The Rate-Equivocation Region of the Degraded Discrete-Time Poisson Wiretap Channel

Morteza Soltani, *Student Member, IEEE*, and Zouheir Rezki, *Senior Member, IEEE*

2021 IEEE International Symposium on Information Theory (ISIT) | 978-1-5386-8209-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISIT45174.2021.9517742

Abstract—**This paper addresses the degraded discrete-time Poisson wiretap channel (DT–PWC) in an optical wireless communication system based on intensity modulation and direct detection (IM-DD). Subject to nonnegativity, average-intensity, and bandwidth constraints, we find that the secrecy capacity and the entire boundary of the rate-equivocation region are attained by discrete distributions with a countably infinite number of mass points, but with finitely many mass points in any bounded interval. Additionally, we shed light on the asymptotic behavior of the secrecy capacity in the regimes where the average intensity constraint either tends to zero (low-intensity) or tends to infinity (high-intensity). In the low-intensity regime, we observe that: when the channel gains of the legitimate receiver and the eavesdropper are identical, the secrecy capacity scales linearly in the average-intensity $\mathcal{E}$; whereas when the channel gains are different, the secrecy capacity scales, to within a constant, like $(\alpha_B - \alpha_E)\mathcal{E}\log\log\frac{1}{\mathcal{E}}$, where α_B and α_E are the legitimate receiver's and the eavesdropper's channel gains, respectively. In the high-intensity regime, we establish that the secrecy capacity does not scale with the average intensity constraint.**

I. Introduction

Intensity modulation and direct detection (IM-DD) is the simplest and the most commonly used technique for optical wireless communications. In this scheme, the channel input modulates the intensity of the emitted light. Thus, the input signal is proportional to the light intensity and is nonnegative. The receiver is usually equipped with a photodetector that absorbs an integer number of photons and generates a real-valued output corrupted by noise. Depending on the distribution of the corrupting noise, there exist several models for the underlying optical wireless communication channels. Free space optical (FSO) channels [1], [2], optical channels with input-dependent Gaussian noise [2], [3], and Poisson optical channels [2], [4]–[6] are the most widely used models for optical wireless communications. Due to the photon counting process at the receiver, the Poisson model is apparently the most accurate one. The studies conducting research on Poisson optical channels are mainly categorized into two mainstreams. The first category considers the continuous-time Poisson model where the input signals can admit arbitrarily waveforms and there are no bandwidth constraints on the transmission. The second category concerns the discrete-time Poisson channel and deals with the cases where stringent transmission bandwidths are assumed.

The capacity of the continuous-time Poisson channel is known in closed-form [4], [7]. For the peak-intensity constrained or peak- and average-intensity constrained inputs the capacity of the continuous-time Poisson channel is achieved by a binary distribution with mass points located at the origin and the peak-intensity constraint [7]. However, the channel capacity of the average-intensity constrained input is *infinite* and the capacity-achieving input is unknown [7]. For the discrete-time Poisson channel, Shamai [5] studied the single-user channel capacity and showed that the capacity-achieving distribution under nonnegativity, peak- and average-intensity constraints is discrete with a finite number of mass points. In [6], [8], authors provided an asymptotic analysis of the channel capacity in the regimes where the peak- and/or average-intensity constraints tend to zero (low-intensity regime) or to infinity (high-intensity regime) and derived upper and lower bounds which in some cases coincide. Considering an average-intensity constraint only, Martinez provided lower and upper bounds on the channel capacity that are tight in the high-intensity regime [9], [10]. Recently, Cheraghchi and Ribeiro studied the structure of capacity-achieving input distribution of the discrete-time Poisson channel with nonnegativity and average-intensity constraints [11] and also derived improved capacity upper bounds [11], [12].

In this work, we consider a degraded *discrete*-time PWC (DT–PWC) which consists of a transmitter, a legitimate user, and an eavesdropper. As we will show next, the current setup is fundamentally different from its continuous-time counterpart studied in [13]. For the DT–PWC with nonnegativity and average-intensity constraints, we show that every point on the boundary of the rate-equivocation region is attained by a unique distribution satisfying the following structural properties: **P1: the support set of the optimal solution contains finitely many mass points in any bounded interval**; **P2: the support set of the optimal solution is an unbounded set**. This result generalizes the one in [11] which deals with the capacity (without a secrecy constraint) and captures it as a single point of the rate-equivocation region. Finally, we study the asymptotic behavior of the secrecy capacity in the low- and high-intensity regimes and characterize the secrecy capacity in these regimes. In the low-intensity regime, we find the closed-form expression of the secrecy capacity for the case when the channel gains of the legitimate receiver and the eavesdropper are identical. Whereas, when the channel gains are different, we characterize the capacity within a constant gap. In the high-intensity regime, we establish that the secrecy capacity does *not* scale with the average-intensity constraint.

