Physical-Layer Security for Indoor Visible Light Communications: Secrecy Capacity Analysis

Jin-Yuan Wang, Member, IEEE, Cheng Liu, Jun-Bo Wang, Member, IEEE, Yongpeng Wu, Senior Member, IEEE, Min Lin, Member, IEEE, and Julian Cheng, Senior Member, IEEE

Abstract—This paper investigates the physical-layer security for an indoor visible light communication network consisting of a transmitter, a legitimate receiver, and an eavesdropper. Both the main channel and the wiretapping channel have non-negative inputs, which are corrupted by additive white Gaussian noises. Considering the illumination requirement and the physical characteristics of lighting source, the input is also constrained in both its average and peak optical intensities. Two scenarios are investigated: one is only with an average optical intensity constraint and the other is with both average and peak optical intensity constraints. Based on the information theory, closed-form expressions of the upper and lower bounds on secrecy capacity for the two scenarios are derived. Numerical results show that the upper and lower bounds on secrecy capacity are tight, which validates the derived closed-form expressions. Moreover, the asymptotic behaviors in the high signal-to-noise ratio (SNR) regime are analyzed from the theoretical aspects. At high SNR, when only considering the average optical intensity constraint, a small performance gap exists between the asymptotic upper and lower bounds on secrecy capacity. When considering both average and peak optical intensity constraints, the asymptotic upper and lower bounds on secrecy capacity coincide with each other. These conclusions are also confirmed by numerical results.

Index Terms—Gaussian noise, physical-layer security, secrecy capacity, visible light communications.

I. INTRODUCTION

WITH THE widespread use of light-emitting diodes (LEDs) for commercial lighting applications, visible light communication (VLC) has attracted increasing attention in recent years. Due to the combination of communication and illumination, VLC is regarded as one of the most important wireless communication technologies for future indoor access [1].

In the last decade, the point-to-point (P2P) VLC has achieved rapid development in many fields, especially in channel modelling [2], modulation [3], coding [4], equalization [5], channel estimation [6], indoor positioning [7], channel capacity analysis [8]–[11] and transceiver design [12]. At present, the research focus of VLC is being changed from P2P communications to network aspects. In VLC networks, data privacy is becoming a main concern for users. Although it is propagated via the line-of-sight path, the VLC signal is broadcasted to all users illuminated by the LEDs. Such a broadcast feature provides convenience for data transmission, but it also offers an opportunity for unintended users to eavesdrop the information, which imposes a security risk to legitimate users. Therefore, information security becomes an urgent issue to be addressed. Traditional security schemes are performed at upper-layers of the network stack by using access control, password protection and end-to-end encryption [13]. The safety of traditional security schemes is built on the limited storage capacity and computational power of the eavesdroppers. Recently, physical-layer (PHY) security, which exploits the channel characteristics to hide information from eavesdroppers and does not rely on the upper-layer encryption, has been proposed as an efficient supplement to traditional security schemes.

Secure transmission is important for radio frequency wireless communications (RFWC). The PHY security was first investigated in 1949 by Shannon, who proposed the concept of perfect secrecy over noiseless channels [14]. Under the noisy channels, Wyner analyzed the secrecy capacity via the wiretap channel [15]. In [16], the secrecy capacity of the single-input single-output (SISO) Gaussian wiretap channel was derived. Under the non-degraded wiretap channel, a single-letter
characterization of the secrecy capacity was derived in [17]. Recently, the secrecy performance analysis over the SISO scenario was extended to that over the multi-input multi-output (MIMO) scenario. For MIMO wiretap channels with confidential messages, Liu and Poor [18] analyzed the secrecy capacity region. For artificial noisy MIMO channels, the secrecy capacity was studied in [19] by using the ordered eigenvalues of Wishart matrices. Shlezinger et al. [20] obtained the secrecy capacity for MIMO channels with finite memory. With the help of a cooperative jammer, a lower bound of the secrecy capacity for the MIMO channels was derived in [21].

Although much work has been done to investigate the secrecy capacity for RFWC, the developed theory is not directly applicable to VLC. The main differences between RFWC and VLC are highlighted as follows. First, the transmit signal in RFWC can be bipolar or unipolar, while the signal in VLC must be unipolar because the optical intensity is typically used to carry information. Moreover, the average power in RFWC is the mean square value of a signal, but the average power in VLC is the mean value of the signal [22]. Also, a lower average power is usually preferred for RFWC, but VLC has a predefined average intensity according to the dimming target, which is not an objective function but a constraint [22]. Therefore, the aforementioned features should be considered for practical VLC. In [23], the secrecy capacity was analyzed for direct current biased VLC, where a uniform input distribution is used to derive the lower bound of secrecy capacity. In [24], the secrecy capacity of multiple-input single-output (MISO) VLC channels was investigated, where the input distribution was chosen as a truncated generalized normal (TGN) distribution. To obtain the optimal and robust beamforming, Arfaoui et al. [25] also employed the TGN distribution for the input. Due to the constraints of the input signal in VLC, the uniform and TGN input distributions are generally not optimal [8], [10]. By using the variational method, an improved input distribution can be obtained [8], [10]. By employing a discrete input distribution, the authors in [26] derived an upper bound on the secrecy capacity for the MISO VLC channels. However, the theoretical expression of the secrecy capacity is not obtained. In [27], the secrecy outage probability (SOP) was analyzed for a hybrid VLC-RFWC system with energy harvesting. In [28], the SOP and the average secrecy capacity were discussed for VLC with spatially random terminals. Note that the dimming requirement for indoor VLC was not considered in [27] and [28]. In our previous work [29], three lower bounds on the secrecy capacity were obtained. However, no upper bound has been obtained. Moreover, the peak optical intensity constraint is not considered. To the best of the authors’ knowledge, the secrecy capacity for VLC has not been systematically investigated.

In this paper, the secrecy capacity for an indoor VLC system with a transmitter, a legitimate receiver, and an eavesdropper is investigated. The main contributions are summarized as follows:

1) The secrecy capacity for indoor VLC with only an average optical intensity constraint is analyzed. By using the existing channel capacity results, the entropy-power inequality (EPI) and the variational method, two lower bounds on secrecy capacity are obtained. Applying the dual expression of the secrecy capacity, the upper bound on the secrecy capacity is obtained. Numerical results validate the derived closed-form expressions.

2) The secrecy capacity for indoor VLC with both average and peak optical intensity constraints is investigated. In practical VLC, the peak optical intensity of the LED is also limited. By adding a peak optical intensity constraint on the input signal, the lower and upper bounds on the secrecy capacity are further derived, which are in closed forms. The accuracy of the derived closed-form expressions is confirmed by numerical results.

3) The asymptotic behaviors at high signal-to-noise ratio (SNR) are analyzed. Through theoretical analysis, it is shown that the asymptotic lower and upper bounds do not coincide but with a small gap when only considering the average optical intensity constraint. When considering both average and peak optical intensity constraints, the asymptotic lower and upper bounds coincide, and thus the secrecy capacity can be obtained precisely.

The reminder of this paper is organized as follows. Section II describes the system model. With different constraints, the secrecy capacity bounds and the asymptotic behavior are analyzed in Section III and Section IV, respectively. Numerical results are presented in Section V. Conclusions and future directions are presented in Section VI.

Notations: Throughout this paper, italicized symbols denote scalar values; \( N \left( \bar{0}, \sigma^2 \right) \) stands for a Gaussian distribution with zero mean and variance \( \sigma^2 \); \( E(\cdot) \) denotes the expectation operator; \( \text{var}(\cdot) \) denotes the variance of a variable; \( f_X(x) \) denotes the probability density function (PDF) of \( X \). We use \( H(\cdot) \) for the entropy, \( D(\cdot \| \cdot) \) for the relative entropy, and \( I(\cdot ; \cdot) \) for the mutual information. We use \( \ln(\cdot) \) for the natural logarithm and \( Q(\cdot) \) for the Gaussian Q-function.

