Gaussian Wiretap Channel with an Amplitude Constraint

Omur Ozel Ersen Ekrem Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland College Park, MD 20742
omur@umd.edu *ersen@umd.edu* *ulukus@umd.edu*

***Abstract*—We consider the Gaussian wiretap channel with an amplitude constraint, i.e., a peak power constraint, on the channel input. We show that the entire rate-equivocation region of the Gaussian wiretap channel with an amplitude constraint is obtained by discrete input distributions with finite support. We prove this result by considering the existing single-letter description of the rate-equivocation region, and showing that discrete distributions with finite support exhaust this region. Our result highlights an important difference between the peak power constraint and the average power constraint cases: Although, in the average power constraint case, both the secrecy capacity and the capacity can be achieved simultaneously, our results show that in the peak power constraint case, in general, there is a tradeoff between the secrecy capacity and the capacity, in the sense that, both may not be achieved simultaneously.**

I. Introduction

We consider the Gaussian wiretap channel [1]–[3] which consists of a transmitter, a legitimate user and an eavesdropper as shown in Fig. 1. In the Gaussian wiretap channel, each link is a memoryless additive white Gaussian noise (AWGN) channel. In this model, the goal of the transmitter is to have secure communication with the legitimate user while keeping the eavesdropper ignorant of this communication as much as possible.

Since the Gaussian wiretap channel is stochastically degraded, its rate-equivocation region is known in a single-letter form due to [1]. Under an average power constraint, the entire rate-equivocation region of the Gaussian wiretap channel can be obtained by evaluating this single-letter expression. In particular, under an average power constraint, Gaussian input with full power attains both the secrecy capacity and the capacity of the channel between the transmitter and the legitimate user, providing the entire rate-equivocation region. One important implication of this result is that the transmitter and the legitimate user do not compromise from their communication rate in order to maximize the equivocation of their communication at the eavesdropper. In other words, there is no tradeoff between the rate and the equivocation for the average power constrained Gaussian wiretap channel.

In this work, we consider the Gaussian wiretap channel under a peak power constraint, i.e., an amplitude constraint on the channel input. Similar to the average power constraint case, here also, we can use the existing single-letter description for the rate-equivocation region of the Gaussian wiretap channel due to [1]. However, unlike the average power constraint case, here, due to the peak power constraint, the corresponding optimization problems are harder to solve explicitly. For example, the entropy-power inequality, which is the key tool to obtain the rate-equivocation region under an average power constraint, falls short of providing a tight result for the rate-equivocation region under a peak-power constraint.

This work was supported by NSF Grants CNS 09-64632, CCF 09-64645, CCF 10-18185 and CNS 11-47811.

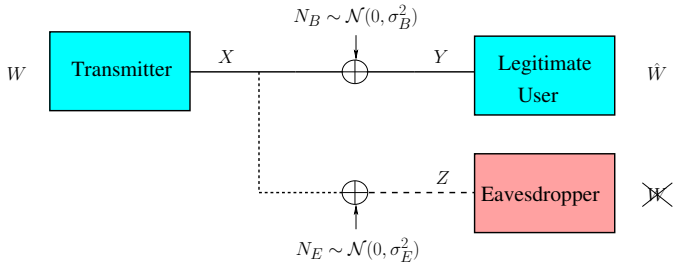

Fig. 1. The Gaussian wiretap channel.

We circumvent difficulties arising from the existence of a peak power constraint by using the methodology originally devised by [4], and later, extended further by [5]–[10]. In [4], Smith studied the AWGN channel under a peak power constraint and proved that the optimal input distribution is discrete with finite support. This methodology considers the functional optimization problem associated with the capacity of the AWGN channel, obtains the necessary and sufficient conditions for the optimal input distribution, and proves by contradiction that the optimal input distribution should be discrete with finite support.

In this work, we use this methodology [4], [8], [10] to study the Gaussian wiretap channel with an amplitude constraint. First, we consider the single-letter description of the rate-equivocation region under a peak power constraint, and obtain necessary and sufficient conditions for the optimal input distribution. Next, we prove by contradiction that the optimal input distribution should be discrete with finite support.

