Optical Wiretap Channel with Input-Dependent Gaussian Noise Under Peak Intensity Constraint

Author(s):
Soltani, Morteza; Rezki, Zouheir

Publication date:
2018-02

Permanent link:
https://doi.org/10.3929/ethz-b-000245062

International Zurich Seminar on Information and Communication (IZS), February 21 – 23, 2018

Optical Wiretap Channel with Input-Dependent Gaussian Noise Under Peak Intensity Constraint

Morteza Soltani and Zouheir Rezki
University of Idaho
Department of Electrical and Computer Engineering
83844 Moscow, Idaho
Email: solt8821@vandals.uidaho.edu, zrezki@uidaho.edu

***Abstract*—This paper studies the optical wiretap channel with input-dependent Gaussian noise, in which the main distortion is caused by an additive Gaussian noise whose variance depends on the current signal strength. Subject to non-negativity and peak-intensity constraints on the channel input, we first evaluate the conditions under which this wiretap channel is stochastically degraded. We then study the secrecy-capacity-achieving input distribution of this wiretap channel and prove it to be discrete with a finite number of mass points. Moreover, we show that the entire rate-equivocation region of this wiretap channel is also obtained by discrete input distributions with a finite support. Similar to the case for the Gaussian wiretap channel under a peak-power constraint, here too, we observe that under non-negativity and peak-intensity constraints, there is a tradeoff between the secrecy capacity and the capacity in the sense that both may not be achieved simultaneously.**

I. Introduction

Exchanging confidential information over a communication medium (wired, wireless or optical) in the presence of unauthorized eavesdroppers has been always a challenging problem for system designers. This problem has been conventionally addressed by cryptographic encryption [1] without considering the imperfections introduced by the communication channel. In this model, using *secret keys* are the main approach for having secure communications. Wyner [2], on the other hand, proved the possibility of secure communications without relying on encryption by introducing the notion of a stochastically degraded wiretap channel.

For the class of degraded wiretap channels, it has been established in [2] that there exists a single-letter characterization for the rate-equivocation region. Authors in [3] studied the Gaussian wiretap channel under an average power constraint and obtained a single-letter expression for the entire rate-equivocation region. Particularly, they showed that under an average power constraint, the Gaussian distribution is the optimal input distribution for attaining both the capacity and secrecy capacity with no compromise between the communication rate and the equivocation rate at the eavesdropper. On the other hand, under a peak-power constraint, the work in [4] proved that the entire rate-equivocation region of the Gaussian wiretap channel is achieved by discrete input distributions with finite support. More specifically, the secrecy-capacity achieving input distribution may not be identical to the capacity-achieving counterpart in general, resulting in a tradeoff between the rate and its equivocation.

This work considers an *optical* wiretap channel based on intensity modulation with input-dependent Gaussian noise which consists of a transmitter, a legitimate user and an eavesdropper. We first evaluate the conditions under which the optical wiretap channel with input-dependent Gaussian noise is stochastically degraded. We then use the results in [2] to conclude that there exists a single-letter expression for the entire rate-equivocation region. Next, we employ the functional optimization problem addressed in [5] to obtain necessary and sufficient conditions, also known as Karush-Kuhn-Tucker (KKT) conditions, for the optimal input distribution. Finally, we prove by contradiction that the secrecy capacity as well as the entire rate-equivocation region of this wiretap channel, are obtained by discrete input distributions with a finite number of mass points. We provide numerical results which demonstrate that similar to the case of the Gaussian wiretap channel under a peak-power constraint, here too, the secrecy capacity and the capacity are not achieved by the same distribution in general. This, in turn, implies that for this wiretap channel, there is a tradeoff between the rate and its equivocation.

Due to the existence of input-dependent noise components, our technical proofs differ from those of [4]. Our analysis for showing the analyticity of the mutual information densities is more challenging. Additionally, our contradiction statements for proving the discreteness of the optimal input distribution are different.