II. System Model

As shown in Fig. 1, we consider an indoor VLC network consisting of a transmitter (i.e., Alice), a legitimate receiver (i.e., Bob), and an eavesdropper (i.e., Eve). Alice is deployed on the ceiling, while Bob and Eve are placed on the floor.

![Fig. 1. An VLC network with one transmitter, one legitimate receiver and one eavesdropper.](image-url)
When Alice transmits data bits to Bob, Eve as a passive eavesdropper can also receive the signals intended for Bob. In the network, Alice is equipped with a single LED to transmit optical intensity signals, while Bob and Eve are equipped with one photodiode (PD) individually to perform the optical-to-electrical conversions. The received signals at Bob and Eve can be expressed, respectively, as

\[
\begin{align*}
Y_B &= H_B X + Z_B \\
Y_E &= H_E X + Z_E,
\end{align*}
\]

where \( X \) is the transmit optical intensity signal; \( H_B \) and \( H_E \) denote the channel gains of the main channel and the eavesdropping channel, respectively; \( Z_B \sim N(0, \sigma_B^2) \) and \( Z_E \sim N(0, \sigma_E^2) \) stand for the additive white Gaussian noises at Bob and Eve, where \( \sigma_B^2 \) and \( \sigma_E^2 \) denote the variances of the noises at Bob and Eve, respectively.

Because the intensity modulation and direct detection is employed for VLC, \( X \) is restricted to be nonnegative such that

\[
X \geq 0.
\]

In practical VLC systems, the peak optical intensity of the LED is also limited. Therefore, the peak optical intensity constraint is given by

\[
X \leq A,
\]

where \( A \) is the peak optical intensity of the LED.

For a practical LED, its average optical intensity is constrained by the nominal optical intensity. In order to satisfy the illumination requirements in VLC, the average optical intensity cannot change with time. Mathematically, the average optical intensity constraint is given by

\[
E(X) = \xi P,
\]

where \( \xi \in (0, 1] \) is the dimming target, \( P \in (0, A] \) is the nominal optical intensity of the LED.

In indoor VLC, the channel gain \( H_k \) \((k = B \text{ or } E)\) can be expressed as [30]

\[
H_k = \left\{ \begin{array}{ll}
\frac{(m + 1)A_k}{2\pi D_k^2} T_A g\cos^n(\varphi_k) \cos(\psi_k), & \text{if } 0 \leq \psi_k \leq \Psi \\
0, & \text{if } \psi_k \geq \Psi
\end{array} \right.
\]

where \( m \) is the order of the Lambert emission; \( A_k \) is the physical area of the PD; \( T_A \) and \( g \) are the optical filter gain and the concentrator gain of the PD. \( \Psi \) is the field of view (FOV) of the PD; \( D_k, \varphi_k \) and \( \psi_k \) are respectively the distance, the irradiance angle and the incidence angle from Alice to Bob \((k = B)\) or Eve \((k = E)\), as shown in Fig. 2. Obviously, when the positions of Alice, Bob and Eve are fixed, the channel gains \( H_B \) and \( H_E \) are constants.

### III. Secrecy Capacity for VLC With Only an Average Optical Intensity Constraint

In this section, we focus on the VLC with only an average optical intensity constraint. Therefore, we only consider the constraints (2) and (4). If the main channel is worse than the eavesdropping channel \((i.e., H_B/\sigma_B < H_E/\sigma_E)\), then the main channel is stochastically degraded with respect to the eavesdropping channel, and the secrecy capacity is essentially zero. Alternatively, if \( H_B/\sigma_B \geq H_E/\sigma_E \), the secrecy capacity can be expressed as [23], [31]

\[
C_s = \max_{f_X(x)} \left[ I(X;Y_B) - I(X;Y_E) \right]
\]

s.t. \( \int_0^\infty f_X(x)dx = 1 \)

\[
E(X) = \int_0^\infty xf_X(x)dx = \xi P,
\]

where \( C_s \) denotes the secrecy capacity, and \( f_X(x) \) denotes the PDF of the input signal. In this section, the lower and upper bounds of the secrecy capacity will be derived. Moreover, the asymptotic behavior of the secrecy capacity is also analyzed.

#### A. Lower Bound on Secrecy Capacity

By using the channel capacity bounds derived in [32], a lower bound on the secrecy capacity is derived as (7) in the following theorem. Moreover, by using the EPI and the variational method, another lower bound on the secrecy capacity is derived as (8) in the following theorem.

Theorem 1: The secrecy capacity for the channel in (1) with constraints (2) and (4) is lower-bounded by each of the following two bounds (7) and (8), i.e.,

\[
C_s \geq \ln \left( \frac{\sigma_E^2 \beta e^{-\frac{\delta^2}{2\sigma_E^2}}}{\beta e^{-\frac{\delta^2}{2\sigma_E^2}} + \sqrt{2\pi} \sigma_E Q\left( \frac{\delta - H_E \xi P}{\sigma_E} \right)} \right) - \frac{1}{2} Q\left( \frac{\delta}{\sigma_E} \right)
\]

\[
- \frac{\delta}{\sqrt{2\pi} \sigma_E} e^{-\frac{\delta^2}{2\sigma_E}} - \frac{\delta^2}{2\sigma_E} Q\left( \frac{\delta + H_E \xi P}{\sigma_E} \right)
\]

\[
- \frac{\delta + H_E \xi P}{\beta} - \frac{\sigma_E}{\sqrt{2\pi} \beta} e^{-\frac{\delta^2}{2\sigma_E^2}},
\]

and

\[
C_s \geq \frac{1}{2} \ln \left( \frac{\sigma_B^2}{2\pi \sigma_B^2} \frac{e^{\xi P^2 H_B^2} + 2\pi \sigma_B^2}{H_E^2 \xi P^2 + \sigma_E^2} \right),
\]

In this paper, the natural logarithms are employed, and thus the secrecy capacity is in nats/transmission.
where $\beta > 0$ and $\delta \geq 0$ in (7) are free parameters. Suboptimal but useful choices for $\beta$ and $\delta$ are given, respectively, by (9) and (10) as shown at the top of this page.

Proof: See Appendix A and Appendix B.

Remark 1: When $\sqrt{\pi H_B} > H_E$, it is obvious that the lower bound (8) is a monotonically increasing function with respect to the dimming target $\xi$. In this case, the performance of (8) can be improved by increasing the value of $\xi$. Moreover, it is challenging to analyze the monotonicity of the lower bound (7) with respect to $\xi$, which will be given by using a numerical method in Section V.