M. Soltani was with the Department of Electrical and Computer Engineering, University of Idaho, Moscow, Idaho, USA, e-mail: solt8821@vandals.uidaho.edu, and Z. Rezki is with the Department of Electrical and Computer Engineering, University of California Santa Cruz, CA, USA, e-mail: zrezki@ucsc.edu. This material is based upon work supported by the National Science Foundation (CAREER) under Grant No. 2114779.

II. The Degraded Discrete-Time Poisson Wiretap Channel

In the considered wiretap channel, confidential data are transmitted by sending pulse amplitude modulated (PAM) intensity signals which are constant in discrete time slots of duration Δ seconds [5]. This model is referred to as the DT–PWC where a bandwidth constraint is imposed on the input signals by constraining the signals to be rectangular PAM of duration Δ seconds. We note that in the limiting case where the pulse duration Δ converges to zero, i.e., $\Delta \to 0$, the DT–PWC becomes the CT–PWC. In this limiting case, the transmitted pulses are no longer required to be rectangular PAM signals and can admit any arbitrary waveforms. Notice that the results pertaining to the degraded CT–PWC have been reported by Laourine and Wagner in [13]. Therefore, in this work, our mere focus is on addressing the problem of secure communications over the DT–PWC, i.e., the case where Δ does *not* approach zero.

A. Channel Model

In the DT–PWC, the receiver is modeled as a photon counter which generates an integer representing the number of received photons. Specifically, in each time slot of Δ seconds an input intensity X is corrupted by the constant channel gains α_B and α_E and the combined impact of background radiation as well as the photodetectors' dark currents λ_B and λ_E at the legitimate user's and the eavesdropper's receivers, respectively. The channel outputs at the legitimate receiver and the eavesdropper are denoted by Y and Z, respectively, and are random variables related to the number of received photon in Δ seconds. These channel outputs conditioned on the input signal obey the Poisson distributions with mean $(\alpha_B X+\lambda_B)\Delta$ and $(\alpha_E X+\lambda_E)\Delta$, respectively, i.e., [5, equation 16]

$$p_{Y|X}(y|x) = e^{-(\alpha_B x+\lambda_B)\Delta}\,\frac{[(\alpha_B x+\lambda_B)\Delta]^y}{y!},\ y\in\mathbb{N}, \quad (1)$$

$$p_{Z|X}(z|x) = e^{-(\alpha_E x+\lambda_E)\Delta}\,\frac{[(\alpha_E x+\lambda_E)\Delta]^z}{z!},\ z\in\mathbb{N}, \quad (2)$$

where $\mathbb{N}$ is the set of all nonnegative integers. It is worth mentioning that in this work, we assume that the dark currents of the legitimate receiver and the eavesdropper are positive constants, i.e., $\lambda_B > 0$ and $\lambda_E > 0$.

In the DT–PWC, the channel input X is a nonnegative random variable representing the intensity of the optical signal. Since intensity is constrained due to a safety restriction by an average-intensity constraint, the input must satisfy $X \geq 0$ and $\mathbb{E}[X] \leq \mathcal{E}$ [2]. In this work, we are interested in the *degraded* DT–PWC. Therefore, we are interested in the case where the following conditions hold

$$\alpha_B \geq \alpha_E, \quad (3)$$

$$\frac{\lambda_B}{\alpha_B} \leq \frac{\lambda_E}{\alpha_E}, \quad (4)$$

which implies that the random variables X, Y, and Z form the Markov chain $X \to Y \to Z$ and consequently, the DT–PWC becomes stochastically degraded [13]–[15]. In the sequel, without loss of generality, we consider that at least one of the inequalities (3) or (4) is strict, since otherwise, the secrecy capacity (defined later) would be equal to zero.

