of optimal parameters and power regulation. Section 4 includes analysis with the auxiliary random variable used at Alice. Section 5 describes the estimation of the necessary code length for the given required levels of performances via the finite length analysis. The paper is concluded in Section 6.

2. Formulation of the Model

Throughout this paper, we consider a model of optical wiretap channel with linear attenuation and background noises based on on-off keying (OOK) modulation as shown in Fig. 1. This model consists of the main channel W_B with which Alice transmits a confidential message to Bob and the wiretapper channel W_E with which Eve attempts to observe the confidential message. Bob and Eve receive the OOK signals by an on-off detector based on photon counting. The main and wiretapper channels are characterized by two parameters: the channel transmittances η_y and η_z, and the dark count rates (DCR) λ_y [counts/sec] (cps) and λ_z [cps], respectively. In this work, we dare to assume that the channels are fading free, in order to derive potentially achievable performances in good propagation conditions.

Alice is subject to the constraint with the maximum available transmission power of P [W], and transmits on- and off-signals encoding symbols "1" and "0" with probabilities q and $1-q$, respectively. The on-signal "1" is conveyed by a laser pulse of width Δ_p [s] and an average photon number n_A. The off-signal "0" is conveyed by the vacuum pulse. Bob and Eve receive the attenuated pulses of the average photon numbers $n_B = \eta_y n_A$ and $n_E = \eta_z n_A$, respectively. Detector efficiencies are renormalized into the channel transmittances. In order to compare the fraction of power received by two parties, we introduce the relative transmittance $\eta_{zy} \equiv \eta_z/\eta_y$. In the LoS scenario, $\eta_{zy} \leq 1$ can be valid. The detector time resolutions for Bob and Eve are finite, and assumed to be the same, Δ [s], for simplicity, and to be larger than the laser pulse width, i.e., $\Delta > \Delta_p$. This time resolution actually sets the maximum limit of repetition rate of optical pulses.

The above channel model should be regarded as a practical reduction of Poisson channel [23], [24], which assumes an arbitrary short time resolution $\Delta \to 0$, i.e., an infinite detector bandwidth, and has been extensively studied in [25], where the analytical formulas of the secrecy capacity were derived.

In the following, we mathematically formulate the model mentioned above.

2.1. Power Constraint

Alice needs to optimize the input probability q and the average photon number n_A within the maximum available transmission power P. In this work, we consider an optical channel at a center frequency $f_0 = 200$ THz (wavelength of 1.5 μm, which is eye safe and commonly used in optical fiber communications) with a certain bandwidth B [Hz]. The pulsed laser of Alice is assumed to be Fourier-transform limited, i.e., $B\Delta_p = 1$. The value of B must be larger than the detector bandwidth Δ^{-1}. For simplicity, an average photon number at each frequency $\bar{n}(f)$ of

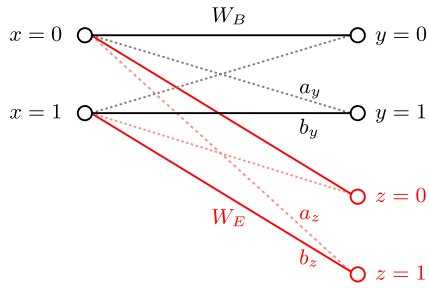


Fig. 2. Channel diagram of wiretap channel.

the on-signal pulse is assumed to be the same value n_A within the bandwidth B. Thus, the power per on-signal pulse is

$$P_{\mathrm{p}} = \int_{-\infty}^{\infty} \bar{n}(f) h f df \simeq \int_{f_0 - B/2}^{f_0 + B/2} n_A h f df = \frac{n_A h f_0}{\Delta_{\mathrm{p}}} \tag{1}$$

where h is Planck's constant. The total power of the OOK transmission is then

$$P_{\mathrm{total}} = q \frac{\Delta_{\mathrm{p}}}{\Delta} P_{\mathrm{p}} = q \frac{n_A h f_0}{\Delta} \tag{2}$$

which must be constrained by the maximum available power P. Thus, we have the following power constraint:

$$q \frac{n_A h f_0}{\Delta} \leq P. \tag{3}$$

2.2. Channel Matrices

The symbols for Alice, Bob, and Eve are defined as x, y, and z, drawn from the binary random variables X, Y, and Z, respectively. The on-off detectors at Bob and Eve discriminate the signals by the absence or presence of counts as "0" or "1". Since the system is assumed to be stationary and memoryless, the main channel W_B illustrated in Fig. 2 can be fully described by the elementary channel with the channel matrix given as

$$W_B(1|0) = 1 - e^{-\lambda_y \Delta} \equiv a_y, \quad W_B(1|1) = 1 - e^{-(\eta_y n_A + \lambda_y \Delta)} \equiv b_y$$

and

$$W_B(0|0) = e^{-\lambda_y \Delta} = 1 - a_y, \quad W_B(0|1) = e^{-(\eta_y n_A + \lambda_y \Delta)} = 1 - b_y.$$

Note that the DCR λ_y is understood to include not only the dark counts of the detector but also the background noises in the main channel. Similarly, the elements of the channel matrix of the wiretapper channel W_E are given by

$$W_E(1|0) = 1 - e^{-\lambda_z \Delta} \equiv a_z, \quad W_E(1|1) = 1 - e^{-(\eta_z n_A + \lambda_z \Delta)} \equiv b_z$$
$$W_E(0|0) = e^{-\lambda_z \Delta} = 1 - a_z, \quad W_E(0|1) = e^{-(\eta_z n_A + \lambda_z \Delta)} = 1 - b_z.$$

2.3. Channel Capacity and Secrecy Rate

In this subsection, we introduce necessary measures and formulas to evaluate the performance of our model. In particular, starting with channel capacity, we provide the formula for achievable secrecy rate maximized over possible transmission strategies without the auxiliary random variable V. The secrecy capacity is defined as the maximum achievable secrecy rate

optimized also over the auxiliary random variable V in addition to the input variable X [10], because the additional randomness with V can be helpful for deceiving Eve, especially when the wiretapper channel W_E is not worse than the main channel W_B and, hence, can improve the secrecy rate. We will work on it later in Section 4.

Considering the standard channel coding without Eve, the maximum achievable rate of reliable transmission is called channel capacity and is given by

$$C = \max_{P_X} I(X;Y) \tag{4}$$

where $I(X;Y)$ is the mutual information between the random variables X and Y. The maximization is taken over all possible input probability distribution P_X.