B. Upper Bound on Secrecy Capacity

To obtain the upper bound on the secrecy capacity, the dual expression of the secrecy capacity is employed [33]. For an arbitrary conditional PDF $g_{Y_B|Y_E}(y_B|y_E)$, the following equality always holds [34]

$$I(X;Y_B|Y_E) + E_{X|Y_E} \left( D \left( f_{Y_B|Y_E}(y_B|y_E)||g_{Y_B|Y_E}(y_B|y_E) \right) \right) = E_{X|Y_E} \left( D \left( f_{Y_B|X,Y_E}(y_B|x,y_E)||g_{Y_B|Y_E}(y_B|y_E) \right) \right).$$

(11)

According to the non-negativity property of the relative entropy, we have

$$I(X;Y_B|Y_E) \leq E_{X|Y_E} \left( D \left( f_{Y_B|X,Y_E}(y_B|x,y_E)||g_{Y_B|Y_E}(y_B|y_E) \right) \right).$$

(12)

Note that selecting any $g_{Y_B|Y_E}(y_B|y_E)$ will result in an upper bound of $I(X;Y_B|Y_E)$. Therefore, we have

$$I(X;Y_B|Y_E) = \min_{g_{Y_B|Y_E}(y_B|y_E)} E_{X|Y_E} \left( D \left( f_{Y_B|X,Y_E}(y_B|x,y_E)||g_{Y_B|Y_E}(y_B|y_E) \right) \right).$$

(13)

Note that, to achieve the secrecy capacity, there exists a unique input PDF $f_{X^*}(x)$ that maximizes $I(X;Y_B|Y_E)$ subject to the constraints in (6). Therefore, we have

$$C_s = \max_{f_X(x)} I(X;Y_B|Y_E) = I(X^*;Y_B|Y_E),$$

(14)

where $X^*$ denotes the optimal input, and its corresponding PDF is $f_{X^*}(x)$.

According to (13) and (14), we have

$$C_s \leq E_{X^*|Y_E} \left( D \left( f_{Y_B|X,Y_E}(y_B|x,y_E)||g_{Y_B|Y_E}(y_B|y_E) \right) \right).$$

(15)

It can be seen from (15) that selecting any $g_{Y_B|Y_E}(y_B|y_E)$ will lead to an upper bound of the secrecy capacity. To obtain a good upper bound, a clever choice of $g_{Y_B|Y_E}(y_B|y_E)$ should be found. By using the principle of dual expression of the secrecy capacity, an upper bound of the secrecy capacity in (6) is derived in the following theorem.

Theorem 2: The secrecy capacity for the channel in (1) with constraints (2) and (4) is upper-bounded by

$$C_s \leq \left\{ \begin{array}{ll}
\ln \left( \frac{4e}{\pi} \left( \frac{1}{\sqrt{2\pi} \sigma_B} + \frac{H_B \xi_P}{H_B} \right) \right), & \\
\ln \left( \frac{2\sqrt{\pi} \sigma_B + \frac{H_B \xi_P}{H_B}}{2\pi \sigma_B} \right), & \text{if } \frac{H_B \sigma_B^2}{H_B^2} + \frac{\sigma_E^2}{2\pi} \leq \frac{H_B \sigma_B}{H_B} \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B \xi_P}{2\pi} \right), & \text{if } \frac{H_B \sigma_B^2}{H_B^2} + \frac{\sigma_E^2}{2\pi} \leq \frac{H_B \sigma_B}{H_B} \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B \xi_P}{2\pi} \right).
\end{array} \right.$$

(16)

Proof: See Appendix C.

Remark 2: When $\sqrt{\pi H_B} > H_E$, it is straightforward to show that (16) is a monotonically increasing function with respect to the dimming target $\xi$. In this case, the larger the dimming target is, the larger the upper bound on secrecy capacity becomes. When $\sqrt{(H_B^2 \sigma_B^2/H_B^2 + \sigma_E^2)/(2\pi)} \leq \frac{H_B}{H_B} \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B \xi_P}{2\pi} \right)$, the upper bound (16) is independent of the dimming target.

C. Asymptotic Behavior Analysis

In indoor VLC environment, typical illumination requirement leads to a large transmit optical intensity, which can offer a high SNR at the receiver [35]. Therefore, we are more interested in the behavior of the VLC system in the high SNR regime. By analyzing Theorem 1 and Theorem 2, the asymptotic behavior of the secrecy capacity bounds at high SNR is derived in the following corollary.

Corollary 1: For the channel in (1) with constraints (2) and (4), the asymptotic behavior of the secrecy capacity bounds at high SNR is given by

$$\ln \left( \frac{H_B \sigma_B}{H_B \sigma_B} \right) \leq \lim_{P \to \infty} C_s \leq \ln \left( \frac{2\sqrt{\pi}}{\pi} \right) + \ln \left( \frac{H_B \sigma_B}{H_B \sigma_B} \right).$$

(17)

Proof: See Appendix D.

Remark 3: From Corollary 1, it can be found that the asymptotic upper and lower bounds on secrecy capacity do not coincide in the sense that their difference equals $\ln(2\sqrt{\pi/\pi}) \approx 0.048$ nats/transmission instead of zero. Although a performance gap between the asymptotic upper and lower bounds exists, the difference is so small and thus it can be ignored.
IV. Secrecy Capacity for VLC With Both Average and Peak Optical Intensity Constraints

As is well known, the peak optical intensity of an LED is also limited. In this section, we consider the constraints (2), (3) and (4). Similarly, if \( H_B/\sigma_B < H_E/\sigma_E \), the secrecy capacity is zero. If \( H_B/\sigma_B \geq H_E/\sigma_E \), the secrecy capacity can be expressed as [23], [31]

\[
C_s = \max_{f(x)} \left[ I(X;Y_B) - I(X;Y_E) \right]
\]

\[
\text{s.t. } \int_0^A f_X(x)dx = 1
\]

\[
\int_0^A x f_X(x)dx = \xi P.
\]

In this section, the bounds of the secrecy capacity and their asymptotic behaviors for this case will be derived.

A. Lower Bound on Secrecy Capacity

Let \( \alpha = \xi P/A \) denote the average to peak optical intensity ratio (APOIR). Two lower bounds on the secrecy capacity can be derived by analyzing (18), and these lower bounds are shown in the following theorem.

**Theorem 3:** The secrecy capacity for the channel in (1) with constraints (2), (3) and (4) can be lower-bounded by each of the following two bounds (19) and (20), i.e.,

\[
C_s \geq \begin{cases} C_{s,1}, & 0 < \alpha < 0.5 \\ C_{s,2}, & 0.5 \leq \alpha \leq 1 \end{cases}
\]

(19)

and

\[
C_s \geq \begin{cases} \frac{1}{2} \ln \left[ \frac{3\sigma_E^2 (H_B^2 A^2 + 2\pi e\sigma_B^2)}{2\pi e\sigma_B^2 (H_E^2 \xi^2 P^2 + 3\sigma_E^2)} \right], & \alpha = 0.5 \\ \frac{1}{2} \ln \left[ \frac{\sigma_E^2 H_B^2 e^{-2\xi P} \left( \frac{\alpha}{e} \right)^2 + 2\pi e\sigma_B^2}{2\pi e\sigma_B^2 H_E^2 A (cA - 2)} + 2H_E^2 e^{-\xi P} - H_E^2 \xi^2 P^2 + \sigma_E^2 \right], & \alpha \neq 0.5 \text{ and } \alpha \in (0, 1] \end{cases}
\]

(20)

where \( C_{s,1} \) and \( C_{s,2} \) in (19) can be written, respectively, as (21) and (22) as shown at the bottom of this page, where \( \hat{\mu} \) in (21) is the solution to the following equation

\[
\alpha = \frac{1}{\mu} - e^{-\hat{\mu}}.
\]

(23)

In (21) and (22), \( \mu > 0 \) and \( \delta > 0 \) are free parameters.

Suboptimal but useful choices for \( \mu \) and \( \delta \) are given by

\[
\delta = \sigma_E \ln \left( 1 + \frac{H_B A}{\sigma_E} \right),
\]

\[
\mu = \tilde{\mu} \left( 1 - e^{-\alpha^2/2\sigma_E^2} \right).
\]

(24)

Moreover, \( c \) in (20) is the solution to the following equation

\[
\alpha = \frac{1}{1 - e^{-cA} - \frac{1}{cA}}.
\]

(25)

**Proof:** See Appendix E and Appendix F.

**Remark 4:** It can be easily proved that the curve of (20) is symmetric with respect to \( \alpha = 0.5 \). Moreover, it is challenging to analyze the relationship between lower bound (19) and \( \alpha \). Alternatively, numerical results are provided in Section V.