In the last part of our paper, we provide some numerical results which highlight an important difference between the peak power constraint and the average power constraint cases. As mentioned, in the average power constraint case, both the secrecy capacity and the capacity are simultaneously achieved by the same input distribution (Gaussian distribution

with full power). On the other hand, our numerical results demonstrate that under a peak power constraint, in general, the secrecy capacity and the capacity are not achieved by the same distribution. In other words, under a peak power constraint, in general, there is a tradeoff between the rate and its equivocation in the sense that when we want to maximize the equivocation, we may need to compromise from the rate.

II. System Model and Main Results

The Gaussian wiretap channel is defined by

$$Y_i = X_i + N_{B_i}, \qquad i = 1, \dots, n \tag{1}$$

$$Z_i = X_i + N_{E_i}, \qquad i = 1, \dots, n \tag{2}$$

where X_i, Y_i, Z_i denote the channel input, the legitimate user's observation and the eavesdropper's observation, respectively. N_{B_i} and N_{E_i} are i.i.d. zero-mean Gaussian random variables with variances σ_B^2 and σ_E^2, respectively, where $\sigma_B^2 < \sigma_E^2$. We assume that there is an amplitude constraint on the channel input X_i as

$$|X_i| \leq A, \quad i = 1, \dots, n \tag{3}$$

An $(n, 2^{nR})$ code for the Gaussian wiretap channel with peak power constraint consists of a message set $W \in \mathcal{W} = \{1, \dots, 2^{nR}\}$, an encoder at the transmitter $f_n : \mathcal{W} \to \mathbb{R}^n$ satisfying the peak power constraint in (3), 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 $(1/n)H(W|Z^n)$, where W is a uniformly distributed random variable over $\mathcal{W}$. Probability of error for a code is defined as $P_e^n = \Pr[g_n(f_n(W)) \neq W]$. 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

$$R_e \leq \lim_{n\to\infty} \frac{1}{n} H(W|Z^n) \tag{4}$$

The rate-equivocation region consists of all achievable rate-equivocation pairs, and is denoted by $\mathcal{C}$. 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 $\lim_{n\to 0}(1/n)I(W; Z^n) = 0$. Supremum of such rates is defined to be the secrecy capacity and denoted by C_s.

Since the Gaussian wiretap channel is stochastically degraded, its entire rate-equivocation region $\mathcal{C}$ can be expressed in a single-letter form by using the result of [1].

Theorem 1 *The rate-equivocation region of the Gaussian wiretap channel with a peak power constraint is given by the union of the rate-equivocation pairs (R, R_e) satisfying*

$$R \leq I(X;Y) \tag{5}$$

$$R_e \leq I(X;Y) - I(X;Z) \tag{6}$$

for some input distribution $F_X \in \Omega$, where the feasible set Ω is given by

$$\Omega \triangleq \left\{ F_X : \int_{-A}^{A} dF_X(x) = 1 \right\} \tag{7}$$

Since the rate-equivocation region $\mathcal{C}$ is convex due to time-sharing, it can be characterized by finding the tangent lines to the region $\mathcal{C}$, which are given by the solutions of

$$\max_{F_X \in \Omega} g_\mu(F_X) = \max_{F_X \in \Omega} (\mu + 1) I(X;Y) - I(X;Z) \tag{8}$$

for all $\mu \geq 0$.

Our main result is to show that the maximizer distribution for (8) is discrete with finite support.

Theorem 2 *Let F_X^* be the maximizer of the optimization problem in (8) with a support set $\mathcal{S}_{F_X^*}$. The support set $\mathcal{S}_{F_X^*}$ is a finite set.*

Theorem 2 implies that the secrecy capacity C_s is also achieved by a discrete distribution with finite support.

Corollary 1 *Let F_X^* be the distribution that attains the secrecy capacity of the Gaussian wiretap channel with a peak power constraint. The support set $\mathcal{S}_{F_X^*}$ is a finite set.*

In the next two sections, we first prove Corollary 1, and next, by using the proof of Corollary 1, we prove Theorem 2.