In this paper, we extend the above definition slightly so that not only the input probability q but also the input signal intensity (the average photon number n_A) are simultaneously optimized under the power constraint (3). Therefore, the channel W_B is not a given fixed matrix but a 2-by-2 matrix variable through the parameter n_A to be optimized. The channel capacity is then defined as

$$C \equiv \max_{q,n_A} f_B(q,n_A) \tag{5}$$

where

$$f_B(q,n_A) \equiv h_2\big((1-q)a_y + q(1-b_y)\big) - (1-q)h_2(a_y) - qh_2(b_y) \tag{6}$$

with the binary entropy function defined as

$$h_2(q) \equiv -q\log_2 q - (1-q)\log_2(1-q). \tag{7}$$

In the wiretap channel coding, we concern the asymptotically maximum achievable secrecy rate of reliable transmission to Bob while ensuring the ITS against Eve, which is defined in the form as [9]

$$R_S = \max_{P_X}[I(X;Y) - I(X;Z)]. \tag{8}$$

To have a positive value of R_S, the relation $I(X;Y) \geq I(X;Z)$ should hold for any X, which means that the main channel W_B is better than the wiretapper channel W_E, regardless of the input strategy. If this is the case, the wiretap channel is said to be more capable and the above quantity coincides with the secrecy capacity, which will be mentioned later in Section 4. In this paper, we deal with general cases, not necessarily being more capable, by assuming that the wiretapper channel W_E is not worse than the main channel. It depends on $\eta_y, \lambda_y, \eta_z$ and λ_z whether the wiretap channel is more capable or less capable. Now, the similar extension for the simultaneous optimization of q and n_A is made as

$$R_S \equiv \max_{q,n_A} f_{BE}(q,n_A) \tag{9}$$

where

$$f_{BE}(q,n_A) \equiv f_B(q,n_A) - f_E(q,n_A) \tag{10}$$

and

$$f_E(q,n_A) \equiv h_2((1-q)a_z + q(1-b_z)) - (1-q)h_2(a_z) - qh_2(b_z). \tag{11}$$

3. Numerical Results of Channel Capacity and Secrecy Rate

It is generally difficult to derive a closed form expression for the channel capacity (5) and the secrecy rate (9), except for simple channels such as a binary symmetric channel. Hence, we carry

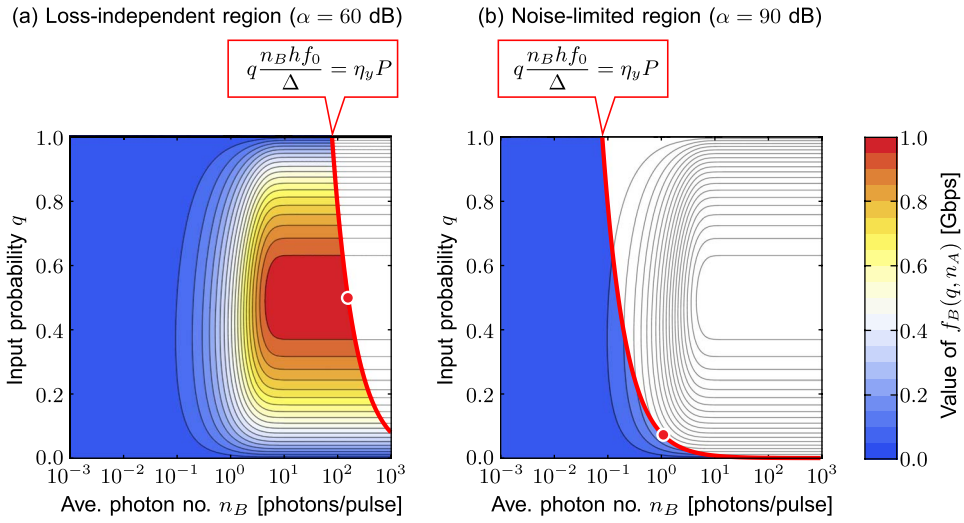


Fig. 3. Contour plots of $f_B(q, n_A)$ as a function of input probability q and average photon number $n_B = \eta_y n_A$ of the received pulse. (a) The loss-independent region with $\alpha = -\log_{10}\eta_y = 60$ dB. (b) The noise-limited region with $\alpha = 90$ dB. The red circle and the white painted area in each plot represent the channel capacity C and the non-allowed region due to the power constraint, respectively. Parameter values: $P = 10$ mW, $\lambda_y = 10$ kcps, and $\Delta = 1$ ns.

out the numerical optimization in order to obtain these quantities. Throughout this section, we adopt a set of parameters as follows: $P = 10$ mW, $\lambda_y = 10$ kcps, $\lambda_z = 1$ cps, and $\Delta = 1$ ns, where the value of the time resolution Δ corresponds to the maximum possible pulse repetition rate of 1 GHz. Note that the above parameters represent the case where Alice and Bob have the transmitter and the detector which will be available at the current level of technology, respectively, whereas Eve may have a much less noisy detector. In this case, the wiretap channel is not more capable for all possible values of n_A.

3.1. Channel Capacity

In this subsection, we present basic results of the channel capacity when there is nothing to do with the wiretapper channel, discuss important features in our model, and prepare ourselves for the main analysis on the secrecy rate.

Fig. 3 shows contour plots of the mutual information $f_B(q, n_A)$ as a function of input probability q and average photon number $n_B = \eta_y n_A$ of the received pulse. The calculations are demonstrated for two typical cases: (a) for a sufficiently small attenuation α (short distance transmission), where an attenuation α is defined by $\alpha = -\log_{10}\eta_y$, and (b) for a larger attenuation α (long distance transmission). From this figure, we can know how the channel capacity and the optimal q and n_B (and hence n_A) are determined as the attenuation α varies. The power constraint translated in terms of received power at Bob is represented by the left lower region below the boundary (red solid line), which is referred to as the allowed region. The channel capacity C, indicated by the red circle, can be found on this boundary line. The right upper region is not allowed by the power constraint, referred to as the non-allowed region.

In Fig. 3(a), the power constraint border (red line) crosses the plateau of the maximum value of $f_B(q, n_A)$. As the attenuation α increases (the amount of the received power $\eta_y P$ decreases), the non-allowed region (right-upper area) extends to the left-lower side. Unless the power constraint border gets out of the plateau of the maximum of $f_B(q, n_A)$, the value of the channel capacity remains the same value, independent of α. In this region, Alice's power is sufficient enough to transmit the signals such that Bob's detector can well discriminate them, not limited by the noises. We refer to the region as the loss-independent region.

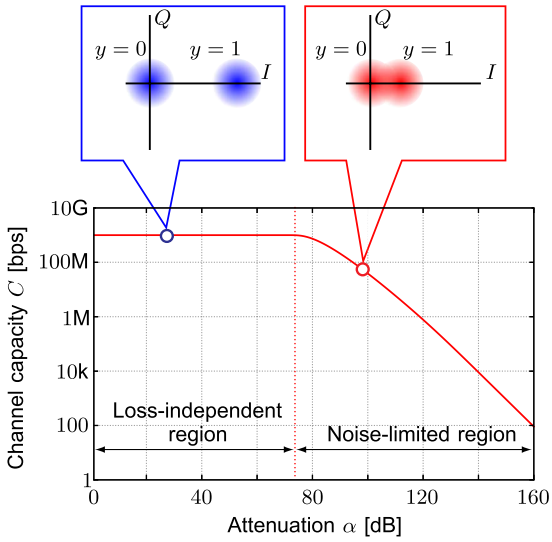


Fig. 4. Channel capacity C as a function of attenuation $\alpha = -\log_{10}\eta_y$. The upper insets are the intensity-quadrature constellations for received signals in the loss-independent (left) region and the noise-limited region (right). Parameters: $P = 10$ mW, $\lambda_y = 10$ kcps, and $\Delta = 1$ ns.