B. Upper Bound on Secrecy Capacity

According to (15) and referring to **Theorem 2**, we have the following theorem.

**Theorem 4:** The secrecy capacity for the channel in (1) with constraints (2), (3) and (4) is upper-bounded by

\[
C_s \leq \frac{1}{2} \ln \left[ \frac{H_B^2 A^2 \sigma_E^2 + 2\pi e\sigma_B^2}{2\pi e\sigma_B^2 H_E^2 A (cA - 2)} + 2H_E^2 e^{-\xi P} - H_E^2 \xi^2 P^2 + \sigma_E^2 \right] - \mu \alpha \left[ 1 - 2Q \left( \frac{\delta + H_B A}{\sigma_E} \right) \right] - \frac{\mu \sigma_E}{H_E A} \sqrt{2\pi} \left( e^{-\frac{\delta^2}{2\sigma_E^2}} - e^{-\frac{(H_B A + \delta)^2}{2\sigma_E^2}} \right),
\]

(21)

\[
C_{s,1} = \frac{1}{2} \ln \left[ 1 + H_B^2 A^2 \frac{e^{2\hat{\mu}} (1 - e^{-\hat{\mu}})}{2\pi e\sigma_B^2} \right] - \frac{\delta}{\sigma_E} - \frac{\delta^2}{2\sigma_E^2} + \frac{1}{2} \ln \left( H_E A \sqrt{2\pi} \right) \left[ e^{-\frac{\delta^2}{2\sigma_E^2}} - e^{-\frac{(H_B A + \delta)^2}{2\sigma_E^2}} \right] - \mu \alpha \left[ 1 - 2Q \left( \frac{\delta + H_B A}{\sigma_E} \right) \right] - \frac{\mu \sigma_E}{H_E A} \sqrt{2\pi} \left( e^{-\frac{\delta^2}{2\sigma_E^2}} - e^{-\frac{(H_B A + \delta)^2}{2\sigma_E^2}} \right),
\]

(22)

\[
C_{s,2} = \frac{1}{2} \ln \left[ 1 + H_B^2 A^2 \frac{e^{2\hat{\mu}} (1 - e^{-\hat{\mu}})}{2\pi e\sigma_B^2} \right] - \frac{\delta}{\sigma_E} - \frac{\delta^2}{2\sigma_E^2} + \frac{1}{2} \ln \left( H_E A \sqrt{2\pi} \right) \left[ e^{-\frac{\delta^2}{2\sigma_E^2}} - e^{-\frac{(H_B A + \delta)^2}{2\sigma_E^2}} \right] - \mu \alpha \left[ 1 - 2Q \left( \frac{\delta + H_B A}{\sigma_E} \right) \right] - \frac{\mu \sigma_E}{H_E A} \sqrt{2\pi} \left( e^{-\frac{\delta^2}{2\sigma_E^2}} - e^{-\frac{(H_B A + \delta)^2}{2\sigma_E^2}} \right).
\]

(26)

**Proof:** See Appendix G.

**Remark 5:** It can be easily shown that the upper bound (26) is a monotonically non-decreasing function with respect to the APOIR \( \alpha \).
Asymptotic Behavior Analysis

By analyzing Theorem 3 and Theorem 4, the asymptotic behavior of the secrecy capacity bounds in the high SNR regime is derived in the following corollary.

Corollary 2: For the channel in (1) with constraints (2), (3) and (4), the asymptotic behavior of the secrecy capacity bounds at asymptotically high SNR is given by

$$\ln \left( \frac{H_B \sigma_E}{H_E \sigma_B} \right) \leq \lim_{P \to \infty} C_s \leq \ln \left( \frac{H_B \sigma_E}{H_E \sigma_B} \right).$$

Proof: See Appendix H.

Remark 6: From Corollary 2, it can be found that the asymptotic upper and lower bounds on secrecy capacity coincide in the sense that their gap is equal to zero.

V. Numerical Results

In this section, selected numerical examples will be provided to verify the derived expressions of secrecy capacity. Here, a practical indoor VLC system within a $10 \times 10 \times 3 \text{m}$ room is considered. Alice is installed on the ceiling, whose coordinate is $(a, b, c)$. Bob and Eve are deployed on the floor, whose coordinates are $(d, e, f)$ and $(x, y, f)$. To facilitate the evaluation, the noise variances of Bob and Eve are assumed to be the same and normalized to be 1, i.e., $\sigma_B^2 = \sigma_E^2 = 0 \text{ dB}$ [8]. The other simulation parameters are listed in Table I.

A. Results of VLC Only With an Average Optical Intensity Constraint

To verify the accuracy of the lower bounds (7), (8) and the upper bound (16), Figs. 3-5 and Table II are provided in this subsection.

Fig. 3 shows the secrecy capacity bounds versus $P$ with different $H_B/H_E$ when $\xi = 0.2$. $(a, b, c) = (5 \text{m}, 5 \text{m}, 3 \text{m})$ and $(d, e, f) = (5 \text{m}, 4.5 \text{m}, 0 \text{m})$. For comparison, the Shannon limit is also presented. Obviously, the Shannon capacity is always larger than the secrecy capacity bounds. When $P$ is small, all secrecy capacity bounds increase rapidly with the increase of $P$. When $P$ is large, with the increase of $P$, the secrecy capacity bounds increase slowly and then tend to stable values. Moreover, with the increase of $H_B/H_E$, the secrecy capacity bounds also increase. This indicates that the larger the difference between $H_B$ and $H_E$ is, the better the system performance becomes. It can also be observed that the performance of (8) outperforms that of (7) at low SNR. However, at high SNR, eq. (7) achieves better performance than (8). That is, the gap between (8) and (16) is tighter than that between (7) and (16) at low SNR. At high SNR, the gap between (7) and (16) is tighter than that between (8) and (16). Moreover, the difference between (7) and (16) becomes so

Note that when $(x, y, f) = (4.93 \text{m}, 1.73 \text{m}, 0 \text{m}), H_B/H_E = 30$; when $(x, y, f) = (5.66 \text{m}, 0.16 \text{m}, 0 \text{m}), H_B/H_E = 300$; and when $(x, y, f) = (9.7 \text{m}, 9.87 \text{m}, 0 \text{m}), H_B/H_E = 3000$. 

| $P$ (dB) | Performance gaps (nats/transmission) |
|---------|------------------------------------|
| $H_B = 3000 H_E$ | $H_B = 300 H_E$ | $H_B = 30 H_E$ |
| 65      | 0.11118                             | 0.05804                             | 0.04971                             |
| 70      | 0.07856                             | 0.05198                             | 0.04888                             |
| 75      | 0.05803                             | 0.04971                             | 0.04588                             |
| 80      | 0.05198                             | 0.04888                             | 0.04587                             |
| 85      | 0.04871                             | 0.04588                             | 0.04544                             |
small and it can be ignored. Specifically, Table II quantitatively shows the performance gaps between (7) and (16). As can be seen, in the high SNR regime, the performance gap for each scenario is about 0.048 nats/transmission, which indicates that the asymptotic upper and lower bounds on secrecy capacity do not coincide. However, the difference is so small so that it can be ignored. This conclusion coincides with that in Corollary 1.