B. The Rate-Equivocation Characterization of the DT–PWC

An $(n, 2^{nR})$ code for the DT–PWC consists of the random variable W (message set) uniformly distributed over $\mathcal{W} = \{1, 2, \cdots, 2^{nR}\}$, an encoder at the transmitter $f_n : \mathcal{W} \to \mathbb{R}_+^n$ satisfying the positivity- and average-intensity constraints, and a decoder at the legitimate user $g_n : \mathbb{N}^n \to \mathcal{W}$. 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 $P_e^n = \Pr[g_n(Y^n) \neq W]$. A rate-equivocation pair (R, R_e) is said to be achievable if there exists an $(n, 2^{nR})$ code satisfying $\lim_{n\to\infty} P_e^n = 0$ and $R_e \leq \lim_{n\to\infty}\dfrac{1}{n}H(W|Z^n)$. The rate-equivocation region consists of all achievable rate-equivocation pairs. A rate R is said to be perfectly secure if we have $R_e = R$, that is, if there exists an $(n, 2^{nR})$ code satisfying $\lim_{n\to\infty}\frac{1}{n}I(W;Z^n) = 0$, where $I(W;Z^n)$ is the mutual information between the random variables W and Z^n. The supremum of such rates is defined to be the secrecy capacity and is denoted by C_S.

Since under the assumptions (3)–(4), the DT–PWC is degraded, its entire rate-equivocation region, denoted by $\mathcal{R}$, can be expressed in a single-letter expression, and it is given by the union of all rate-equivocation pairs (R, R_e) such that [14]

$$\begin{cases} 0 \leq R \leq I(X;Y), \\ 0 \leq R_e \leq I(X;Y) - I(X;Z), \end{cases} \quad (5)$$

for some input distribution $F_X \in \mathcal{F}^+$ where $\mathcal{F}^+ \overset{\triangle}{=} \left\{F_X : \int_0^\infty dF_X(x) = 1, \int_0^\infty x\,dF_X(x) \leq \mathcal{E}\right\}$.

III. Main Results

In this section, we present our main results regarding the structure of the optimal input distributions achieving the secrecy capacity and exhausting the entire rate-equivocation region of the degraded DT–PWC. Furthermore, we characterize the behavior of the asymptotic secrecy capacity in the low- and high-intensity regimes.

A. Structure of the Secrecy-Capacity-Achieving Distributions

For the degraded DT–PWC, the secrecy capacity is given by a single-letter expression as [5], [16, Chap. 3]

$$C_S(\mathcal{E}) = \sup_{F_X\in\mathcal{F}^+} f_0(F_X) \overset{\triangle}{=} \sup_{F_X\in\mathcal{F}^+}[I(X;Y) - I(X;Z)] \quad (6)$$

The optimal input is characterized as follows.

Theorem 1. *There exists a unique input distribution that attains the secrecy capacity of the DT–PWC with nonnegativity and average-intensity constraints. The optimal distribution is discrete with a countably infinite number of mass points, but only finitely many mass points in any bounded interval.*

Proof. To prove Theorem 1, we first prove that the set of input distributions $\mathcal{F}^+$ is compact and convex. We then show that the objective function in (6) is continuous, strictly concave, and weakly differentiable in the input distribution F_X. Therefore, we conclude that the solution to the optimization problem (6) exists and is unique. We continue the proof by showing first that the intersection of the support set of the optimal input distribution denoted by $\mathcal{S}_{F_X^*}$ with any bounded interval B contains a finite number of mass points, i.e., $|\mathcal{S}_{F_X^*} \cap B| < \infty$, where $|B|$ denotes the cardinality of the set B. Then, we show that $\mathcal{S}_{F_X^*}$ must be an unbounded set. These structural properties imply that the optimal distribution is discrete with a countably infinite number of mass points, but with finitely many mass points in any bounded interval. The first property is shown by means of contradiction. We assume that $|\mathcal{S}_{F_X^*} \cap B| = \infty$. Then, using the KKT conditions and invoking the Bolzano-Weierstrass and Identity Theorems from complex analysis, we find that the Lagrangian multiplier is upper bounded by $-\infty$ which is a contradiction. The second property is also shown through contradiction. Assuming that the optimal support set is bounded, we consider the following cases: 1) if the legitimate user's and the eavesdropper's channel gains are not identical, our contradiction hinges on the fact that a linearly increasing function in x must be lower bounded by another function which grows as fast as $x \log x$ which is a contradiction for large values of x; 2) if the channel gains are identical, we find that the Lagrangian multiplier would be lower bounded by a constant and using the Envelope Theorem [17], we observe that the secrecy capacity must at least grow linearly in the average-intensity constraint. However, in Theorems 5 and 6, we establish that the secrecy capacity is always upper bounded by a constant for all values of the average-intensity. Therefore, the desired contradiction occurs. A detailed proof is provided in [18, Section IV-C]. ■

Next, we establish the existence of a mass point at $x = 0$ in the support set of the secrecy-capacity-achieving input distribution.