III. Proof of Corollary 1

We note that the secrecy capacity of the Gaussian wiretap channel with peak power constraint is given by

$$C_s = \max_{F_X \in \Omega} g_0(F_X) = \max_{F_X \in \Omega} I(X;Y) - I(X;Z) \tag{9}$$

where the objective function $g_0(F_X)$ is a strictly concave functional of the input distribution F_X due to the assumption $\sigma_B^2 < \sigma_E^2$. Moreover, the feasible set Ω is convex and sequentially compact with respect to the Levy metric [4]. Thus, (9) is a convex optimization problem with a unique solution.

Next, we obtain the necessary and sufficient conditions that the optimal distribution F_X^* of the optimization problem in (9) should satisfy. To this end, we introduce some notation which will be frequently used throughout the paper. Since both channels are AWGN, the output densities for Y and Z exist for any input distribution F_X, and are given by

$$p_Y(y; F_X) = \int_{-A}^{A} \phi_B(y - x) dF_X \tag{10}$$

$$p_Z(z; F_Z) = \int_{-A}^{A} \phi_E(z - x) dF_X \tag{11}$$

where $\phi_B(y), \phi_E(z)$ are zero-mean Gaussian densities with variances σ_B^2 and σ_E^2, respectively.

We define the equivocation density $r_e(x; F_X)$ as

$$r_e(x; F_X) = i_B(x; F_X) - i_E(x; F_X) \tag{12}$$

where $i_B(x; F_X)$ and $i_E(x; F_X)$ are the mutual information densities for the main channel and the wiretapper's channel

$$i_B(x; F_X) = -\phi_B(x) * \log\left(p_Y(x; F_X)\right) - \frac{1}{2}\log\left(2\pi e \sigma_B^2\right) \tag{13}$$

$$i_E(x;F_X) = -\phi_E(x) * \log\left(p_Z(x;F_X)\right) - \frac{1}{2}\log\left(2\pi e\sigma_E^2\right) \tag{14}$$

where $*$ denotes the convolution. We note that the convolutions in (13) and (14) follow from the symmetry of the Gaussian density function. The mutual information and the mutual information density are related through

$$I(X;Y) = \int_{-A}^{A} i_B(x;F_X)dF_X(x) \tag{15}$$

$$I(X;Z) = \int_{-A}^{A} i_E(x;F_X)dF_X(x) \tag{16}$$

Since the Gaussian wiretap channel is stochastically degraded, without loss of generality, we can assume $Z = Y + Z_D$ for some zero-mean Gaussian random variable Z_D with variance $\sigma_D^2 = \sigma_E^2 - \sigma_B^2$. We denote the density of Z_D by $\phi_D(x)$ which leads to the identity $\phi_E = \phi_B * \phi_D$. Using this identity in conjunction with (13)-(14), the equivocation density $r_e(x;F_X)$ in (12) can be expressed as

$$\begin{aligned} r_e(x;F_X) &= \frac{1}{2}\log\left(\frac{\sigma_E^2}{\sigma_B^2}\right) \\ &- \phi_B(x) * \left[\log\left(p_Y(x;F_X)\right) - \phi_D(x) * \log\left(p_Z(x;F_X)\right)\right] \end{aligned} \tag{17}$$

Now, we are ready to obtain the necessary and sufficient conditions for the optimal distribution of the optimization problem in (9). To this end, first, we note that the objective function $g_0(F_X)$ in (9) is Frechet differentiable and the derivative of $g_0(F_X)$ at F_{X_0} in the direction of F_X is given by [4], [10]

$$\begin{aligned} &\lim_{\theta\to 0}\frac{1}{\theta}\left[g_0(\theta F_X + (1-\theta)F_{X_0}) - g_0(F_{X_0})\right] \\ &= \int_{\mathbb{R}} \left(p_Y(y;F_{X_0}) - p_Y(y;F_X)\right)\log\left(p_Y(y;F_{X_0})\right)dy \\ &\quad - \int_{\mathbb{R}} \left(p_Z(z;F_{X_0}) - p_Z(z;F_X)\right)\log\left(p_Z(z;F_{X_0})\right)dz \end{aligned} \tag{18}$$

which, using the equivocation density in (17), is expressed as

$$\begin{aligned} &\lim_{\theta\to 0}\frac{1}{\theta}\left[g_0(\theta F_{X_0} + (1-\theta)F_X) - g_0(F_X)\right] \\ &\qquad = \int_{-A}^{A} r_e(x;F_{X_0})dF_X - g_0(F_{X_0}) \end{aligned} \tag{19}$$