II. System Model

In the considered optical wiretap channel, the channel input X is a nonnegative random variable representing the intensity of the optical signal. Since intensity is constrained due to practical and safety restrictions by a peak constraint in general, the input has to satisfy $X \leq A$ [6]. Therefore, the channel input is constrained as

$$0 \leq X \leq A. \tag{1}$$

This work has been supported by King Abdullah University of Science and Technology (KAUST), under a competitive research grant (CRG) OSR-2016-CRG5-2958-01.

In this setup, each link is a memoryless channel and is defined by [7]

$$Y = X + \sqrt{X}N_{B,1} + N_{B,0}, \tag{2}$$

$$Z = X + \sqrt{X}N_{E,1} + N_{E,0}, \tag{3}$$

where Y and Z denote the legitimate user's and the eavesdropper's observations, respectively. $N_{B,0}$ and $N_{E,0}$ are independent identically distributed (i.i.d.) zero-mean Gaussian random variables with variances σ_B^2 and σ_E^2, describing the input-independent noise components at the legitimate user and the eavesdropper, respectively. $N_{B,1}$ and $N_{E,1}$ are i.i.d. zero-mean Gaussian random variables with variances $\eta_B^2\sigma_B^2$ and $\eta_E^2\sigma_E^2$, describing the input-dependent noise components at the legitimate user and the eavesdropper, respectively, where η_B^2 and η_E^2 are the ratios of the input-dependent noise variances to the input-independent noise variances of the legitimate user's and the eavesdropper's channels, respectively. Furthermore, $N_{B,0}$ and $N_{B,1}$ are assumed to be independent and so are $N_{E,0}$ and $N_{E,1}$.

In this optical wiretap channel, since the input-dependent distortion is caused by the laser diode at the transmitter side [7], we consider the input-dependent noise components in both legitimate user's and wiretap channels to be statistically equivalent, i.e., $\sigma_B^2\eta_B^2 = \sigma_E^2\eta_E^2$. However, the variance of the input-independent noise of the wiretap channel is assumed to be strictly greater than that of the legitimate user's channel, i.e., $\sigma_E^2 > \sigma_B^2$ (otherwise the secrecy capacity defined later in this Section is zero). Therefore, under the conditions $\sigma_B^2\eta_B^2 = \sigma_E^2\eta_E^2$ and $\sigma_E^2 > \sigma_B^2$, the random variables X, Y and Z form a Markov chain $X \to Y \to Z$ and consequently the optical wiretap channel becomes stochastically degraded. As a result, the rate-equivocation region of such an optical wiretap channel can be expressed in a single-letter form due to [2].

An $(n, 2^{nR})$ code for the peak intensity-constrained optical wiretap channel with input-dependent Gaussian noise consists of the random variable W (message set) uniformly distributed over the set $\mathcal{W} = \{1, 2, \cdots, 2^{nR}\}$, an encoder at the transmitter $f_n : \mathcal{W} \to [0, A]^n$ satisfying the non-negativity and peak-intensity constraints, and a decoder at the legitimate user $g_n : \mathbb{R}^n \to \mathcal{W}$. Equivocation of a code is measured by the normalized conditional entropy $\frac{1}{n}H(W|Z^n)$. The probability of error for such a code is defined as $P_e^n = \Pr\left\{g_n(Y^n) \neq W\right\}$. A rate-equivocation pair (R, R_e) is said to be achievable if there exists an $(n, 2^{nR})$ code satisfying

$$\lim_{n\to\infty} P_e^n = 0, \tag{4}$$

$$R_e \leq \lim_{n\to\infty} \frac{1}{n} H(W|Z^n). \tag{5}$$

The rate-equivocation region consists of all achievable rate-equivocation pairs, and is denoted by $\mathcal{E}$. A rate R is said to be perfectly secure if we have $R_e = R$, i.e., if there exists an $(n, 2^{nR})$ code satisfying $\lim_{n\to\infty} \frac{1}{n} I(W; Z^n) = 0$. The supremum of such rates is defined to be the secrecy capacity and denoted by C_S.