Proposition 1. *Let $\mathcal{S}_{F_X^*}$ be the support set of the secrecy-capacity-achieving input distribution F_X^* for the DT–PWC under nonnegativity- and average-intensity constraints. Then $x = 0 \in \mathcal{S}_{F_X^*}$.*

Proof. The proof is by contradiction and follows along similar lines of [19, Proposition 1] with the difference that the conditional channel laws follow Poisson distributions. A detailed proof is presented in [18, Appendix B]. ■

Next, we establish that the support set of the *capacity-achieving* (with no secrecy constraint) input distribution of the DT- Poisson channel also has a mass point at the origin.

Corollary 1. *The capacity-achieving distribution of the discrete-time Poisson channel, i.e., the case without secrecy constraint, under nonnegativity- and average-intensity constraints has a mass point located at the origin.*

Proof. The proof is via contradiction and it follows along similar lines of the proof of Proposition 1 without a secrecy constraint, i.e., disregarding the eavesdropper's link. ■

It is worth mentioning that this result provides an alternative proof of the existence of a mass point at the origin which was previously established in [20, Corollary 2].

B. Structure of the Optimal Distributions Exhausting the Entire Rate-Equivocation Region

By a time-sharing argument, it can be shown that the rate-equivocation region of the DT–PWC is convex. Therefore, the region can be characterized by finding tangent lines to $\mathcal{R}$ which are given by the solutions of

$$\sup_{F_X \in \mathcal{F}^+} f_\mu(F_X) \overset{\triangle}{=} \sup_{F_X \in \mathcal{F}^+} \left[\mu I(X;Y) + (1-\mu) \times [I(X;Y) - I(X;Z)]\right], \; \forall\, \mu \in [0,1], \tag{7}$$

We start by characterizing the optimal distributions exhausting the entire rate-equivocation region when nonnegativity and average-intensity constraints are active.

Theorem 2. *Every point on the boundary of the rate-equivocation region of the DT–PWC with nonnegativity and average-intensity constraints is achieved by a unique and discrete input distribution with a countably infinite number of mass points, but finitely many mass points in any bounded interval.*

Proof. The proof of Theorem 2 follows along similar lines of the proof of Theorem 1 with a difference in the unboundedness proof of the optimal support set. Here, we do not consider different cases on the channel gains and the desired contradiction occurs by showing that a linearly increasing function in x would be lower bounded by another function growing as fast as $x \log x$. A detailed proof is provided in [18, Section IV-E]. ■

A direct consequence of Theorem 2 is that when $\mu = 1$ in (7) (the point corresponding to the capacity of the DT Poisson channel with nonnegativity and average-intensity constraints), the optimal distribution is discrete with a countably infinite number of mass points, but finitely many mass points in any bounded interval. This result coincides with the one established in [11, Theorem 15].

Remark. *As mentioned earlier, in this work, we do not consider the case where $\lambda_B = 0$ and $\lambda_E \geq 0$. However, in our extended version of the paper, we have established that the structural results pertaining to the non-zero dark current case will indeed carry over to this case. For details, please refer to [18, Appendix I].*

C. Asymptotic Behavior of the Secrecy Capacity in the Low- and High-Intensity Regimes

This section investigates the asymptotic analysis for the secrecy capacity of the DT–PWC in both low- and high-intensity regimes.

1) Low-Intensity Regime: We formalize the results for the cases $\alpha_B = \alpha_E$ and $\alpha_B > \alpha_E$ in Theorem 3 and Theorem 4, respectively.[1]

Theorem 3. *If the channel gains $\alpha_B = \alpha_E$, then the secrecy capacity satisfies*

$$\lim_{\mathcal{E}\to 0} \frac{C_S(\mathcal{E})}{\mathcal{E}} = \left[\alpha_B \log\left(\frac{\lambda_E}{\lambda_B}\right)\right]. \tag{8}$$

Proof. We first show that the secrecy capacity is a concave function in the average-intensity constraint. Next, we invoke the secrecy capacity per unit cost argument established by El-Halabi *et al.* [21] to find a closed-form expression of the secrecy capacity. However, we note that the secrecy capacity per unit cost argument does not lead to the characterization of the secrecy-capacity-achieving input distribution [21]. Thus, in this case, we do not characterize the optimal input distribution. This is because, as established by Theorem 1, the optimal distribution admits a countably infinite number of mass points, and evaluating the mutual information difference is onerous. A detailed proof is presented in [18, Appendix E]. ■