Fig. 6 shows the secrecy capacity bounds versus $A$ with different $H_B/H_E$ when $\xi = 0.2, P = A, (a, b, c) = (5m, 5m, 3m)$ and $(d, e, f) = (5m, 4.5m, 0m)$. In this figure, the Shannon limit is also provided. Once again, the performance of Shannon limit always outperforms that of all secrecy capacity bounds. Similar to Fig. 3, the secrecy capacity bounds increase and then tend to stable values with the increase of $A$. When $A$ is small (i.e., at low SNR), the value of (20) is larger than that of (19). However, when $A$ is large (i.e., at high SNR), the effect of the dimming target becomes weak. Moreover, at low SNR, the gap between (8) and (16) is smaller than that between (7) and (16). At high SNR, the opposite is the case. This conclusion consists with that in Fig. 3.

Fig. 5 shows the secrecy capacity bounds versus $H_B/H_E$ when $\xi = 0.2$. It can be observed that the secrecy capacity bounds are zero when $H_B/H_E < 1$, which indicates that the information-theoretic security cannot be achieved. When $H_B/H_E > 1$, the secrecy capacity bounds are larger than zero. The zone that $H_B/H_E > 1$ is named as the available zone. In this zone, the secure transmission can be guaranteed. Moreover, the secrecy capacity bounds increase with the increase of $H_B/H_E$. Furthermore, eq. (8) is tighter than (7) at low SNR, while the performance of (7) is better than that of (8) at high SNR. Similar conclusion can be drawn from Fig. 4.

### B. Results of VLC With Both Average and Peak Optical Intensity Constraints

To verify the accuracy of the lower bounds (19), (20) and the upper bound (26), Figs. 6–8 and Table III are provided in this subsection.

| $A$ (dB) | Performance gaps (nats/transmission) |
|---------|-------------------------------------|
| $H_B = 3000H_E$ | $H_B = 300H_E$ | $H_B = 30H_E$ |
| 65 | $8.0331 \times 10^{-2}$ | $1.1486 \times 10^{-2}$ | $1.4744 \times 10^{-3}$ |
| 70 | $3.1006 \times 10^{-2}$ | $4.1499 \times 10^{-3}$ | $5.1763 \times 10^{-4}$ |
| 75 | $1.1479 \times 10^{-2}$ | $1.4750 \times 10^{-3}$ | $1.7993 \times 10^{-4}$ |
| 80 | $4.1472 \times 10^{-3}$ | $5.1785 \times 10^{-4}$ | $6.2036 \times 10^{-5}$ |
| 85 | $1.4741 \times 10^{-3}$ | $1.8001 \times 10^{-4}$ | $2.1242 \times 10^{-5}$ |

Fig. 6 shows the secrecy capacity bounds versus $A$ with different $H_B/H_E$ when $\xi = 0.2, P = A, (a, b, c) = (5m, 5m, 3m)$ and $(d, e, f) = (5m, 4.5m, 0m)$. In this figure, the Shannon limit is also provided. Once again, the performance of Shannon limit always outperforms that of all secrecy capacity bounds. Similar to Fig. 3, the secrecy capacity bounds increase and then tend to stable values with the increase of $A$. When $A$ is small (i.e., at low SNR), the value of (20) is larger than that of (19). However, when $A$ is large (i.e., at high SNR), the performance of (7) is better than that of (8) at high SNR.
the performance of (19) is better than that of (20). At high SNR, the difference between (19) and (26) is very small and can be ignored. Different from Table II, the performance gaps between (19) and (26) in Table III are almost zero, which coincides with the conclusion in Corollary 2. This indicates that the asymptotic upper and lower bounds on secrecy capacity coincide at high SNR.

Fig. 7 shows the secrecy capacity bounds versus $\xi$ when $H_B/H_E = 300$, $P = A$, $(a, b, c) = (2.5m, 2.5m, 3m)$ and $(d, e, f) = (2.5m, 2m, 0.8m)$. Obviously, the dimming target has a strong impact on system performance. For (19) and (26), when $A = 35$ dB, the secrecy capacity bounds increase rapidly with $\xi$; when $A = 65$ dB, the impact of $\xi$ is slight, and the secrecy capacity bounds almost achieve stable values. However, for (20), the curve is completely symmetric with respect to $\xi = 0.5$, and the maximum value is obtained when $\xi = 0.5$. It can be found from Fig. 7(a) that (20) is better than (19) at low SNR. However, at high SNR as shown in Fig. 7(b), it is better to employ (19) as the lower bound. Similar results can also be seen in Fig. 6.

Fig. 8 shows secrecy capacity bounds versus $H_B/H_E$ when $\xi = 0.2$ and $P = A$. Here, the Shannon limit is also provided. As can be seen, the performance of Shannon limit always outperforms that of all secrecy capacity bounds. Obviously, with the increase of $H_B/H_E$, the secrecy performance improves. At the available zone, the secure communications can be implemented. Moreover, the values of lower bound (20) are almost larger than that of (19) at low SNR, and the performance of (19) is better than that of (20) at high SNR. This observation is the same as that in Fig. 7.

C. Results of Insecure Region

As it is known, when the main channel is worse than the eavesdropping channel (i.e., $H_B/\sigma_B < H_E/\sigma_E$), the secrecy capacity is zero, and thus secure transmission cannot be guaranteed. Here, the “insecure region” [36] is analyzed, which represents the receive region that the secrecy capacity is zero. If $\sigma_B = \sigma_E$, the indoor system is insecure when $H_B < H_E$. According to (5), it can be known that the insecure region is a disc with center $(a, b, f)$ and radius $\sqrt{(a-d)^2 + (b-e)^2}$.

To verify the insecure region, Fig. 9 shows secrecy capacity bound (16) for different positions of Eve when $\xi = 0.2$, $P = 50$ dB and $(a, b, c) = (3m, 3m, 3m)$. In Fig. 9, the dark blue area represents the insecure region. As shown in Fig. 9(a), when Bob is located underneath Alice, i.e., $(d, e, f) = (5m, 5m, 0m)$, no area in the receiver plane belongs to the insecure region. That is, the secure transmission can be guaranteed for all positions of the receiver plane. When Bob moves to the coordinate $(3m, 3m, 0m)$, the insecure region enlarges. Moreover, when Bob moves to the corner, i.e., $(d, e, f) = (0m, 0m, 0m)$, all areas become the insecure region. By observing Fig. 9, the insecure region is a disc with center $(5m, 5m, 0m)$ and radius $\sqrt{(5-d)^2 + (5-e)^2}$.

Fig. 10 shows secrecy capacity bound (26) for different positions of Eve when $\xi = 0.2$, $A = P = 50$ dB and $(a, b, c) = (3m, 3m, 3m)$. In Fig. 10, when Bob is located at $(5m, 5m, 0m)$, the insecure region is large. When Bob is located underneath Alice in Fig. 10(b), the insecure region seems to vanish. When Bob moves to the corner in Fig. 10(c), the insecure region enlarges once again. From Fig. 10,
the insecure region is a disc with center \((3m, 3m, 0m)\) and radius \(\sqrt{(3 - d)^2 + (3 - e)^2}m\).

VI. CONCLUSIONS

Unlike conventional RFWC, the indoor VLC is well modelled with optical intensity constraints imposed on the channel input. Therefore, the PHY security in VLC is different from that in RFWC. In this paper, we have investigated the secrecy capacity for indoor VLC. Two scenarios are considered, i.e., one is only with an average optical intensity constraint, and the other is with both average and peak optical intensity constraints. Closed-form expressions of the lower and upper bounds on secrecy capacity are derived. It is shown that the gap between the lower and upper bounds is small, which verifies the accuracy of the derived expressions. Moreover, at high SNR, when only considering the average optical intensity constraint, the asymptotic lower and upper bounds do not coincide but with a small performance gap (i.e., 0.048 nats/transmission). When both average and peak optical intensity constraints are considered, the asymptotic lower and upper bounds coincide, and thus the secrecy capacity can be obtained precisely.