The entire rate-equivocation region of the optical wiretap channel is given by the union of the rate-equivocation pairs (R, R_e) such that [2]

$$R \leq I(X; Y), \tag{6}$$

$$R_e \leq I(X; Y) - I(X; Z), \tag{7}$$

for some input distribution $F_X \in \mathcal{A}^+$, where $I(X;Y)$ and $I(X;Z)$ are the mutual information of the legitimate user's and the eavesdropper's channels, respectively, and the feasible set $\mathcal{A}^+$ is given by

$$\mathcal{A}^+ \triangleq \left\{F_X : \int_0^A dF_X(x) = 1\right\}. \tag{8}$$

III. Main Results

This section presents the main results about the optical wiretap channel with input-dependent Gaussian noise when non-negativity and peak-intensity constraints are imposed on the channel input.

A. Results on the Secrecy Capacity

The secrecy capacity of the optical wiretap channel with input-dependent Gaussian noise under non-negativity and peak-intensity constraints is given by the solution of the following optimization problem

$$\max_{F_X \in \mathcal{A}^+} g_0(F_X), \tag{9}$$

where $g_0(F_X) = I(X;Y) - I(X;Z)$ is the objective function of the optimization problem.

Under the constraints (1), the solution of (9) is discrete with a finite support as stated by Theorem 1.

Theorem 1. *There exists a unique input distribution that attains the secrecy capacity of the optical wiretap channel with input-dependent Gaussian noise under non-negativity and peak-intensity constraints. Furthermore, the support set of this optimal input distribution is a finite set.*

Proof. The proof is provided in Section IV. ∎

B. Results on the Rate-Equivocation Region

By a time-sharing argument, the rate-equivocation region of the optical wiretap channel with input-dependent Gaussian noise is convex. Therefore, the region can be characterized by finding tangent lines to $\mathcal{E}$, which are given by the solutions of

$$\max_{F_X \in \mathcal{A}^+} g_\lambda(F_X), \tag{10}$$

where $g_\lambda(F_X) = \lambda I(X;Y) + (1-\lambda)\left[I(X;Y) - I(X;Z)\right]$ for all $\lambda \in [0, 1]$. Next, we establish that the entire rate-equivocation region of the optical wiretap channel with input-dependent Gaussian noise under constraints(1) is also obtained by discrete input distributions with finite supports.

Theorem 2. *There exists a unique input distribution that achieves the boundary of the rate-equivocation region of the optical wiretap channel with input-dependent Gaussian*

noise under non-negativity and peak-intensity constraints. This optimal input distribution is discrete with a finite support.

Proof. Due to length constraint, the proof is given in [8, Section IV-D]. ∎

It is worth mentioning that for the case when η_B^2 and η_E^2 are 0 (i.e., the optical wiretap channel with input-independent Gaussian noise), similar approaches to those presented in [4] can be used to prove the discreteness of the optimal solutions of (9) and (10). An interesting observation is that our approach for proving the discreteness of the optimal solutions of (9) and (10) when $\eta_B^2, \eta_E^2 \neq 0$ cannot be generalized to the case when $\eta_B^2 = \eta_E^2 = 0$. This can also be observed in [9].