Theorem 4. *If the channel gains $\alpha_B > \alpha_E$, then the secrecy capacity satisfies*

$$\begin{aligned}\frac{1}{2} &\le \liminf_{\mathcal{E}\to 0} \frac{C_S(\mathcal{E})}{(\alpha_B - \alpha_E)\mathcal{E}\log\log\frac{1}{\mathcal{E}}} \\ &\le \limsup_{\mathcal{E}\to 0} \frac{C_S(\mathcal{E})}{(\alpha_B - \alpha_E)\mathcal{E}\log\log\frac{1}{\mathcal{E}}} \le 2.\end{aligned} \tag{9}$$

Proof. We establish Theorem 4 by providing lower and upper bounds on the secrecy capacity. The lower bound is based on evaluating the mutual information difference for the binary input distribution with mass points located at $\{0, \zeta\}$ with corresponding probability masses $\{1-p, p\}$, where $\zeta \triangleq \sqrt{\frac{\lambda_B}{\alpha_B^2\Delta}\log\frac{1}{\mathcal{E}}}$ and $p = \frac{\mathcal{E}}{\zeta}$. Furthermore, we upper bound the secrecy capacity of the DT–PWC under an average-intensity constraint by the capacity of another discrete-time Poisson channel whose input is X and whose output is $\widetilde{Z}$ with $p_{\widetilde{Z}|X}(\widetilde{z}|x) = e^{-(\widetilde{\alpha}x+\widetilde{\lambda})\Delta}\frac{[(\widetilde{\alpha}x+\widetilde{\lambda})\Delta]^{\widetilde{z}}}{\widetilde{z}!}$, where $\widetilde{\alpha} \triangleq \alpha_B - \alpha_E$, $\widetilde{\lambda} \triangleq \left(\frac{\alpha_B}{\alpha_E} - 1\right)\lambda_E$, and the input is subject to nonnegativity and average-intensity constraint $\mathbb{E}[X] \le \mathcal{E}$. We derive the upper bound by invoking the results found by Lapidoth and Moser pertaining to the asymptotic capacity of the discrete-time Poisson channel with an average-intensity constraint and with constant nonzero dark current [8, Proposition 2]. A detailed proof is presented in [18, Appendix F]. ■

Theorem 4 suggests that the asymptotic secrecy capacity scales, to within a constant, like $\mathcal{E}\log\log\frac{1}{\mathcal{E}}$ in the low-average-intensity regime when the channel gains are different.

Finally, it is worth mentioning that the capacity of the discrete-time Poisson channel in the low-intensity regime and with constant non-zero dark current also scales like $\mathcal{E}\log\log\frac{1}{\mathcal{E}}$ [8, Proposition 2]. This implies that in the low-intensity regime the capacity and secrecy capacity (for the case of different channel gains) scale similarly with the average-intensity constraint. However, when channel gains are identical, the channel capacity still scales like $\mathcal{E}\log\log\frac{1}{\mathcal{E}}$ (because of disregarding the eavesdropper's link in channel capacity calculations), but the secrecy capacity scales linearly with the average-intensity constraint.

2) High-Intensity Regime: We start by considering two scenarios based on the degradedness conditions in (3)–(4) and for each of these scenarios, we provide an upper bound on the secrecy capacity. The first scenario deals with the case where the inequality (3) is tight and the inequality (4) is strict, i.e., $\alpha_B = \alpha_E$, $\frac{\lambda_E}{\alpha_E} > \frac{\lambda_B}{\alpha_B}$. The second scenario refers to the case where the inequality (3) is strict and the inequality (4) is either strict or tight, i.e., $\alpha_B > \alpha_E$, $\frac{\lambda_E}{\alpha_E} \ge \frac{\lambda_B}{\alpha_B}$.[2] Although for both scenarios, the final results are the same (cf. Theorem 5 and Theorem 6 below), we found it more convenient to distinguish the two scenarios as the proof techniques are different.

Before we present the main results regarding the asymptotic behavior of the secrecy capacity in the high-intensity regime, we state a lemma which we use in our analysis throughout this subsection.