After obtaining the secrecy capacity bounds for the indoor VLC, exploring the schemes to enhance the PHY security is the natural next step. As future research directions, it is of interest to seek new power, code, channel, and signal detection approaches to improve the PHY security for indoor VLC.

APPENDIX A

PROOF OF LOWER BOUND (7) IN THEOREM 1

For two arbitrary functions \(f_1(x)\) and \(f_2(x)\), we have
\[
\max(f_1(x) - f_2(x)) \geq \max f_1(x) - \max x f_2(x) [33].
\]
Therefore, the secrecy capacity in (6) is lower-bounded by
\[
C_s \geq \max f(x) I(X; Y_B) - \max f(x) I(X; Y_E) \Delta C_B - C_E. \quad (A.1)
\]

According to [32], a lower bound of \(C_B\) can be easily obtained in [29, eq. (12)], and an upper bound of \(C_E\) can be easily obtained in [29, eq. (13)]. Then, submit [29, eqs. (12) and (13)], eq. (7) can be derived.

APPENDIX B

PROOF OF LOWER BOUND (8) IN THEOREM 1

According to [23, eq. (29)] and the EPI [37, eq. (9.181)], the objective function in (6) can be lower-bounded by
\[
C_s \geq \max_{f(x)} \left\{ \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f_{\mathbb{N}|X}(y_B, y_E) \ln \left[ f_{\mathbb{N}|X,Y_E}(y_B|X, y_E) \right] dy_B dy_E \right\}
\]

\[
-\left( \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f_{\mathbb{N}|X}(y_B, y_E) \ln \left[ g_{\mathbb{N}|Y_E}(y_B|y_E) \right] dy_B dy_E \right) \left( I_1 - I_2 \right).
\]
Furthermore, \( \mathcal{H}(Y_E|X^*, Y_B) \) can be expressed as
\[
\mathcal{H}(Y_E|X^*, Y_B) = \frac{1}{2} \ln \left[ 2\pi e \left( \frac{H_B^2E^2}{H_B^2} \sigma_B^2 + \sigma_E^2 \right) \right]. \tag{C.5}
\]

Substituting (C.3), (C.4) and (C.5) into (C.2), \( I_1 \) can be finally written as
\[
I_1 = -\frac{1}{2} \ln \left[ 2\pi e \sigma_B^2 \left( 1 + \frac{H_B^2E^2}{H_B^2} \sigma_E^2 \right) \right]. \tag{C.6}
\]

The main challenge of deriving \( I_2 \) in (C.1) is that the input can be arbitrarily large without a peak optical intensity constraint. That makes it much harder to find a bound on expression like \( E_X(X^2) \). To obtain \( I_2 \), \( g_{Y_B|Y_E}(y_B|y_E) \) is chosen as
\[
g_{Y_B|Y_E}(y_B|y_E) = \frac{1}{2s^2} e^{-\frac{(y_B-y_E)^2}{2s^2}}, \tag{C.7}
\]
where \( \mu \) and \( s \) are two free parameters to be determined.

Moreover, \( f_{Y_B|Y_E|X}(y_B, y_E|X) \) can be written as
\[
f_{Y_B|Y_E|X}(y_B, y_E|X) = \frac{e^{-\frac{(y_E-H_B^2E^2X^2)}{2s^2}} - e^{\frac{-(y_B-H_B^2E^2X^2)}{2s^2}}}{\sqrt{2\pi s}B} \sqrt{\frac{H_B^2E^2}{H_B^2} \sigma_B^2 + \sigma_E^2}. \tag{C.8}
\]

Therefore, \( I_2 \) can be written as (C.9) as shown at the bottom of this page. Because \( |a-b| \leq |a|+|b| \) always holds, eq. (C.9) can be upper-bounded by
\[
I_2 \leq \ln(2s^2) + \frac{2}{s^2} \left( |\mu| \frac{\sqrt{H_B^2E^2|\sigma_B^2 + \sigma_E^2|}}{2\pi} + \left| 1 - \frac{H_B^2E^2}{2\pi} \right| \right) \times E_X \left[ \int_{-\infty}^{\infty} e^{\frac{-(y_B-H_B^2E^2X^2)}{2s^2}} |n + H_B^2E^2X| \, dn \right]. \tag{C.10}
\]

Because \( |a+b| \leq |a|+|b| \) always holds, eq. (C.10) can be further upper-bounded by
\[
I_2 \leq \ln(2s^2) + \frac{2}{s^2} \left( |\mu| \frac{\sqrt{H_B^2E^2|\sigma_B^2 + \sigma_E^2|}}{2\pi} + \left| 1 - \frac{H_B^2E^2}{2\pi} \right| \right) \times \left[ \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B^2E^2}{2\pi} \right]. \tag{C.11}
\]

To obtain a tight upper bound of \( I_2 \), the minimum value of \( I_3 \) in (C.11) should be determined. In the following, three cases are considered:

Case 1: when \( \mu < 0 \), \( I_3 \) is given by
\[
I_3 = -\left[ \left\{ \frac{\sqrt{H_B^2E^2|\sigma_B^2 + \sigma_E^2|}}{2\pi} + \frac{H_B^2E^2}{H_B^2} \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B^2E^2}{2\pi} \right) \right\} \mu \right. \\
+ \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B^2E^2}{H_B^2} \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B^2E^2}{2\pi} \right) \right] \tag{C.12}
\]

Case 2: when \( 0 \leq \mu \leq H_B^2E^2/H_B^2 \), \( I_3 \) is given by
\[
I_3 = \left[ \left\{ \frac{\sqrt{H_B^2E^2|\sigma_B^2 + \sigma_E^2|}}{2\pi} - \frac{H_B^2E^2}{H_B^2} \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B^2E^2}{2\pi} \right) \right\} \mu \right. \\
+ \frac{\sigma_B}{\sqrt{2\pi}} - \frac{H_B^2E^2}{H_B^2} \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B^2E^2}{2\pi} \right) \right]. \tag{C.13}
\]

If \( \sqrt{\left( \frac{H_B^2E^2}{H_B^2} + \frac{\sigma_E}{\sigma_E} \right)} \geq H_B^2E^2 / \sqrt{2\pi} + H_B^2E^2 / 2\pi \), we have \( I_3 \geq \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B^2E^2}{2\pi} \). Otherwise, we have \( I_3 \geq \sigma_B + H_B^2E^2 / 2\pi \).

Case 3: when \( \mu > H_B^2E^2/H_B^2 \), \( I_3 \) is given by
\[
I_3 = \left[ \left\{ \frac{\sqrt{H_B^2E^2|\sigma_B^2 + \sigma_E^2|}}{2\pi} + \frac{H_B^2E^2}{H_B^2} \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B^2E^2}{2\pi} \right) \right\} \mu \right. \\
- \frac{\sigma_B}{\sqrt{2\pi}} - \frac{H_B^2E^2}{H_B^2} \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B^2E^2}{2\pi} \right) \right]. \tag{C.14}
\]

According to the above three cases, we have
\[
I_3 \geq \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B^2E^2}{2\pi}, \tag{C.15}
\]

if \( \sqrt{\left( \frac{H_B^2E^2}{H_B^2} + \frac{\sigma_E}{\sigma_E} \right)} \geq H_B^2E^2 / \sqrt{2\pi} + H_B^2E^2 / 2\pi \),

\[
I_3 \geq \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B^2E^2}{2\pi}, \tag{C.15}
\]

if \( \sqrt{\left( \frac{H_B^2E^2}{H_B^2} + \frac{\sigma_E}{\sigma_E} \right)} \geq H_B^2E^2 / \sqrt{2\pi} + H_B^2E^2 / 2\pi \).