IV. Proof of the Main Results

A. Preliminaries and Notation

Since both channels are AWGN with input-dependent noise, the output densities for Y and Z exist for any input distribution F_X, and are given by

$$P_Y(y; F_X) = \int_0^A p(y|x)\, dF_X(x), \;\; y \in \mathbb{R} \tag{11}$$

$$P_Z(z; F_X) = \int_0^A p(z|x)\, dF_X(x), \;\; z \in \mathbb{R} \tag{12}$$

where $p(y|x)$ and $p(z|x)$ are given by [7]

$$p(y|x) = \frac{1}{\sqrt{2\pi\, \sigma_{B,X}^2(x)}} \exp\Big(-\frac{(y-x)^2}{2\,\sigma_{B,X}^2(x)}\Big), \tag{13}$$

$$p(z|x) = \frac{1}{\sqrt{2\pi\, \sigma_{E,X}^2(x)}} \exp\Big(-\frac{(z-x)^2}{2\,\sigma_{E,X}^2(x)}\Big), \tag{14}$$

where $\sigma_{B,X}^2(x) = \sigma_B^2(1+\eta_B^2 x)$ and $\sigma_{E,X}^2(x) = \sigma_E^2(1+\eta_E^2 x)$. We define the rate-equivocation density $r_e(x; F_X)$ as

$$r_e(x; F_X) = i_B(x; F_X) - i_E(x; F_X), \tag{15}$$

where $i_B(x; F_X)$ and $i_E(x; F_X)$ are the mutual information densities for the legitimate user's and eavesdropper's channel, respectively and are given by

$$\begin{aligned} i_B(x; F_X) = &- \int_{\mathbb{R}} p(y|x) \log\left(P_Y(y; F_X)\right)\, dy \\ &- \frac{1}{2}\log\Big(2\pi e \sigma_{B,X}^2(x)\Big), \end{aligned} \tag{16}$$

$$\begin{aligned} i_E(x; F_X) = &- \int_{\mathbb{R}} p(z|x) \log\left(P_Z(z; F_X)\right)\, dz \\ &- \frac{1}{2}\log\Big(2\pi e \sigma_{E,X}^2(x)\Big). \end{aligned} \tag{17}$$

The mutual information and the mutual information density are related through

$$I(X;Y) = \int_0^A i_B(x; F_X)\, dF_X(x), \tag{18}$$

$$I(X;Z) = \int_0^A i_E(x; F_X)\, dF_X(x). \tag{19}$$

One can show that the conditional densities in (13) and (14) are bounded as [9, Lemma 3]

$$\exp(-\alpha - \beta' y^2) \leq p(y|x) \leq \exp(\alpha - \beta y^2), \tag{20}$$

$$\exp(-\mu - \xi' z^2) \leq p(z|x) \leq \exp(\mu - \xi z^2), \tag{21}$$

for all $x \in [0, A]$, $y \in \mathbb{R}$, where $\alpha, \beta, \beta', \mu, \xi$ and ξ' are positive constants. Hence, for all $F_X \in \mathcal{A}^+$

$$\exp(-\alpha - \beta' y^2) \leq P_Y(y; F_X) \leq \exp(\alpha - \beta y^2), \tag{22}$$

$$\exp(-\mu - \xi' z^2) \leq P_Z(z; F_X) \leq \exp(\mu - \xi z^2). \tag{23}$$

Thus, we can write

$$\left|\log\left(P_Y(y; F_X)\right)\right| \leq \alpha + \beta' y^2, \tag{24}$$

$$\left|\log\left(P_Z(z; F_X)\right)\right| \leq \mu + \xi' z^2. \tag{25}$$

Next, we prove Theorem 1 using the preliminaries provided in this section.

B. Proof of Theorem 1

To prove Theorem 1, we first prove that the set of input distributions $\mathcal{A}^+$ satisfying (8), is compact and convex. We then show that the objective function in (9) is continuous, strictly concave and weakly differentiable in the input distribution F_X and hence we conclude that the solution to the optimization problem (9) exists and is unique. We continue the proof by deriving the necessary and sufficient conditions (KKT conditions) for the optimality of the optimal input distribution F_X^* and finally by means of contradiction we show that this optimal input distribution is discrete with a finite number of mass points.

Throughout the paper, we occasionally refer the reader to the technical report [8] where we have presented details that we can not provide here due to length constraint.