Following similar arguments to those in [4], the necessary and sufficient Kuhn-Tucker conditions for the optimal distribution F_X^* maximizing (9) can be obtained from (19) as follows

$$r_e(x;F_X^*) \le C_s,\ \forall x \in [-A,A] \tag{20}$$

$$r_e(x;F_X^*) = C_s,\ \forall x \in \mathcal{S}_{F_X^*} \tag{21}$$

where the secrecy capacity C_s can be expressed as

$$C_s = h_Y(F_X^*) - h_Z(F_X^*) + \frac{1}{2}\log\left(\frac{\sigma_E^2}{\sigma_B^2}\right) \tag{22}$$

We now prove that the support set $\mathcal{S}_{F_X^*}$ of the optimal distribution is a finite set by contradiction. To reach a contradiction, we use the optimality conditions given by (20)-(21). To this end, we note that both $i_B(x;F_X)$ and $i_E(x;F_X)$ have analytic extensions over the whole complex plane $\mathbb{C}$ [4], and, hence, the equivocation density $r_e(x;F_X)$ also has an analytic extension over $\mathbb{C}$. Now, let us assume that $\mathcal{S}_{F_X^*}$ has infinite number of elements. In view of the optimality condition (21), analyticity of $r_e(z,F_X)$ over all $\mathbb{C}$ and the identity theorem for complex numbers, if $\mathcal{S}_{F_X^*}$ has infinite number of elements, we should have $r_e(z;F_X^*) = C_s$ for all $z \in \mathbb{C}$, which, in turn, implies

$$r_e(x;F_X^*) = C_s, \qquad \forall x \in \mathbb{R} \tag{23}$$

Next, we show that (23) results in a contradiction. To this end, we rearrange (23) by using (17) to get

$$\int_{\mathbb{R}} \phi_B(y-x)v(y)dy = 0, \quad \forall x \in \mathbb{R} \tag{24}$$

where $v(y)$ and c are defined as

$$\begin{aligned} v(y) &= c + \log\left(p_Y(y;F_X^*)\right) \\ &\quad - \int_{\mathbb{R}} \phi_D(\tau)\log\left(p_Z(y-\tau;F_X^*)\right)d\tau \end{aligned} \tag{25}$$

$$c = h_Y(F_X^*) - h_Z(F_X^*) \tag{26}$$

Next, we show that if (24) holds, we should have $v(y) = 0,\ \forall y \in \mathbb{R}$. To this end, we note that since $p_Y(y;F_X^*) = \int_{-A}^{A}\phi_B(y-x)dF_X^*(x)$, Jensen's inequality implies

$$\frac{1}{\sqrt{2\pi\sigma_B^2}} \ge p_Y(y;F_X^*) \ge \frac{1}{\sqrt{2\pi\sigma_B^2}} e^{-\frac{1}{2\sigma_B^2}\int_{-A}^{A}(y-x)^2 dF_X^*(x)} \tag{27}$$

which, in turn, implies $\left|\log\left(p_Y(y;F_X^*)\right)\right| \le \alpha y^2 + \beta$ for some $\alpha,\beta > 0$. Similarly, we can show that $\left|\log\left(p_Z(y;F_X^*)\right)\right| \le \kappa y^2 + \gamma$ for some $\kappa,\gamma > 0$. Consequently, we have $|v(y)| \le \eta y^2 + \zeta$ for some $\eta,\zeta > 0$, which, in conjunction with (24), implies that $v(y) = 0$ for all $y \in \mathbb{R}$ [8, Corollary 9].