Lemma 1. *For a degraded DT–PWC (i.e., when the conditions in* (3)–(4) *hold true), the mutual information difference $f_0(F_X) = I(X;Y) - I(X;Z)$ can be upper bounded as*

$$\begin{aligned}f_0(F_X) &= I(X;Y) - I(X;\widetilde{Y}) + I(X;\widetilde{Y}) - I(X;Z) \\ &\le I(X;Y) - I(X;\widetilde{Y}) + I(X;\widetilde{Z}),\end{aligned} \tag{10}$$

where $\widetilde{Y} \triangleq Y + N_D$, with N_D being a Poisson distributed random variable with mean $\lambda_D\Delta$ independent of X and Y, where $\lambda_D \triangleq \frac{\alpha_B}{\alpha_E}\lambda_E - \lambda_B$. Moreover, $\widetilde{Z}|X$ is a Poisson random variable with mean $(\widetilde{\alpha}X + \widetilde{\lambda})\Delta$ independent of $Z|X$ and such that $\widetilde{Y}|X = Z|X + \widetilde{Z}|X$, where $\widetilde{\alpha} = \alpha_B - \alpha_E$ and $\widetilde{\lambda} = \left(\frac{\alpha_B}{\alpha_E} - 1\right)\lambda_E$.

Proof. The proof follows along a similar line of [13, Lemma 1, Lemma 7]. ■

Now, we are ready to present the asymptotic results of the secrecy capacity in the high-intensity regime.

a) Upper Bound on the Secrecy Capacity When $\alpha_B = \alpha_E$ and $\frac{\lambda_E}{\alpha_E} > \frac{\lambda_B}{\alpha_B}$: We start by noting that according to Lemma 1, the random variable $\widetilde{Z} \equiv 0$, the upper bound in (10) is tight and the secrecy capacity is equal to

$$\begin{aligned}C_S(\mathcal{E}) &= f_0(F_X^*) \\ &= H_Y(F_X^*) - H_{\widetilde{Y}}(F_X^*) + H_{\widetilde{Y}|X}(F_X^*) - H_{Y|X}(F_X^*),\end{aligned} \tag{11}$$

where $F_X^* \in \mathcal{F}^+$, and $H_Y(F_X^*)$ and $H_{\widetilde{Y}}(F_X^*)$ are the entropies of the discrete random variables Y and $\widetilde{Y}$, respectively, induced by the optimal input distribution F_X^*. Furthermore,

[1] Note that $\alpha_B \ge \alpha_E$ due the degradedness assumption (3)

[2] As we mentioned at the end of subsection II-A, one of the conditions in (3)–(4) is assumed to be strict, otherwise the secrecy capacity would be equal to zero.

$H_{Y|X}(F_X^*)$ and $H_{\widetilde{Y}|X}(F_X^*)$ are the conditional entropies of $Y|X$ and $\widetilde{Y}|X$, respectively, induced by F_X^*. Next, we present the upper bound on the secrecy capacity of the DT–PWC in the high-intensity regime.

Theorem 5. *If $\alpha_B = \alpha_E$, $\frac{\lambda_E}{\alpha_E} > \frac{\lambda_B}{\alpha_B}$, then the secrecy capacity of the DT–PWC with nonnegativity and average-intensity constraints is upper bounded by*

$$C_S(\mathcal{E}) \leq \frac{\frac{\lambda_D^2}{2} + \frac{\lambda_D}{\Delta}}{\lambda_B}. \tag{12}$$

Proof. Under the assumption of $\alpha_B = \alpha_E$ and $\frac{\lambda_E}{\alpha_E} > \frac{\lambda_B}{\alpha_B}$, we first show that $H_Y(F_X^*) - H_{\widetilde{Y}}(F_X^*) < 0$. Thus, to upper bound the secrecy capacity, it is sufficient to provide an upper bound for the term $H_{\widetilde{Y}|X}(F_X^*) - H_{Y|X}(F_X^*)$. A detailed proof is presented in [18, Appendix G]. ■

From Theorem 5, we notice that the upper bound in (12) holds for all values of the average-intensity constraint. This implies that the secrecy capacity of the DT–PWC does not scale with the average-intensity constraint, i.e., $C_S(\mathcal{E}) = O(1)$, if $\alpha_B = \alpha_E$, $\frac{\lambda_E}{\alpha_E} > \frac{\lambda_B}{\alpha_B}$.