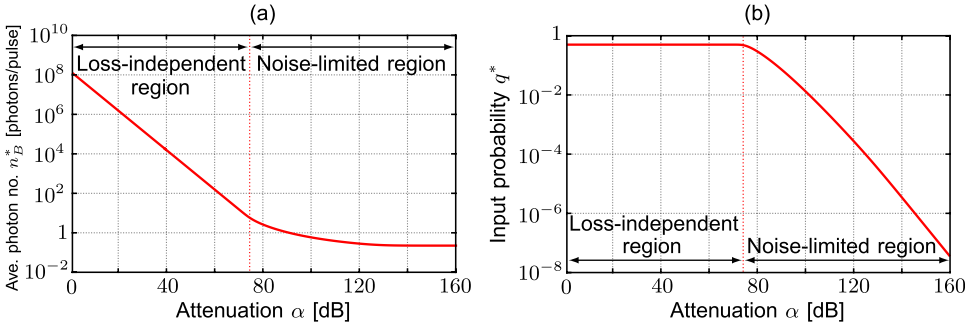


Fig. 5. Optimal parameters for the channel capacity C in Fig. 4. (a) Average photon number n_B^*. (b) Input probability q^*.

When the power constraint border has once gotten out of the plateau of the maximum of $f_B(q, n_A)$, as depicted in Fig. 3(b), the channel capacity starts to decrease. One can see the optimal q should also decrease. This means that Alice had better to send the on-signal less frequently to be able to make the on-signal as bright as possible under the power constraint so that Bob's detector can discriminate it from the noise background with high SNR. We refer to the region as the noise-limited region.

Such behaviors can be explicitly seen in Fig. 4 by the channel capacity C as a function of attenuation α. The optimal parameters n_B^* and q^* are shown in Fig. 5(a) and (b), respectively. In the loss-independent region, although n_B^* decreases as α increases, Bob can still have a sufficiently high SNR, hence the capacity is unchanged. The q^* is about 0.5. In the noise-limited region, n_B^* stays at a level of around 1 photon/pulse so that the SNR for the received signals is not further degraded (keeping the distance between the on- and off-signals in the I-Q constellation diagram the same order as the noise distribution), while q^* should decrease as α increases so that the power constraint is satisfied. The channel capacity decreases as α increases, according roughly to q^*.

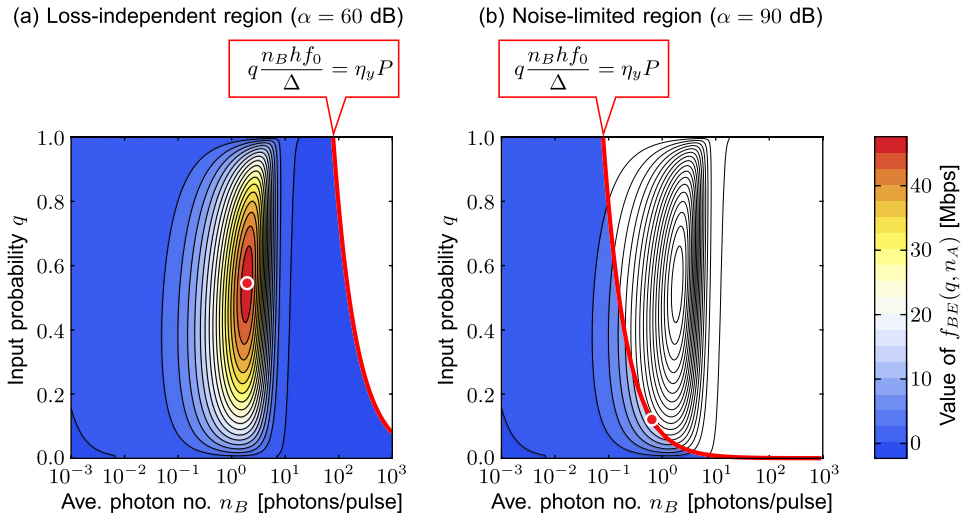


Fig. 6. Contour plots of $f_{BE}(q, n_A)$ as a function of input probability q and average photon number n_B of the received pulse and input probability q. (a) The loss-independent region with $\alpha = -\log_{10}\eta_y = 60$ dB. (b) The noise-limited region with $\alpha = 90$ dB. The red circle and the white painted area denote the secrecy rate R_S and the non-allowed region due to the power constraint, respectively. Parameters: $P = 10$ mW, $\eta_{zy} = 0.95$, $\lambda_y = 10$ kcps, $\lambda_z = 1$ cps, and $\Delta = 1$ ns.

3.2. Secrecy Rate

In this subsection, based on the analysis carried out in the previous subsection, we move onto the main analysis on the secrecy rate R_S, and discuss the optimal strategy.

Fig. 6 shows contour plots of $f_{BE}(q, n_A)$ as a function of input probability q and average photon number n_B of the received pulse. Contrary to $f_B(q, n_A)$ shown in Fig. 3, the function $f_{BE}(q, n_A)$ sharply decreases at large n_B, which is intuitively understood that the bright pulse increases the information leakage against Eve. Moreover, the value of $f_{BE}(q, n_A)$ can be negative, because Bob's detector is much more noisy than Eve's one, and hence, the wiretap channel is not more capable.

Fig. 6(a) is for the loss-independent region. The maximum of $f_{BE}(q, n_A)$ (red circle) is located inside the allowed region. Unless the power constraint border (red solid line) passes over this maximum to the left-lower side, the secrecy rate R_S can be realized at this maximum. Thus, the optimal parameters (q^*, n_A^*) satisfy the strict inequality as

$$q^* \frac{n_A^* h f_0}{\Delta} < P \tag{12}$$

indicating that Alice should not use the available power fully but regulate the transmission power properly to prevent the confidential information from leaking against Eve.

Similarly to the channel capacity, the secrecy rate begins to decrease when the power constraint border line has once passed over the maximum of $f_{BE}(q, n_A)$ as shown in Fig. 6(b). In this region, the secrecy rate is located on this border such that Alice should use all the available power to retain the necessary SNR. Thus, the optimal parameters (q^*, n_A^*) satisfy the power constraint with holding equality as

$$q^* \frac{n_A^* h f_0}{\Delta} = P. \tag{13}$$

In Fig. 7, we calculate the secrecy rate R_S as a function of attenuation α taking the above consideration into account. As indicated in the figure, the secrecy rate decreases as the relative transmittance η_{zy} gets close to 1, which is the case where Eve receives the equal amount of

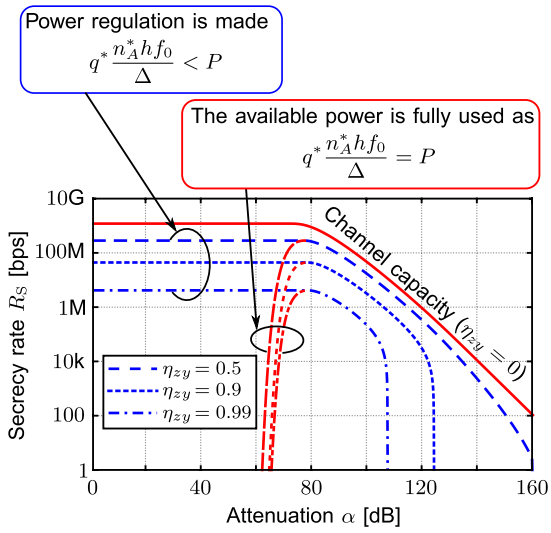


Fig. 7. Secrecy rate R_S as a function of attenuation $\alpha = -\log_{10}\eta_y$ with various relative transmittances η_{zy}. For comparison, the cases where the available power at Alice is used up are also shown. Parameters: $P = 10$ mW, $\lambda_y = 10$ kcps, $\lambda_z = 1$ cps, and $\Delta = 1$ ns.

power as Bob. Compared to the channel capacity denoted by the solid line, we can observe some unique features of the secrecy rate R_S in terms of the dependence on attenuation α. First, in the noise-limited region, R_S decreases rapidly at a certain threshold point. In this figure, R_S for $\eta_{zy} = 0.9$ and $\eta_{zy} = 0.99$ rapidly fall down to 0 at around $\alpha = 124.4$ dB and 107.6 dB, respectively. Second, if the available input power is fully used up in the loss-independent region, R_S rapidly falls down to 0 as α decreases, and equivalently, the distance between Alice and Bob gets shorter.