Now, we show that we cannot have $v(y) = 0,\ \forall y \in \mathbb{R}$, and therefore, reach a contradiction. In particular, we show that there exists y' such that $v(y) < 0, \forall y \ge y'$. To this end, we first note that since the wiretap channel is stochastically degraded, we have $c < 0$. Next, we introduce the following lemma.

Lemma 1 *There exists sufficiently large y' such that $\forall y \ge y'$, we have*

$$\int_{\mathbb{R}} \phi_D(\tau)\log\left(p_Z(y-\tau;F_X^*)\right)d\tau \ge \log\left(p_Y(y;F_X^*)\right) \tag{28}$$

To prove Lemma 1, first, we find lower and upper bounds for the output densities $p_Z(y;F_X^*)$ and $p_Y(y;F_X^*)$ in terms of $\phi_E(y)$ and $\phi_Z(y)$, respectively. Next, we show that for sufficiently large y, there is a non-zero gap between these two bounds, which implies (28). Due to the space limitations here, we omit the details of the proof.

Lemma 1 and the fact that $c < 0$ imply that $v(y) < 0, \forall y \ge y'$, which, in turn, implies that (24) cannot hold. This, in turn, implies that $\mathcal{S}_{F_X}^*$ cannot have infinite number of elements;

completing the proof of Corollary 1.

We provide a plot of the equivocation density for an optimal input distribution in Fig. 2. We set the associated parameters as $A = 2.6$, $\sigma_B^2 = 1$ and $\sigma_E^2 = 2$, for which the optimal input distribution is quaternary located at $x = \pm 0.64$ and $x = \pm 2.6$ with probability masses 0.2496 at $x = \pm 0.64$ and 0.2504 at $x = \pm 2.6$. We observe that the equivocation density is less than or equal to the secrecy capacity and it is equal to the secrecy capacity at the mass points; verifying the optimality conditions in (20)-(21).

IV. Proof of Theorem 2

In this section, we extend our analysis in the previous section to the entire rate-equivocation region which can be characterized by solving the following optimization problem

$$\max_{\mathcal{F}_X \in \Omega} g_\mu(F_X) = \max_{\mathcal{F}_X \in \Omega} \mu I(X;Y) + I(X;Y) - I(X;Z) \tag{29}$$

for all $\mu \geq 0$. Since the objective function $g_\mu(F_X)$ in (29) is strictly concave, and the feasible set Ω is convex and sequentially compact with respect to the Levy metric, the optimization problem in (29) has a unique maximizer. We denote the optimal input distribution for (29) as F_X^* which depends on the value of μ.

Now, we obtain the necessary and sufficient conditions for the optimal distribution of the optimization problem in (29). To this end, we note that $g_\mu(F_X)$ is Frechet differentiable, and its derivative at F_{X_0} in the direction of F_X is given as

$$\begin{aligned}&\lim_{\theta \to 0} \frac{1}{\theta} \left[g_\mu(\theta F_X + (1-\theta) F_{X_0}) - g_\mu(F_{X_0}) \right] \\ &= \int_{-A}^{A} \left[\mu i_B(x; F_{X_0}) + r_e(x; F_{X_0}) \right] dF_X - g_\mu(F_{X_0}) \end{aligned} \tag{30}$$

Using similar arguments to those in [4], the necessary and sufficient conditions for the optimal distribution of the optimization problem in (29) can be obtained as follows

$$\mu i_B(x; F_X^*) + r_e(x; F_X^*) \leq (\mu+1) I_B(F_X^*) - I_E(F_X^*), \quad x \in [-A, A] \tag{31}$$

$$\mu i_B(x; F_X^*) + r_e(x; F_X^*) = (\mu+1) I_B(F_X^*) - I_E(F_X^*), \quad x \in \mathcal{S}_{F_X^*} \tag{32}$$

Now, we show that the optimal input distribution F_X^* should have finite support. Similar to the proof of Corollary 1, here also, we prove the finiteness of the support set by contradiction and using the optimality conditions in (31)-(32).