b) Upper Bound on the Secrecy Capacity When $\alpha_B > \alpha_E$ and $\frac{\lambda_E}{\alpha_E} \geq \frac{\lambda_B}{\alpha_B}$: In this case, we first note that due to Lemma 1, the secrecy capacity can be upper bounded as

$$\begin{aligned} C_S(\mathcal{E}) &= \sup_{F_X \in \mathcal{F}^+} [I(X;Y) - I(X;Z)] \\ &= \sup_{F_X \in \mathcal{F}^+} [I(X;Y) - I(X;\widetilde{Y}) + I(X;\widetilde{Y}) - I(X;Z)] \\ &\leq \underbrace{\sup_{F_X \in \mathcal{F}^+} [I(X;Y) - I(X;\widetilde{Y})]}_{\triangleq C_{S,U1}} \\ &\quad + \underbrace{\sup_{F_X \in \mathcal{F}^+} [I(X;\widetilde{Y}) - I(X;Z)]}_{\triangleq C_{S,U2}}. \end{aligned} \tag{13}$$

Then, we upper bound each of the terms $C_{S,U1}(\mathcal{E})$ and $C_{S,U2}(\mathcal{E})$ and show that these upper bounds are constant values and do not scale with the average-intensity constraint. These results are formally stated by the following theorem.

Theorem 6. *If $\alpha_B > \alpha_E$ and $\frac{\lambda_E}{\alpha_E} \geq \frac{\lambda_B}{\alpha_B}$, then the secrecy capacity of the DT–PWC with nonnegativity- and average-intensity constraints is upper bounded by*

$$C_S(\mathcal{E}) \leq \frac{\frac{\lambda_D^2}{2} + \frac{\lambda_D}{\Delta}}{\lambda_B} + \frac{1}{\Delta} \log\left(\frac{\alpha_B}{\alpha_E}\right). \tag{14}$$

Proof. We start the proof by noting that since Y and $\widetilde{Y}$ in (13) satisfy the condition in Theorem 5, then $C_{S,U1}(\mathcal{E})$ in (13) can be readily upper bounded by a constant value as

$$C_{S,U1}(\mathcal{E}) \leq \frac{\frac{\lambda_D^2}{2} + \frac{\lambda_D}{\Delta}}{\lambda_B}. \tag{15}$$

To upper bound $C_{S,U2}(\mathcal{E})$, we first note that it corresponds to the secrecy capacity of a degraded DT–PWC whose input is X, and whose outputs are $\widetilde{Y}$ and Z. Observe that $\widetilde{Y}|X$ is a Poisson distributed random variable with mean $(\alpha_B X + \frac{\alpha_B}{\alpha_E}\lambda_E)\Delta$. Also, $Z|X$ is another Poisson distributed random variable with mean $(\alpha_E X + \lambda_E)\Delta$. Note that the observations of the eavesdropper, i.e., Z is obtained from $\widetilde{Y}$ by thinning with erasure probability $1 - \frac{\alpha_E}{\alpha_B}$ [13], [15]. Next, we note that this new DT–PWC is degraded because the conditions in (3)–(4) are met since $\alpha_B > \alpha_E$ and $\frac{\lambda_E}{\alpha_E} = \frac{\frac{\alpha_B}{\alpha_E}\lambda_E}{\alpha_B}$. As a result, we have that $I(X;\widetilde{Y}|Z) = I(X;\widetilde{Y}) - I(X;Z)$ and $C_{S,U2} = \sup_{F_X \in \mathcal{F}^+} I(X;\widetilde{Y}|Z)$. By applying the duality upper bound in [3], [6] to the conditional mutual information $I(X;\widetilde{Y}|Z)$, we find an upper bound on the secrecy capacity as

$$C_{S,U2}(\mathcal{E}) \leq \frac{1}{\Delta} \log\left(\frac{\alpha_B}{\alpha_E}\right). \tag{16}$$

A detailed proof is presented in [18, Appendix H]. ■

Since the upper bound in (14) is a constant value and does not scale with the average-intensity constraint, then combining Theorem 5 and Theorem 6, we infer that the secrecy capacity does not scale with the average-intensity constraint in the high-intensity regime, i.e., $C_S(\mathcal{E}) = O(1)$.

Lastly, note that the capacity of the discrete-time Poisson channel with constant non-zero dark current under an average-intensity constraint scales logarithmically with the average-intensity constraint [6, Theorem 7], while we proved that the secrecy capacity of DT–PWC is a constant and does not scale with the constraint.