The optimal parameters n_A^*, n_B^*, and q^* are depicted in Fig. 8. Interestingly enough, in contrast to the secrecy rate itself, the behaviors of these parameters seem to be irrespective to relative transmittance η_{zy}. Fig. 8(a) indicates that n_A^* increases as α increases in both the loss-independent and noise-limited regions, whereas n_A^* for the channel capacity (solid line) stays constant. This means that, for the secrecy rate, Alice should properly regulate the input power according to the distance between Alice and Bob. Fig. 8(b) shows the average photon number $n_B^* = \eta_y n_A^*$ of the received pulse. As seen from the figure, in the loss-independent region, n_B^* is kept unchanged even if the attenuation varies, while this value slightly decreases but remains at few photons in the noise-limited region, so that only Bob can discriminate the received signal from the noises but Eve should not so. In contrast to the average photon number behaviors, the optimal input probability q^* behaves in a way showing no significant difference between the secrecy rate and channel capacity, as shown in Fig. 8(c).

3.3. Secrecy Rate of Wiretap Channel Coding and Secure key Rate of QKD

In Fig. 9, we show simultaneously in the same graph the secrecy rate obtained in the previous subsection and the secure key rate of QKD schemes. The secrecy rate measures a message rate of wiretap channel coding for one-way transmission, while the secure key rate of QKD does a rate of key exchange with quantum channel and an authenticated public (classical) channel. The two schemes are based on different assumptions on Eve. Fig. 9 aims at showing how we can increase the rate and distance of FSO links with ITS by compromising the assumption on Eve within reasonable practical conditions.

The curve labeled with “decoyed BB84” shows a theoretical prediction of the secure key rate via BB84 [16] employing the decoy-pulse method [26]. Here, we assume an ideal linear

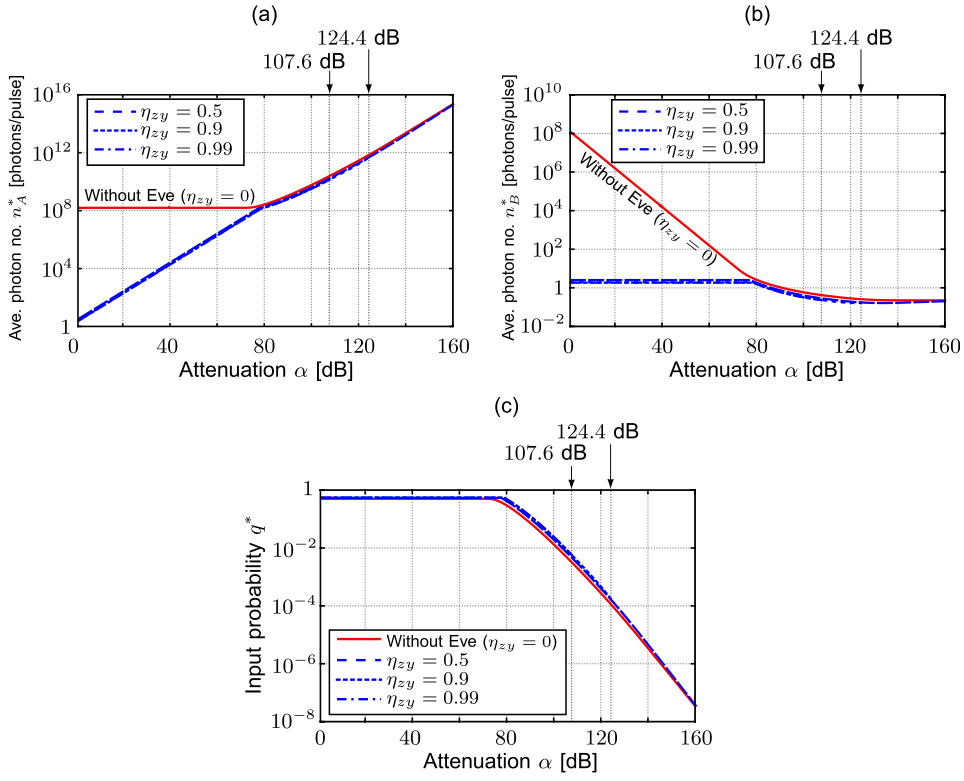


Fig. 8. Optimal parameters for the secrecy rate R_S in Fig. 7. Since the secrecy rate decreases to 0, the curves for $\eta_{zy} = 0.9$ and $\eta_{zy} = 0.99$ are shown up to $\alpha = 124.4$ dB and 107.6 dB, respectively. The solid line denotes the parameter for the case without Eve ($\eta_{zy} = 0$), which leads to the channel capacity C. (a) Average photon number n_A^* of the input pulse. (b) Average photon number n_B^* of the received pulse. (c) Input probability q^*.

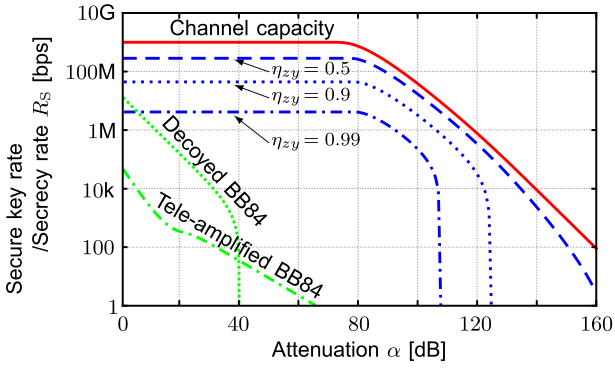


Fig. 9. Secrecy rate R_S and secure key rate of QKD (BB84 [16] protocol). Parameters for wiretap channel: $P = 10$ mW, $\lambda_y = 10$ kcps, $\lambda_z = 1$ cps, and $\Delta = 1$ ns. Parameters for QKD: pulse generation rate = 1 GHz and DCR of a detector = 100 cps.

attenuation channel and a single photon detector with a repetition rate of 1 GHz and a DCR of 100 cps, which is a typical DCR for the current QKD systems. This figure indicates that the secure key rate rapidly falls down at a distance of 40 dB attenuation, which is roughly the best link budget for a low earth orbit (LEO) to ground distance in optical space communications [27].

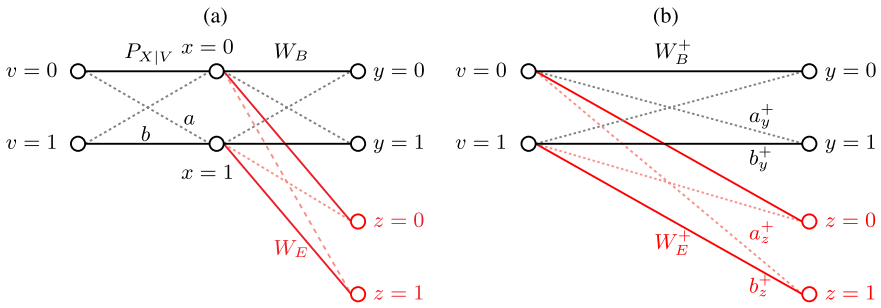


Fig. 10. (a) Channel diagram of the wiretap channel with an auxiliary random channel $P_{X|V}$. (b) Channel diagram of the concatenated channels W_B^+, W_E^+.