1) The feasible set $\mathcal{A}^+$ is compact and convex: The proof follows along similar lines as in [10, Appendix A.1].

2) $g_0(F_X)$ is continuous in input distribution F_X: It is established in [8, Section IV-B-2] that $g_0(F_X)$ is continuous in F_X.

3) $g_0(F_X)$ is strictly concave in F_X: The proof is given in [8, Section IV-B-Lemma 1].

4) $g_0(F_X)$ is weakly differentiable: We provide the proof in [8, Section IV-B-4].

Since the feasible set $\mathcal{A}^+$ is compact and convex and the objective function $g_0(F_X)$ is continuous, strictly concave and weakly differentiable, steps analogous to [5, Corollary 1] yield the following necessary and sufficient conditions for the optimality of the distribution F_X^*

$$r_e(x; F_X^*) \leq C_S, \;\; \forall x \in [0, A] \tag{26}$$

$$r_e(x; F_X^*) = C_S, \;\; \forall x \in S_{F_X^*} \tag{27}$$

where $S_{F_X^*}$ is the support set of F_X^* and the secrecy capacity C_S is expressed as

$$\begin{aligned} C_S = I_B(F_X^*) - I_E(F_X^*) = \\ h_Y(F_X^*) - h_Z(F_X^*) + \frac{1}{2}\mathbb{E}_{F_X^*}\left[\log\left(\frac{\sigma_{E,X}^2(x)}{\sigma_{B,X}^2(x)}\right)\right], \end{aligned} \tag{28}$$

where $I_B(F_X^*)$ and $I_E(F_X^*)$ are the mutual information for Bob and Eve, respectively, generated by the optimal input distribution F_X^*. Similarly, $h_Y(F_X^*)$ and $h_Z(F_X^*)$ are the differential entropies of Y and Z, respectively, generated by the input distribution F_X^*. Moreover, $\mathbb{E}_{F_X^*}$ denotes the expectation operator with respect to optimal distribution F_X^*.

We now prove by contradiction that the secrecy-capacity-achieving input distribution F_X^* has a finite number of mass points. To reach a contradiction, we use the KKT conditions in (26) and (27). To this end, we first show that both $i_B(x;F_X)$ and $i_E(x;F_X)$ have analytic extensions over some open connected set $\mathcal{D}=\left\{w:\Re(w)>-1/\eta_B^2\right\}$ in the complex plane $\mathbb{C}$ that includes the positive real line $\mathbb{R}_0^+$, where $\Re(\cdot)$ denote the real part of a complex variable.

5) The rate-equivocation density $r_e(x;F_X)$ is an analytic function on $\mathcal{D}$: Due to space limitations, we present the proof in [8, Section IV-B-5].

6) The secrecy-capacity-achieving input distribution is discrete: To prove the discreteness of the optimal input distribution F_X^*, we use a contradiction approach. To this end, let us assume that $S_{F_X^*}$ has an infinite number of elements. In view of the optimality condition (27), analyticity of $r_e(w;F_X)$ over the open connected set $\mathcal{D}$ and the identity theorem of complex analysis along with the Bolzano-Weierstrass Theorem, if $S_{F_X^*}$ has an infinite number of mass points, we get $r_e(w;F_X^*)=C_S$ for all $w\in\mathcal{D}$, which results in

$$r_e(x;F_X^*)=C_S,\quad \forall x\in\left(-1/\eta_B^2,\,+\infty\right). \tag{29}$$