Finally, we have
\[
I_2 = \ln(2s^2) + \frac{1}{s^2} E_X \left[ \int_{-\infty}^{\infty} e^{-\frac{(y_E - H_B^2E^2X^2)^2}{2s^2}} \int_{-\infty}^{\infty} e^{-\frac{(y_B - H_B^2E^2X^2)^2}{2s^2}} \left( 1 - \frac{H_B^2E^2}{2\pi} \right) \, dy_B \right]. \tag{C.9}
\]
Substituting (C.15) into (C.11), $I_2$ is further upper-bounded by

$$I_2 \leq \begin{cases} 
\ln \left[ 4e \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B \xi P}{2} \right) \right], & \text{if } \frac{H_B \sigma_E^2 + \sigma_E^2}{2\pi} \geq \frac{H_E}{H_B} \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B \xi P}{2} \right) \\
\ln \left( 4e \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B \xi P}{2} \right) \right), & \text{if } \frac{H_B \sigma_E^2 + \sigma_E^2}{2\pi} \leq \frac{H_E}{H_B} \left( \frac{\sigma_B}{\sqrt{2\pi}} + \frac{H_B \xi P}{2} \right).
\end{cases}$$

(C.16)

Finally, submitting (C.6) and (C.16) into (C.1), eq. (16) can be derived.

**APPENDIX D**

**PROOF OF LOWER BOUND (19) IN THEOREM 3**

According to (A.1), the secrecy capacity in this case can also be written as

$$C_s \geq C_B - C_E. \quad (E.1)$$

When $\alpha \in (0, 0.5)$, $C_B$ is lower-bounded by [32]

$$C_B \geq \frac{1}{2} \ln \left[ 1 + \frac{H_B^2 A^2}{2 \pi e \sigma_B^2} \left( 1 - e^{-\bar{\mu}} \right)^2 \right], \quad (E.2)$$

where $\bar{\mu}$ is the solution to (23). Moreover, $C_E$ is upper-bounded by [32]

$$C_E \leq \frac{Q(\frac{\delta}{\sigma_E})}{\sqrt{2\pi \sigma_E}} + \frac{Q(\frac{\delta + H_E\alpha A}{\sigma_E})}{\sqrt{2\pi \sigma_E}} - Q\left( \frac{\delta}{\sigma_E} \right) - \frac{1}{2} \ln \left( \frac{\delta}{\sigma_E} \right)$$

$$+ \frac{\mu \sigma_E}{H_E A \sqrt{2\pi}} \left( \frac{1}{2} \ln \left( \frac{\delta}{\sigma_E} \right) - \frac{1}{2} \ln \left( \frac{\delta + H_E A}{\sigma_E} \right) \right), \quad (E.3)$$

where $\mu$ and $\delta$ is given by (24). Substituting (E.2) and (E.3) into (E.1), $C_{s,1}$ is derived.

When $\alpha \in [0.5, 1]$, $C_B$ is lower-bounded by [32]

$$C_B \geq \frac{1}{2} \ln \left[ 1 + \frac{H_B^2 A^2}{2 \pi e \sigma_B^2} \right], \quad (E.4)$$

and $C_E$ is upper-bounded by [32]

$$C_E \leq \frac{1}{2} \ln \left[ 1 + \frac{H_B^2 A^2}{2 \pi e \sigma_B^2} \right]$$

$$+ \frac{Q(\frac{\delta + H_E A}{\sigma_E})}{\sqrt{2\pi \sigma_E}} - \frac{1}{2} \ln \left( \frac{\delta}{\sigma_E} \right) - \frac{1}{2} \ln \left( \frac{\delta + H_E A}{\sigma_E} \right), \quad (E.5)$$

Substituting (E.4) and (E.5) into (E.1), $C_{s,2}$ is derived.

**APPENDIX F**

**PROOF OF LOWER BOUND (20) IN THEOREM 3**

In this case, eq. (B.1) can also be derived. Similar to (B.2), a lower bound on the secrecy capacity can be derived by solving the following problem

$$\min_{f_X(x)} \mathcal{J} (f_X(x)) \triangleq \int_0^A f_X(x) \ln [f_X(x)] \, dx$$

s.t. $\int_0^A f_X(x) \, dx = 1$

$$\int_0^A x f_X(x) \, dx = \xi P. \quad (F.1)$$

By employing the variational method [29], the input PDF is derived as

$$f_X(x) = e^{cx+b-1}. \quad (F.2)$$
where $b$ and $c$ are two free parameters.

When $c = 0$, submitting (F.2) into the two constraints in (F.1), we have

$$ f_X(x) = \begin{cases} \frac{1}{A}, & x \in [0, A] \\ 0, & \text{otherwise} \end{cases} \quad (F.3) $$

and $A = 2\xi P$, i.e., $\alpha = 0.5$. Therefore, $\mathcal{H}(X)$ and $\text{var}(Y_E)$ can be written, respectively, as

$$ \mathcal{H}(X) = \ln(A) \quad \text{and} \quad \text{var}(Y_E) = H_E^2 \frac{c^2 P^2}{3} + \sigma_E^2. \quad (F.4) $$

Submitting (F.4) into (B.1), the lower bound on secrecy capacity for $\alpha = 0.5$ is derived.

When $c \neq 0$, $\alpha \neq 0.5$ and $\alpha \in (0, 1]$, submitting (F.2) into the two constraints in (F.1), we have

$$ f_X(x) = \begin{cases} \frac{ce^cx}{e^{cA} - 1}, & x \in [0, A] \\ 0, & \text{otherwise} \end{cases} \quad (F.5) $$

where $c$ is the solution to (25).

Furthermore, $\mathcal{H}(X)$ and $\text{var}(Y_E)$ can be written, respectively, as

$$ \mathcal{H}(X) = \ln \left[ e^{-c\xi P} \left( \frac{e^{cA} - 1}{c} \right) \right] \quad (F.6) $$

and

$$ \text{var}(Y_E) = H_E^2 \left[ \frac{A(cA - 2)}{c(1 - e^{-cA})} + \frac{2}{c^2} - \xi^2 P^2 \right] + \sigma_E^2. \quad (F.7) $$

Submit (F.6) into (B.1), the lower bound on secrecy capacity for $\alpha \neq 0.5$ and $\alpha \in (0, 1]$ is derived.

**APPENDIX G**

**PROOF OF UPPER BOUND (26) IN THEOREM 3**

From (C.1), we have

$$ C_s \leq I_1 + I_2. \quad (G.1) $$

According to (C.2)-(C.6), $I_1$ in this case can also be expressed as

$$ I_1 = \frac{1}{2} \ln \left[ 2\pi e \sigma_B^2 \left( 1 + \frac{H_B^2 \sigma_B^2}{H_E^2 \sigma_E^2} \right) \right] + E_{X^*} \left\{ \left[ \frac{1}{\sqrt{2\pi} \sigma_B} x \sum_{x \in [0, A]} e^{(cA - 1) x} \right]^2 \right\}. \quad (G.2) $$

To obtain $I_2$, $g_{Y_B|Y_E}(y_B|y_E)$ is chosen as

$$ g_{Y_B|Y_E}(y_B|y_E) = \frac{1}{\sqrt{2\pi}s} e^{-\frac{(y_B^2 - \mu y_E^2)^2}{2s^2}}, \quad (G.3) $$

where $\mu$ and $s$ are free parameters to be determined.