Although quantum relay based on tele-amplification [28] has been proposed for extending a QKD distance (see the curve labeled with "tele-amplified BB84"), the secure key rate is always sacrificed while extending the transmission distance.

On the other hand, as shown in Fig. 9, the secrecy rate R_S (blue lines) can cover a wider range in which QKD hardly generates the secure key even for the relative transmittance as high as $\eta_{zy} = 0.99$ for the case where Eve can obtain 99% as much power as Bob. Fig. 9 shows FSO links with ITS is possible even at $\alpha = 80$ dB which roughly corresponds to the best link budget for a GEO-ground distance. Consequently, wiretap channel coding is potentially a promising candidate for realization of the global scale secure network based on FSO communications.

4. Secrecy Capacity

In this section, we extend the analysis to full optimization of secrecy rate by introducing the auxiliary random variable V at Alice, as was formulated by Csiszár and Körner [10] and study the secrecy capacity. This scheme requires us to concatenate an additional channel $P_{X|V}$ to the main channel W_B and the wiretapper channel W_E, respectively. We reformulate the previous tools, present numerical results, and clarify the functional meaning and quantitative effects of the auxiliary random variable V.

4.1. Power Constraint and Channel Matrices

Similarly to the model in Section 2, Alice generates the on- and off-signals corresponding to encoding symbols "1" and "0" with probabilities q and $1-q$, respectively. Then, Alice inputs the sequences into the wiretap channel with picking a symbol and flipping it randomly. Here, the encoding and input symbols are modeled by the auxiliary random variable V and the input random variable X, respectively (more formally, the random variables form a Markov chain V–X–YZ). Since the number taken by the elements of the auxiliary random variable V need not exceed that of the input random variable X [29], we consider the case where V, X, Y, and Z are all binary, as illustrated in Fig. 10(a). The auxiliary channel $P_{X|V}$ from V to X can be modeled by the channel matrix elements with any constants $0 < a, b < 1$ as follows:

$$P_{X|V}(1|0) = a, \quad P_{X|V}(1|1) = b. \tag{14}$$

Then, the probability of the input pulse into the wiretap channel is $q^+ \equiv (1-q)a + q(1-b)$ in each time slot. Thus, the power constraint of (3) which is imposed on X is rewritten as

$$q^+ \frac{n_A h f_0}{\Delta} \leq P. \tag{15}$$

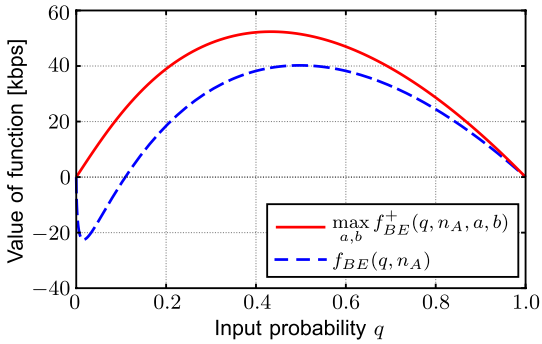


Fig. 11. Comparison of $\max_{a,b} f^+_{BE}(q, n_A, a, b)$ with $f_{BE}(q, n_A)$ varying the input probability q. Parameters: $n_B = 3.2 \times 10^{-3}$ photons/pulse, $\eta_{zy} = 0.95$, $\lambda_y = 10$ kcps, $\lambda_z = 1$ cps, and $\Delta = 1$ ns.

Effectively, we can consider the concatenated channels W_B^+ from V to Y and W_E^+ from V to Z as shown in Fig. 10(b). Given the main channel W_B and the auxiliary channel $P_{X|V}$, the conditional probability of the concatenated channel W_B^+ can be written as

$$W_B^+(y|v) = \sum_{x \in \{0,1\}} W_B(y|x) P_{X|V}(x|v). \tag{16}$$

The channel matrix of W_B^+ is given by

$$W_B^+(1|0) = (1-a)a_y + ab_y \equiv a_y^+, \quad W_B^+(0|0) = 1 - a_y^+$$
$$W_B^+(1|1) = (1-b)a_y + bb_y \equiv b_y^+, \quad W_B^+(0|1) = 1 - b_y^+.$$

Likewise, the channel matrix of the concatenated channel W_E^+ is given by

$$W_E^+(1|0) = (1-a)a_z + ab_z \equiv a_z^+, \quad W_E^+(0|0) = 1 - a_z^+$$
$$W_E^+(1|1) = (1-b)a_z + bb_z \equiv b_z^+, \quad W_E^+(0|1) = 1 - b_z^+.$$

4.2. Secrecy Capacity

With the channel matrices given in the previous subsection, the secrecy capacity C_S is defined and computed as the simultaneous optimization over q, n_A, a, and b

$$C_S = \max_{q, n_A, a, b} f^+_{BE}(q, n_A, a, b) \tag{17}$$

where the function $f^+_{BE}(q, n_A, a, b)$ is defined to be

$$f^+_{BE}(q, n_A, a, b) \equiv f^+_B(q, n_A, a, b) - f^+_E(q, n_A, a, b) \tag{18}$$

and $f^+_B(q, n_A, a, b)$ and $f^+_E(q, n_A, a, b)$ are the mutual information

$$f^+_B(q, n_A, a, b) \equiv h_2\Big((1-q)a_y^+ + q\Big(1 - b_y^+\Big)\Big) - (1-q)h_2\Big(a_y^+\Big) - qh_2\Big(b_y^+\Big) \tag{19}$$
$$f^+_E(q, n_A, a, b) \equiv h_2\big((1-q)a_z^+ + q(1 - b_z^+)\big) - (1-q)h_2(a_z^+) - qh_2(b_z^+) \tag{20}$$

where n_A intervenes through a_y, b_y, a_z, b_z.

In Fig. 11, we compare the function $\max_{a,b} f^+_{BE}(q, n_A, a, b)$ (solid line) optimized over a and b with $f_{BE}(q, n_A)$ (dashed line) for a wiretap channel which is not more capable. The figure indicates that $\max_{a,b} f^+_{BE}(q, n_A, a, b)$ is strictly positive for any input probability $q \in \{0, 1\}$, whereas $f_{BE}(q, n_A)$ becomes negative for small q. Moreover, $\max_{a,b} f^+_{BE}(q, n_A, a, b)$ is larger than

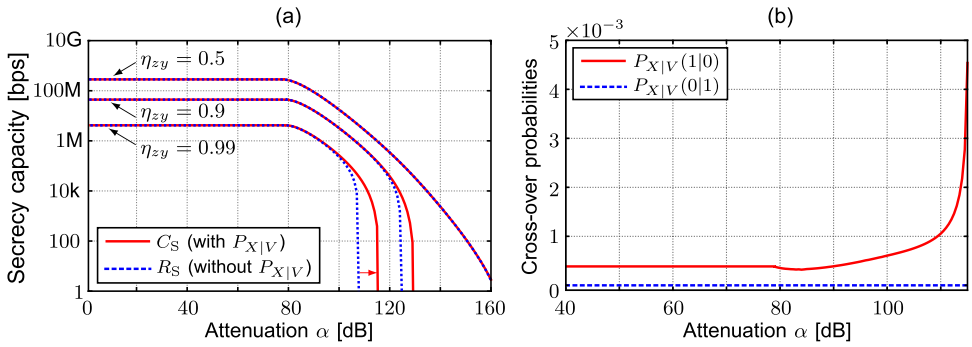


Fig. 12. (a) Secrecy capacity C_S as a function of attenuation $\alpha = -\log_{10}\eta_y$. For comparison, the secrecy rate R_S is also shown. Parameters: $P = 10$ mW, $\lambda_y = 10$ kcps, $\lambda_z = 1$ cps, and $\Delta = 1$ ns. (b) Optimal cross-over probabilities $P_{X|V}(1|0) = a$ and $P_{X|V}(0|1) = 1 - b$ for $\eta_{zy} = 0.99$.