Next, we show that (29) results in a contradiction. By observing the bounds given in (20)–(25), one can easily show that

$$\int_{\mathbb{R}}\exp\left(-\alpha-\beta'y^2\right)\left[-\alpha-\beta'y^2\right]\,dy\le\int_{\mathbb{R}}p(y|x)\times$$
$$\log\left(P_Y(y;F_X^*)\right)\,dy\le\int_{\mathbb{R}}\exp\left(\alpha-\beta y^2\right)\left[\alpha+\beta'y^2\right]\,dy, \tag{30}$$

for all $x\in\left(-1/\eta_B^2,\,A\right)\subset\left(-1/\eta_B^2,\,+\infty\right)$. Similarly,

$$\int_{\mathbb{R}}\exp\left(-\mu-\xi'z^2\right)\left[-\mu-\xi'z^2\right]\,dz\le\int_{\mathbb{R}}p(z|x)\times$$
$$\log\left(P_Z(z;F_X^*)\right)\,dz\le\int_{\mathbb{R}}\exp\left(\mu-\xi z^2\right)\left[\mu+\xi'y^2\right]\,dz, \tag{31}$$

for all $x\in\left(-1/\eta_B^2,\,A\right)$. Therefore, we can write

$$L_B\le-\int_{\mathbb{R}}p(y|x)\log\left(P_Y(y;F_X^*)\right)\,dy+\int_{\mathbb{R}}p(z|x)\times$$
$$\log\left(P_Z(y;F_X^*)\right)\,dz\le U_B, \tag{32}$$

where the lower bound L_B and the upper bound U_B are given respectively as

$$L_B=\int_{\mathbb{R}}\left[-\mu-\xi'z^2\right]\exp\left(-\mu-\xi'z^2\right)\,dz$$
$$+\int_{\mathbb{R}}\left[-\alpha-\beta'y^2\right]\exp\left(\alpha-\beta y^2\right)\,dy, \tag{33}$$
$$U_B=\int_{\mathbb{R}}\left[\mu+\xi'z^2\right]\exp\left(\mu-\xi z^2\right)\,dz$$

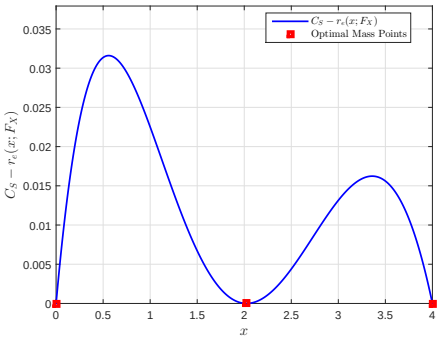

Fig. 1. Illustration of $C_S-r_e(x;F_X)$ yielded by the optimal input distribution when $\sigma_B^2=1$, $\sigma_E^2=2$, $\eta_B^2=0.25$, $\eta_E^2=0.125$ and $A=4$.

$$+\int_{\mathbb{R}}\left[\alpha+\beta'y^2\right]\exp\left(-\alpha-\beta'y^2\right)\,dy. \tag{34}$$

We note that since the constants β,β',ξ and ξ' are all positive, L_B and U_B are finite values. Substituting (16) and (17) into (29) and using the bounds in (32), we can write

$$L_B\le C_S+\frac{1}{2}\log\left(\frac{\sigma_{B,X}^2(x)}{\sigma_{E,X}^2(x)}\right)\le U_B. \tag{35}$$

Now, let $\left\{x^{(n)}\right\}_{n=1}^{\infty}$ be a convergent sequence in $\mathbb{S}\triangleq\left(-1/\eta_B^2,A\right)$ with a limit point $x^{(0)}=-1/\eta_B^2$. It is clear that 1) $x^{(n)}$ and $\sigma_{B,X}^2\left(x^{(n)}\right)$ are real for all positive integers n, and 2) $\lim_{n\to\infty}\sigma_{B,X}^2\left(x^{(n)}\right)=0$. Following the results in [9, Theorem 3] and using (35) we can write

$$\lim_{n\to\infty}(L_B-C_S)\le\lim_{n\to\infty}\frac{1}{2}\log\left(\frac{\sigma_{B,X}^2(x^{(n)})}{\sigma_{E,X}^2(x^{(n)})}\right)\le\lim_{n\to\infty}(U_B-C_S). \tag{36}$$