According to (G.3) and (C.8), $I_2$ can be derived as

$$ I_2 = \frac{1}{2} \ln(2\pi s^2) + E_{X^*} \left\{ \left( \frac{1}{\sqrt{2\pi} \sigma_B} x \sum_{x \in [0, A]} e^{(cA - 1) x} \right)^2 \right\}. \quad (G.4) $$

Owing to $0 \leq X \leq A$ and $E_{X^*}(X) = \xi P$, we have

$$ E_{X^*}(X^2) \leq \int_0^A Ax f_{X^*}(x) dx = A \xi P. \quad (G.5) $$

Therefore, using (G.5), eq. (G.4) can be further written as

$$ I_2 \leq \frac{1}{2} \ln(2\pi s^2) + \left( 1 - \mu \frac{H_B}{H_E} \right)^2 (H_B^2 \sigma_B^2 + \sigma_E^2) + \mu^2 \left( \frac{H_B^2}{H_E^2} \sigma_B^2 + \sigma_E^2 \right) + \frac{1}{2} \ln(2\pi s^2). \quad (G.6) $$

To maximize the term on the right hand side of (G.6), taking the first partial derivative with respect to $\mu$ and $s$, and letting them to be zero, we have

$$ \mu = \frac{H_B}{H_E} \left( H_B^2 \sigma_B^2 + \sigma_E^2 \right) \quad \text{and} \quad s^2 = \frac{H_B^2 \sigma_B^2 + \sigma_E^2}{H_B^2 \sigma_B^2 + \sigma_E^2} \quad (G.7) $$

In this case, eq. (G.6) can be written as

$$ I_2 \leq \frac{1}{2} \ln \left[ \frac{2\pi e \left( H_B^2 \sigma_B^2 + \sigma_E^2 \right) \left( H_B^2 \sigma_B^2 + \sigma_E^2 \right)}{H_B^2 \sigma_B^2 + \sigma_E^2} \right]. \quad (G.8) $$

Substituting (G.2) and (G.8) into (G.1), eq. (26) can be derived.

**APPENDIX H**

**PROOF OF ASYMPTOTIC BEHAVIOR (27) IN COROLLARY 2**

In this section, the asymptotic expression of the lower bound on secrecy capacity is based on (19) in Theorem 3.

When $0 < \alpha < 0.5$ in (19), we have

$$ \lim_{A \to \infty} C_{s,1} = \lim_{A \to \infty} \frac{1}{2} \ln \left[ 1 + H_B^2 A^2 e^{2\alpha \tilde{\mu} (1 - e^{-\tilde{\mu}})^2} \right] + \left[ \frac{1}{\sqrt{2\pi} \sigma_B} x \sum_{x \in [0, A]} e^{(cA - 1) x} \right]^2 \right\} \quad (H.1) $$

where $\tilde{\mu}$ is the solution of (23), $\mu$ and $\delta$ are given by (24).

Moreover, we have

$$ \lim_{A \to \infty} I_6 - \lim_{A \to \infty} \ln A = \frac{1}{2} \ln \left( \frac{H_B^2}{2\pi e \sigma_B^2} \right) - (1 - \alpha) \tilde{\mu} - \ln(1 - \alpha \tilde{\mu}). \quad (H.2) $$
Furthermore, we have
\[
\lim_{A \to \infty} I_7 - \lim_{A \to \infty} \ln A = \ln \left( \frac{H_E}{\sigma_E} \right) - \frac{1}{2} \ln (2\pi e) - (1 - \alpha) \mu - \ln (1 - \alpha \mu). \tag{H.3}
\]
From (H.1) and (H.3), we can get
\[
\lim_{A \to \infty} C_s \geq \ln \left( \frac{H_B E}{H_E \sigma_B} \right). \tag{H.4}
\]
When \(0.5 \leq \alpha < 1\) in (19), we have
\[
\lim_{A \to \infty} C_{s,2} = \lim_{A \to \infty} \frac{1}{2} \ln \left( \frac{1 + H_B^2 A^2}{2\pi e \sigma_B^2} \right) - I_7 - \lim_{A \to \infty} \left[ 1 - 2Q \left( \frac{H_B A + 2\delta}{\sigma_E} \right) \right. \\
\times \ln \left[ \sqrt{2\pi \sigma_E} \left( 1 - 2Q \left( \frac{\delta}{\sigma_E} \right) \right) \right] \left. + Q \left( \frac{\delta}{\sigma_E} \right) + \delta - e^{\frac{\delta}{\sigma_E}} - 1 \right] \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonumber \nonu
Jin-Yuan Wang (S’12–M’16) received the B.S. degree in communication engineering from the College of Information and Electrical Engineering, Shandong University of Science and Technology, Qingdao, China, in 2009, the M.S. degree in electronic and communication engineering from the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2012, and the Ph.D. degree in information and communication engineering from the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, in 2015. He is currently a Lecturer with the College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications. He has authored or co-authored over 80 journal/conference papers. His current research interests include visible light communications. He has been a technical program committee member for many international conferences, such as the IEEE ICC and WTS. He also serves as a reviewer for many journals.

Cheng Liu received the B.S. degree in communication engineering from the School of Information and Electrical Engineering, Hunan University of Science and Technology, China, in 2016. He is currently pursuing the M.S. degree in communication and information system from the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China. His current research interests include physical-layer security in visible light communications.

Jun-Bo Wang (M’11) received the B.S. degree in computer science from the Hefei University of Technology, Hefei, China, in 2003, and the Ph.D. degree in communications engineering from the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, in 2008. He is currently an Associate Professor with the National Mobile Communications Research Laboratory, Southeast University. From 2008 to 2013, he was with the Nanjing University of Aeronautics and Astronautics, China. From 2011 to 2013, he was a Post-Doctoral Fellow at the National Laboratory for Information Science and Technology, Tsinghua University, Beijing, China. Since 2016, he has been a Marie Skłodowska-Curie Visiting Scholar with the University of Kent, Kent, U.K. His current research interests are wireless communications, signal processing, information theory, and coding.

Min Lin (M’13) received the B.S. degree from the National University of Defense Technology, Changsha, China, in 1993, the M.S. degree from the Nanjing Institute of Communication Engineering, Nanjing, China, in 2000, and the Ph.D. degree from Southeast University, Nanjing, in 2008, all in electrical engineering. He is currently a Professor with the Nanjing University of Posts and Telecommunications. He has authored or co-authored over 100 papers. His current research interests include wireless communications and array signal processing. He has served as a TPC member of many IEEE sponsored conferences, including the IEEE ICC and Globecom.

Julian Cheng (S’96–M’04–SM’13) received the B.Eng. degree (Hons.) in electrical engineering from the University of Victoria, Victoria, BC, Canada, in 1995, the M.Sc. (Eng.) degree in mathematics and engineering from Queens University, Kingston, ON, Canada, in 1997, and the Ph.D. degree in electrical engineering from the University of Alberta, Edmonton, AB, Canada, in 2003. He was with Bell Northern Research and NORTEL Networks. He is currently a Full Professor with the School of Engineering, Faculty of Applied Science, The University of British Columbia, Kelowna, BC, Canada. His current research interests include digital communications over fading channels, statistical signal processing for wireless applications, optical wireless communications, and 5G wireless networks. Currently, he serves as the President of the Canadian Society of Information Theory. He was the Co-Chair of the 12th Canadian Workshop on Information Theory in 2011, the 28th Biennial Symposium on Communications in 2016, and the 6th EAI International Conference on Game Theory for Networks (GameNets 216). He currently serves as an Area Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS. He was a past Associate Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE COMMUNICATIONS LETTERS, and the IEEE ACCESS. He served as a Guest Editor for a Special Issue on Optical Wireless Communications of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He is also a Registered Professional Engineer with the Province of British Columbia, Canada.