$f_{BE}(q, n_A)$ at any input probability $q \in \{0, 1\}$. The extension in the transmission distance that will be shown later should be attributed to this increase of the value caused by the auxiliary random variable V.

4.3. Numerical Evaluation

In this subsection, we numerically demonstrate the improvement of transmission distance due to the concatenation of the auxiliary channel $P_{X|V}$. In Fig. 12(a), we compare the secrecy capacity C_S (solid lines) based on (17) with the secrecy rate R_S (dashed lines) based on (9) which was investigated in Sections 2 and 3 (see Fig. 7). According to the figure, the auxiliary random variable V brings about the improvement of transmission distance in the noise limited region, e.g., for $\eta_{zy} = 0.99$, the attenuation α at which the secrecy rate sharply falls is improved by 6 dB, which is equivalent to 40% extension of the transmission distance. This effect becomes significant for larger values of the relative transmittance η_{zy}.

Fig. 12(b) shows the optimal cross-over probabilities $P_{X|V}(1|0) = a$ and $P_{X|V}(0|1) = 1 - b$ for $\eta_{zy} = 0.99$ in Fig. 12(a). Here, $P_{X|V}(1|0)$ is the probability of flipping "0" (off-signal) into "1" (on-signal) and $P_{X|V}(0|1)$ is vice versa. As seen in Fig. 12(b), $P_{X|V}(1|0)$ is non-zero and increases drastically in the noise-limited region, whereas $P_{X|V}(0|1)$ stays 0.

The effect of the auxiliary randomness generated at the sender on the performance has been investigated especially in the multiple receivers scenario [15], [30], [31], namely, the artificial noise is created such that it degrades Eve's channel but does not affect the main channel through the use of the interference effect among the receivers. In contrast to such studies, Fig. 12(b) reveals that the addition of the random pulses has a crucial role in the proposed method. In our case, Eve who may have the less noisy detector than Bob can be further deceived by the dummy pulses that act as extra noises, and the performance is enhanced. This means that the proposed method bears a remarkable resemblance to the decoy method employed in BB84 [26]. In this method, Alice varies the average photon number of each signal pulse randomly among the prescribed levels, thus Eve is prevented from wiretapping the signal pulses, and the security and the transmission distance is boosted.

5. Finite Length Analysis

5.1. Formulation

Although the secrecy capacity investigated in the last section is considered as a reasonable benchmark of the system, it concerns only the achievable rate in the asymptotic limit at code

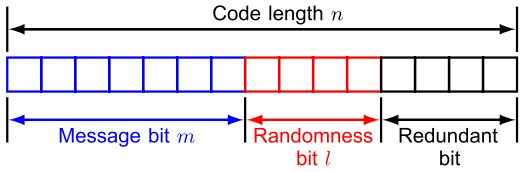


Fig. 13. Conceptual codeword structure of a wiretap channel code.

length $n \to \infty$ and contains no information about practical code construction of finite length n. In this section, in order to estimate required resources for the given levels of reliability for Bob and secrecy against Eve, we introduce a stronger characterization showing how fast the decoding error probability and the leaked information decrease.

As depicted schematically in Fig. 13, a wiretap channel code consists of three types of bits, i.e., m bits conveying the confidential information, l bits as the random dummy information to deceive Eve, and $n - m - l$ redundant bits to perform error correction. Here, let $R_B = m/n$ and $R_E = l/n$ be the coding rate and the randomness rate, respectively.

For such a code, we introduce the measures on the decoding error probability ε_n^B and the leaked information δ_n^E. Given an output via the main channel due to message i from the message set $\mathcal{M}_n$, Bob computes an estimate $\hat{i}$ of message i with his decoder. The decoding error probability ε_n^B is measured as

$$\varepsilon_n^B \equiv \frac{1}{|\mathcal{M}_n|} \sum_{i \in \mathcal{M}_n} \Pr\{i \neq \hat{i}\} \tag{21}$$

where $|\mathcal{M}_n|$ denotes the number of messages included in $\mathcal{M}_n$ and $\Pr\{\cdot\}$ denotes the probability of an event. Also, the leaked information δ_n^E against Eve is measured as

$$\delta_n^E \equiv \frac{1}{|\mathcal{M}_n|} \sum_{i \in \mathcal{M}_n} D\left(P_n^{(i)} \| \pi_n\right) \tag{22}$$

where $D(P_n^{(i)} \| \pi_n)$ is the Kullback-Leibler distance [29] between the output probability distribution $P_n^{(i)}$ via the wiretapper channel due to message i and the target output probability distribution π_n which is generated via the wiretapper channel due to an arbitrarily prescribed input distribution.

According to the theory of wiretap channel coding [21], there exists a code with length n attaining the following upper bounds on the error probability ε_n^B and the leaked information δ_n^E:

$$\varepsilon_n^B \leq 2e^{-nF_c(q,R_B,R_E)}, \quad \delta_n^E \leq 2e^{-nH_c(q,R_E)} \tag{23}$$

where the exponents $F_c(q, R_B, R_E)$ and $H_c(q, R_E)$ are referred to as the error exponent and the secrecy exponent defined as

$$F_c(q, R_B, R_E) \equiv \sup_{r \geq 0} \sup_{0 \leq \rho \leq 1} [\phi(\rho | W_B, q, r) - \rho(R_B + R_E)] \tag{24}$$

$$H_c(q, R_E) \equiv \sup_{r \geq 0} \sup_{0 < \rho < 1} [\phi(-\rho | W_E, q, r) + \rho R_E] \tag{25}$$

respectively. It is known that the error exponent $F_c(q, R_B, R_E)$ is a monotone strictly positive decreasing in $R_B + R_E < I(X; Y)$ and becomes 0 for $R_B + R_E \geq I(X; Y)$. Conversely, the secrecy exponent $H_c(q, R_E)$ is a monotone strictly positive increasing in $R_E > I(X; Z)$ and becomes 0 for $R_E \leq I(X; Z)$.