Since $\lim_{n\to\infty}\frac{1}{2}\log\left(\frac{\sigma_{B,X}^2(x^{(n)})}{\sigma_{E,X}^2(x^{(n)})}\right)=-\infty$ (due to the fact that $\sigma_{E,X}^2(x^{(0)})$ is a finite value) and the $\lim_{n\to\infty}(L_B-C_S)$ is a finite value, thus a contradiction occurs. This, in turn, implies that the support set $S_{F_X^*}$ cannot have an infinite number of elements and therefore the optimal input distribution F_X^* is discrete with a finite number of mass points.

V. Numerical Results

Fig. 1 provides a plot of the equivocation density for an optimal input distribution for $A=4$, $\sigma_B^2=1$, $\sigma_E^2=2$, $\eta_B^2=0.25$, and $\eta_E^2=0.125$. We numerically found that for these parameters, the optimal input distribution is ternary with mass points located at $x=0$, 2.025 and 4 with probability masses 0.2862, 0.3045 and 0.4093, respectively. We observe that $C_S-r_e(x;F_X)$ is generally nonnegative and is equal to zero at the optimal mass points; verifying the optimality conditions in (26) and (27).

Fig 2 illustrates the secrecy capacity C_S and the difference C_B-C_E versus the peak-intensity constraint A, where C_B and C_E are the legitimate user's and the eavesdropper's capacities, respectively. We observe that this difference is in general a

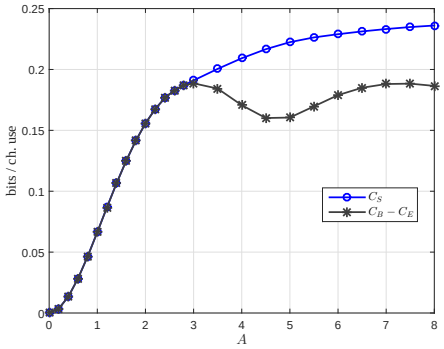

Fig. 2. The secrecy capacity for $\sigma_B^2 = 1$, $\sigma_E^2 = 2$, $\eta_B^2 = 0.25$ and $\eta_E^2 = 0.125$ versus the peak-intensity constraint A.

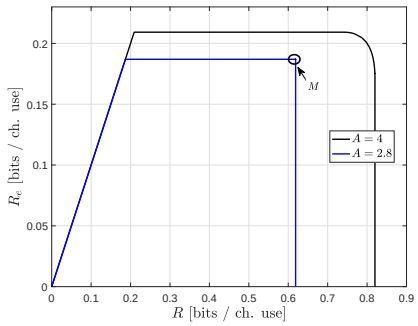

Fig. 3. The rate-equivocation region for $\sigma_B^2 = 1$, $\sigma_E^2 = 2$, $\eta_B^2 = 0.25$, and $\eta_E^2 = 0.125$ under peak-intensity constraints $A = 2.8$ and $A = 4$. Point M refers to the case when secrecy capacity and capacity are achieved simultaneously.

lower bound for the secrecy capacity C_S which can be easily proven. We also observe that, for small values of A, $C_B - C_E$ and C_S are identical. However, as A increases, $C_B - C_E$ and C_S become different. Similar to the secrecy capacity results of the Gaussian wiretap channel under a peak-power constraint provided in [4], here too, $I(X;Y)$ and $I(X;Z)$ are maximized by the same discrete distribution, however, $I(X;Y) - I(X;Z)$ is maximized by a different distribution. As a specific example, when $A = 4$, while both $I(X;Y)$ and $I(X;Z)$ are maximized by the same *binary* distribution with mass points at $x = 0$ and 4 with probability masses 0.5088 and 0.4912, respectively, $I(X;Y) - I(X;Z)$ is maximized by a *ternary* distribution with mass points at $x = 0, 2.025$ and 4 with probability masses 0.2862, 0.3045 and 0.4093, respectively. This explains the difference between C_S and $C_B - C_E$ at $A = 4$ in this figure.