IV. Conclusions

In this paper, we studied the DT–PWC where an average-intensity constraint was considered. Our motivation behind studying the secrecy capacity of such a wiretap channel was that Poisson distribution can model most of the impairments of a practical optical wireless channel (e.g., an optical wireless channel model for visible light communication scenarios). Thus, it is natural to understand the fundamental performance limits of the Poisson optical wireless channel with secrecy constraints. In summary, we found that the secrecy capacity, as well as the entire boundary of the rate-equivocation region, are attained by discrete distributions with a countably infinite number of mass points, but finitely many mass points in any bounded interval. Furthermore, we performed asymptotic analysis for the secrecy capacity in both the low- and high-intensity regimes. In the low-intensity regime and when the channel gains of the legitimate receiver and the eavesdropper were identical, the secrecy capacity scaled linearly in the average-intensity. However, when the channel gains are different, the secrecy capacity is scaled, to within a constant, like $\mathcal{E} \log\log \frac{1}{\mathcal{E}}$. In the high-intensity regime, we established that the secrecy capacity must be constant.

As future work, we plan to derive tight lower and upper bounds on the secrecy capacity in both the low- and high-intensity regimes for the zero dark currents case, i.e., $\lambda_B = 0$ and $\lambda_E \geq 0$.

References

[1] A. Lapidoth, S. M. Moser, and M. A. Wigger, "On the capacity of free-space optical intensity channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4449–4461, Oct. 2009.

[2] 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.

[3] S. M. Moser, "Capacity results of an optical intensity channel with input-dependent Gaussian noise," *IEEE Trans. Inf. Theory*, vol. 58, no. 1, pp. 207–223, Jan. 2012.

[4] A. D. Wyner, "Capacity and error exponent for the direct detection photon channel. i," *IEEE Trans. Inf. Theory*, vol. 34, no. 6, pp. 1449–1461, Nov. 1988.

[5] S. Shamai, "Capacity of a pulse amplitude modulated direct detection photon channel," *IEE Proceedings I - Communications, Speech and Vision*, vol. 137, no. 6, pp. 424–430, Dec. 1990.

[6] A. Lapidoth and S. M. Moser, "On the capacity of the discrete-time Poisson channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 303–322, Jan. 2009.

[7] M. Davis, "Capacity and cutoff rate for Poisson-type channels," *IEEE Trans. Inf. Theory*, vol. 26, no. 6, pp. 710–715, Nov. 1980.

[8] A. Lapidoth, J. H. Shapiro, V. Venkatesan, and L. Wang, "The discrete-time Poisson channel at low input powers," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3260–3272, Jun. 2011.

[9] A. Martinez, "Spectral efficiency of optical direct detection," *J. Opt. Soc. Am. B*, vol. 24, no. 4, pp. 739–749, Apr. 2007.

[10] ——, "A lower bound for the capacity of the discrete-time poisson channel," in *Proc. IEEE Int. Symp. on Inf. Theory*, 2009, pp. 2214–2215.

[11] M. Cheraghchi and J. Ribeiro, "Improved upper bounds and structural results on the capacity of the discrete-time Poisson channel," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, Jul. 2019.

[12] M. Cheraghchi and J. L. Ribeiro, "Non-asymptotic capacity upper bounds for the discrete-time poisson channel with positive dark current," *arXiv*, vol. abs/2010.14858, 2020. [Online]. Available: https://arxiv.org/abs/2010.14858

[13] A. Laourine and A. B. Wagner, "The degraded Poisson wiretap channel," *IEEE Trans. Inf. Theory*, vol. 58, no. 12, pp. 7073–7085, Dec 2012.

[14] A. D. Wyner, "The Wire-tap Channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[15] A. Lapidoth, I. E. Telatar, and R. Urbanke, "On wide-band broadcast channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3250–3258, Dec. 2003.

[16] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[17] D. G. Luenberger, *Optimization by Vector Space Methods*, 1st ed. USA: John Wiley and Sons, Inc., 1997.

[18] M. Soltani and Z. Rezki, "The Degraded Discrete-Time Poisson Wiretap Channel," *arXiv e-prints*, p. arXiv:2101.03650, Jan. 2021.

[19] M. Soltani and Z. Rezki, "Optical wiretap channel with input-dependent Gaussian noise under peak- and average-intensity constraints," *IEEE Trans. Inf. Theory*, vol. 64, no. 10, pp. 6878–6893, Oct 2018.

[20] J. Cao, S. Hranilovic, and J. Chen, "Capacity-achieving distributions for the discrete-time Poisson channel—part i: General properties and numerical techniques," *IEEE Trans. Commun.*, vol. 62, no. 1, pp. 194–202, Jan. 2014.

[21] M. El-Halabi, T. Liu, and C. N. Georghiades, "Secrecy capacity per unit cost," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1909–1920, 2013.