Here, $\phi(\rho | W_B, q, r)$ in (24) and $\phi(-\rho | W_E, q, r)$ in (25) are functions of the given channels W_B, W_E and the input probability q. For the wiretap channel based on the OOK considered in

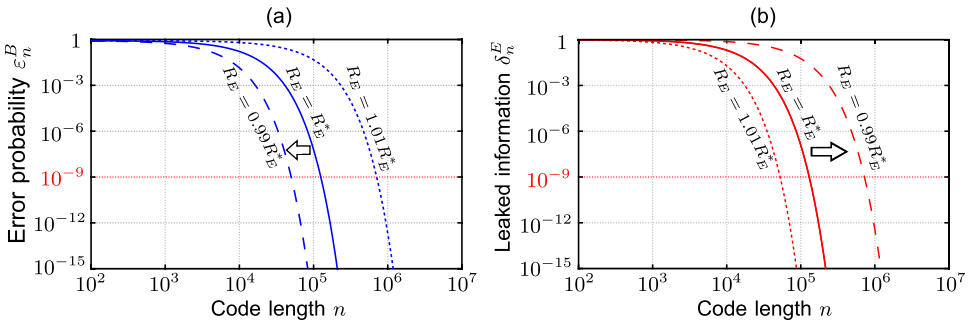


Fig. 14. Code length dependence of (a) error probability ε_n^B and (b) leaked information δ_n^E. The coding rate is fixed as to be $R_B^* = 0.5\ R_S = 22.1$ Mbps (see Fig. 7). The arrows denote the change of the code length dependence when the randomness rate decreases by 1% from $R_E^* = 0.641$ Gbps.

this paper, these functions are given as

$$\phi(\rho|W_B,q,r) \equiv -\log\left[\left(qb_y^{\frac{1}{1+\rho}}e^{r\left(P-\frac{n_A^*hf_0}{\Delta}\right)}+(1-q)a_y^{\frac{1}{1+\rho}}e^{rP}\right)^{1+\rho}\right.$$
$$\left.+\left(q(1-b_y)^{\frac{1}{1+\rho}}e^{r\left(P-\frac{n_A^*hf_0}{\Delta}\right)}+(1-q)(1-a_y)^{\frac{1}{1+\rho}}e^{rP}\right)^{1+\rho}\right] \tag{26}$$

$$\phi(-\rho|W_E,q,r) \equiv -\log\left[\left(qb_z^{\frac{1}{1-\rho}}e^{r\left(P-\frac{n_A^*hf_0}{\Delta}\right)}+(1-q)a_z^{\frac{1}{1-\rho}}e^{rP}\right)^{1-\rho}\right.$$
$$\left.+\left(q(1-b_z)^{\frac{1}{1-\rho}}e^{r\left(P-\frac{n_A^*hf_0}{\Delta}\right)}+(1-q)(1-a_z)^{\frac{1}{1-\rho}}e^{rP}\right)^{1-\rho}\right]. \tag{27}$$

The arbitrary constant $r \geq 0$ is optimized so that each exponent be maximized. The authors of [21] have derived exponents for the wiretap channel with the auxiliary channel $P_{X|V}$. In this paper, however, we only pay attention to the wiretap channel without $P_{X|V}$ for simplicity.

5.2. Code Length Dependence of Error Probability and Leaked Information

For a practical code of finite length n, the coding rate R_B cannot be arbitrarily close to the secrecy capacity (or secrecy rate), as well as the error probability ε_n^B and the leaked information δ_n^E cannot be infinitesimally small. In order to design the practical wiretap channel codes, the coding rate R_B should be compromised to be much lower than the secrecy capacity, and then the necessary code length n for the required levels of ε_n^B and δ_n^E should be investigated. This is actually the motivation to introduce the error exponent $F_c(q,R_B,R_E)$ and the secrecy exponent $H_c(q,R_E)$ [32]–[34]. Although some previous studies (e.g., [25]) have revealed that the secrecy capacity can be asymptotically achieved with constructive codes, the evaluation of both ε_n^B and δ_n^E for finite length codes has never been investigated to our best knowledge.

In Fig. 14, we show the upper bounds on ε_n^B and δ_n^E based on (23) choosing the case of the loss-independent region with $\alpha = 70$ dB and $\eta_{zy} = 0.9$. We again adopt a set of parameters as $P = 10$ mW, $\lambda_y = 10$ kcps, $\lambda_z = 1$ cps, and $\Delta = 1$ ns, which are the same as in Section 3. The secrecy rate R_S is 44.2 Mbps and the optimum parameters are $n_A^* = 1.94 \times 10^7$, $q^* = 0.544$ (see Figs. 7 and 8).

We fix the coding rate $R_B^* = 22.1$ Mbps as to be the half of the secrecy rate R_S. The solid line denotes the case of $R_E^* = 0.641$ Gbps which is set so that $F_c(q,R_B^*,R_E^*) = H_c(q,R_E^*) = 1.59 \times 10^{-4}$,

TABLE 1

Rates and exponents for Fig. 14

	R_E [Gbps]	$R_B^* + R_E$ [Gbps]	$F_c(q, R_B, R_E)$	$H_c(q, R_E)$
$R_E = R_E^*$	0.641	0.663	1.59×10^{-4}	1.59×10^{-4}
$R_E = 0.99R_E^*$	0.634	0.656	4.00×10^{-4}	0.29×10^{-4}
$R_E = 1.01R_E^*$	0.647	0.669	0.28×10^{-4}	3.94×10^{-4}

as shown in Table 1. As seen in this figure, both ε_n^B and δ_n^E begin to decrease rapidly over $n = 10^4$ and reach the standard error-free criterion $\varepsilon_n^B < 10^{-9}$ and the leaked information criterion $\delta_n^E < 10^{-9}$ at around $n = 10^5$, which is the reasonable code length compared with the current technology. In the standard channel coding without Eve, ε_n^B can be reduced arbitrarily by lowering the coding rate R_B with fixing the code length. However, in the wiretap channel coding, since R_E should be kept larger than the mutual information $I(X;Z)$ for the secrecy against Eve, it is not obvious whether there is a code of reasonable length n which satisfies the required levels of both ε_n^B and δ_n^E. Fig. 14 provides the significant knowledge on this point, namely, even for the relative transmittance $\eta_{zy} = 0.9$ which corresponds to the case where Eve can wiretap much power, there is a practical code with sufficiently small ε_n^B and δ_n^E.

In Fig. 14, the dashed line labeled with "$R_E = 0.99R_E^*$" illustrates the case where R_E is set to be 99% of R_E^*. As shown in Table 1, $F_c(q, R_B, R_E)$ increases compared to the case of R_E^* because of its monotonicity in $R_B + R_E$. This brings a decrease in ε_n^B as denoted by the arrow in the figure. On the other hand, $H_c(q, R_E)$ decreases because of its monotonicity in R_E and δ_n^E increases. As seen in the figure, ε_n^B reaches 10^{-9} around at $n = 7 \times 10^4$, which is shorter than the case of R_E^*. On the other hand, δ_n^E reaches only 10^{-1} with this code length. In order to reach $\delta_n^E < 10^{-9}$, a much longer code length of $n \geq 9 \times 10^5$ is required. In contrast to the above case, the dotted line labeled with "$R_E = 1.01R_E^*$" illustrates the case where R_E is set to be 101% of R_E^*. In this case, ε_n^B increases whereas δ_n^E decreases as shown in the figure.

Intuitive examples of the above discussion are as follows; in order to relax the implementation cost of codes, one may wish to change the criteria for the secrecy according to the level of confidentiality of information. In the opposite case, more secure codes may be required to establish secure links leaving the complexity of implementation out of consideration. The discussion in this subsection provides the quantification of such an adaptive change of the performances. In other words, we characterize another clue for controlling the tradeoff between performance and code length via the upper bounds in (23), which is more practical than other examples of tradeoff relation provided in [21], [22].