Fig. 3 depicts the entire rate-equivocation region of the optical wiretap channel with input-dependent Gaussian noise under non-negativity and peak-intensity constraints when $\sigma_B^2 = 1$, $\sigma_E^2 = 2$, $\eta_B^2 = 0.25$, and $\eta_E^2 = 0.125$ for two different values of A. When $A = 2.8$, it is clear from the figure that both the secrecy capacity and the capacity can be attained simultaneously (Point "M" in the figure). In particular, for $A = 2.8$, the binary input distribution with mass points located at $x = 0$ and 2.8 with probabilities 0.5183 and 0.4817, respectively, achieves both the capacity and the secrecy capacity. This implies that, when $A = 2.8$, the transmitter can communicate with the legitimate user at the capacity while achieving the maximum equivocation at the eavesdropper. On the other hand, when $A = 4$, the secrecy capacity and the capacity cannot be achieved simultaneously (notice the curved shape in the figure). More specifically, for $A = 4$, the binary input distribution with mass points located at $x = 0$ and 4 with probabilities 0.5088 and 0.4912 achieves the capacity, while a ternary distribution with mass points located at $x = 0, 2.025, 4$ with probability masses 0.2862, 0.3045 and 0.4093, respectively, achieves the secrecy capacity, i.e., the optimal input distributions for the secrecy capacity and the capacity are different. In other words, there is a tradeoff between the rate and its equivocation.

VI. Conclusions

This paper studies the optical wiretap channel with input-dependent Gaussian noise under non-negativity and peak-intensity constraints. It is shown that the secrecy capacity and the boundary of the entire rate-equivocation region is achieved by discrete input distributions with a finite support. An interesting result that this paper reveals is that under such constraints, the secrecy capacity and the capacity of this optical wiretap channel cannot be obtained simultaneously in general, i.e., there is a tradeoff between the rate and its equivocation in the sense that, to increase the communication rate, one must compromise from the equivocation, and conversely to increase the achieved equivocation, one must compromise from the communication rate.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *j-BELL-SYST-TECH-J*, vol. 28, no. 4, pp. 656–715, 1949.

[2] A. D. Wyner, "The Wire-tap Channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.

[4] O. Ozel, E. Ekrem, and S. Ulukus, "Gaussian Wiretap Channel With Amplitude and Variance Constraints," *IEEE Transactions on Information Theory*, vol. 61, no. 10, pp. 5553–5563, Oct 2015.

[5] J. G. Smith, "The Information Capacity of Amplitude- and Variance-Constrained Scalar Gaussian Channels," *Information and Control*, vol. 18, no. 3, pp. 203–219, April 1971.

[6] S. Arnon, J. Barry, G. Karagiannidis, R. Schober, and M. Uysal, *Advanced Optical Wireless Communication Systems*, 1st ed. New York, NY, USA: Cambridge University Press, 2012.

[7] S. M. Moser, "Capacity Results of an Optical Intensity Channel With Input-Dependent Gaussian Noise," *IEEE Transactions on Information Theory*, vol. 58, no. 1, pp. 207–223, Jan 2012.

[8] M. Soltani and Z. Rezki, "Optical Wiretap Channel with Input-Dependent Gaussian Noise Under Peak and Average Intensity Constraints," *Technical Report*, Apr. 2017. [Online]. Available: https://sites.google.com/site/zouheirrezki/publications

[9] T. H. Chan, S. Hranilovic, and F. R. Kschischang, "Capacity-Achieving Probability Measure for Conditionally Gaussian Channels with Bounded Inputs," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 2073–2088, June 2005.

[10] C. Luo., *Communication for Wideband Fading Channels: On Theory and Practice*. PhD Thesis, Massachusetts Institute of Technology, Feb. 2006.