6. Conclusion

In this paper, we have studied the performance of physical layer security of FSO communications based on the OOK modulation with linear attenuation and background noises, using the secrecy capacity and the code length dependence of the error probability and the leaked information as performance metrics. Although we have mainly focused on the idealistic setting, i.e., without fading, we have numerically shown that the global scale network with ITS would be potentially realized by wiretap channel coding with currently available technologies and there exists a wiretap channel code of a practical length.

We have numerically investigated the secrecy rates and the secrecy capacity and clarified its unique features as follows: (a) Unless the transmission power is regulated optimally, these quantities dramatically drop in the small attenuation region and (b) transmission distance of our proposed method can be much longer than that of QKD even when Eve can obtain 99% as much the fraction of power as Bob. We have also shown that the transmission distance can be extended by introducing the auxiliary random variable V at Alice [10] if the wiretap channel is not more capable. The random additional pulses resulting from the auxiliary channel $P_{X|V}$ play

an essential role in deceiving Eve when the SNR at Bob is worse, which implies the similarity to the decoy method employed in QKD. This physical implication of the effect of the auxiliary random variable has not been explicitly demonstrated so far.

Further, on the basis of the past theoretical study [21], we have introduced the error exponent $F_c(q, R_B, R_E)$ and the secrecy exponent $H_c(q, R_E)$ for our proposed method. We have provided the characterization of such exponents in terms of the code length dependence of the error probability ε_n^B and the leaked information δ_n^E. The code length dependence of ε_n^B and δ_n^E provides (a) the evaluation of ε_n^B and δ_n^E for practical codes of finite length and (b) the necessary code length to satisfy the required levels of both ε_n^B and δ_n^E. Our calculation has indicated the existence of a practical code with the reasonable length and the sufficient performance, even for the case where Eve can obtain 90% as much power as Bob.

There might be many interesting problems left open. We mention two of them. First, our analysis should be extended to include the fading effect. The received signal intensity through a typical FSO channel fluctuates in a time scale of millisecond due to atmospheric scintillation. A straightforward way is to model this fluctuation by renormalizing the noise variance in a log-normal fading distribution, which leads to the degradation of overall performances. A more sophisticated approach is an adaptive scheme. If the CSI can be estimated by Alice, the transmission power can be allocated opportunistically to the instantaneous fading realizations for which Eve obtains a lower instantaneous SNR than that of Bob. As a result, strictly positive secrecy rates are achievable even if, on average, Eve obtains a better SNR than that of Bob [11], [12]. However, this adaptive scheme requires a fast feedforward mechanism in the millisecond time scale and remains a challenge.

Second and finally, multiple colluding eavesdroppers are a likely risk in an FSO link. One can easily imagine that multiple drones tap various places in the FSO link, and collude for getting information. Countermeasures should not be simple, and be sought from the viewpoint not only of coding schemes but of system level solution like monitoring and alarming functions as well.

In spite of such a challenging problem to which we should address in the future, we believe that the potential performances of physical layer security of FSO communications presented in this paper provide insight into a new direction for secure communications. For example, it is noteworthy that performances of physical layer security of FSO channels and QKD are regarded as complementary technologies in the sense of the tradeoff between security level and usability. Thus, they will eventually be integrated to realize high capacity optical communications with ITS and such a combination should provide the new paradigm of secure communications.

References

[1] M. Toyoshima, "Trends in satellite communications and the role of optical free-space communications (invited paper)," *J. Opt. Commun. Netw.*, vol. 4, no. 6, pp. 300–311, 2005.
[2] M. Toyoshima *et al.*, "Special issue on the optical inter-orbit communications engineering test satellite (OICETS)—development and in-orbit experiments," *J. Nat. Inst. Inf. Commun. Technol.*, vol. 59, no. 1/2, pp. 125–134, Mar./Jun. 2012.
[3] X. Sun *et al.*, "Free space laser communication experiments from earth to the lunar reconnaissance orbiter in lunar orbit," *Opt. Exp.*, vol. 21, no. 2, pp. 1865–1871, Jan. 2013.
[4] D. M. Boroson, "Overview of the lunar laser communication demonstration," in *Proc. ICSOS*, May 7–9, 2014, pp. 1–7.
[5] J. C. Juarez *et al.*, "Free-space optical communications for next-generation military networks," *IEEE Commun. Mag.*, vol. 44, no. 11, pp. 46–51, Nov. 2006.
[6] D. Kedar and S. Arnon, "Urban optical wireless communication networks the main challenges and possible solutions," *IEEE Commun. Mag.*, vol. 42, no. 5, pp. S2–S7, May 2004.
[7] M. Agaskar and V. W. S. Chan, "Nulling strategies for preventing interference and interception of free space optical communication," in *Proc. IEEE ICC*, Jun. 9–13, 2013, pp. 2520–2525.
[8] A. Puryear and V. W. S. Chan, "Using spatial diversity to improve the confidentiality of atmospheric free space optical communication," in *Proc. IEEE GLOBECOM*, Dec. 5–9, 2011, pp. 1–6.
[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[10] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, Mar. 1978.
[11] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[12] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[13] 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.*, vol. 6, no. 12, pp. 1072–1081, Dec. 2014.
[14] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photon. J.*, vol. 7, no. 2, pp. 1–14, Apr. 2015.
[15] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Proc. IEEE ICC*, Jun. 10–14, 2014, pp. 3342–3347.
[16] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process*, Dec. 10–12, 1984, pp. 175–179.
[17] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.
[18] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.
[19] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, pp. 1–37, Jul. 2009.
[20] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, May 2011.
[21] T. S. Han, H. Endo, and M. Sasaki, "Reliability and secrecy functions of the wiretap channel under cost constraint," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6819–6843, Nov. 2014.
[22] T. H. Chou, S. C. Draper, and A. M. Sayeed, "Key generation using external source excitation: Capacity, reliability, and secrecy exponent," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2455–2474, Apr. 2012.
[23] Y. M. Kabanov, "The capacity of a channel of the Poisson type," *Theory Probab. Appl.*, vol. 23, no. 1, pp. 143–147, 1978.
[24] A. D. Wyner, "Capacity and error exponent for the direct detection photon channel—Part I," *IEEE Trans. Inf. Theory*, vol. 34, no. 6, pp. 1449–1461, Nov. 1988.
[25] A. Laourine and A. B. Wagner, "The degraded Poisson wiretap channel," *IEEE Trans. Inf. Theory*, vol. 58, no. 12, pp. 7073–7085, Dec. 2012.
[26] W. Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, pp. 1–4, Aug. 2003.
[27] M. Sasaki *et al.*, "Quantum photonic network: Concept, basic tools, and future issues (invited paper)," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 1–13, Nov. 2014.
[28] J. S. Neergaard-Nielsen, Y. Eto, C.-W. Lee, H. Jeong, and M. Sasaki, "Quantum tele-amplification with a continuous-variable superposition state," *Nat. Photon.*, vol. 7, pp. 439–443, May 2013.
[29] I. Csiszár and J. Körner, *Information Theory: Coding Theorem for Discrete Memoryless Systems*. New York, NY, USA: Academic, 1981.
[30] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE VTC–Fall*, Sep. 25–28, 2005, vol. 3, pp. 1906–1910.
[31] A. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP*, Apr. 19–24, 2009, pp. 2437–2440.
[32] R. G. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: Wiley, 1968.
[33] I. Csiszár, "Almost independence and secrecy capacity," *Probl. Inf. Transmiss.*, vol. 32, no. 1, pp. 48–57, 1996.
[34] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3989–4001, Jun. 2011.