Let us assume that $\mathcal{S}_{F_X^*}$ has infinite number of elements. Under this assumption, (32), analyticity of $i_B(x; F_X^*)$ and $r_e(x; F_X^*)$ over all $\mathbb{C}$ and identity theorem of complex numbers imply that $\mu i_B(x; F_X^*) + r_e(x; F_X^*) = (\mu+1) I_B(F_X^*) - I_E(F_X^*)$ over all $\mathbb{C}$, which, in turn, implies that

$$\mu i_B(x; F_X^*) + r_e(x; F_X^*) = (\mu+1) I_B(F_X^*) - I_E(F_X^*) \tag{33}$$

over all $x \in \mathbb{R}$. Next, we show that (33) results in a contradiction. To this end, we first rearrange (33) to obtain

$$\int_{\mathbb{R}} \phi_B(y-x) \hat{v}(y) dy = 0 \tag{34}$$

where $\hat{v}(y)$ and $\hat{c}$ are given by

$$\begin{aligned}\hat{v}(y) &= \hat{c} + (\mu+1) \log\left(p(y; F_X^*)\right) \\ &\quad - \int_{\mathbb{R}} \phi_D(\tau) \log\left(p(y-\tau; F_X^*)\right) d\tau \end{aligned} \tag{35}$$

$$\hat{c} = (\mu+1) h_Y(F_X^*) - h_Z(F_X^*) \tag{36}$$

By using similar arguments to those we provided in the proof of Corollary 1, one can show that $|\hat{v}(y)| \leq \eta y^2 + \zeta$ for some $\eta, \zeta > 0$. By [8, Corollary 9], this implies that if (34) holds, we should have $\hat{v}(y) = 0, \forall y \in \mathbb{R}$. Next, we show that we cannot have $\hat{v}(y) = 0, \forall y \in \mathbb{R}$. Using Lemma 1 and the fact that $h_Y(F_X^*) - h_Z(F_X^*) < 0$ in (35), we get

$$\hat{v}(y) - \mu\big(h_Y(F_X^*) + \log\left(p_Y(y; F_X^*)\right)\big) < 0, \quad \forall y \geq y' \tag{37}$$

Hence, if $\hat{v}(y) = 0, \forall y \in \mathbb{R}$ holds, due to (37), we should have

$$h_Y(F_X^*) + \log\left(p_Y(y; F_X^*)\right) > 0, \quad \forall y \geq y' \tag{38}$$

which implies

$$p_Y(y; F_X^*) \geq e^{-h_Y(F_X^*)}, \quad \forall y \geq y' \tag{39}$$

However, since $p_Y(y; F_X^*)$ is a density function, it has to vanish as $y \to \infty$, and (39) cannot hold. Hence, we reach a contradiction; implying that the optimal input distribution should have a finite support set. This completes the proof of Theorem 2.

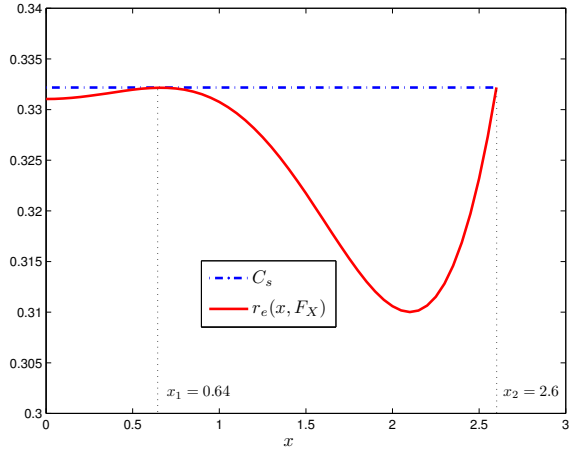

Fig. 2. Illustration of the equivocation density yielded by the optimal input distribution when $\sigma_B^2 = 1$, $\sigma_E^2 = 2$ and $A = 2.6$.

V. Numerical Results

In this section, we provide numerical illustrations for the secrecy capacity and the rate-equivocation region of the Gaussian wiretap channel under a peak power constraint.

We first consider how the secrecy capacity changes with

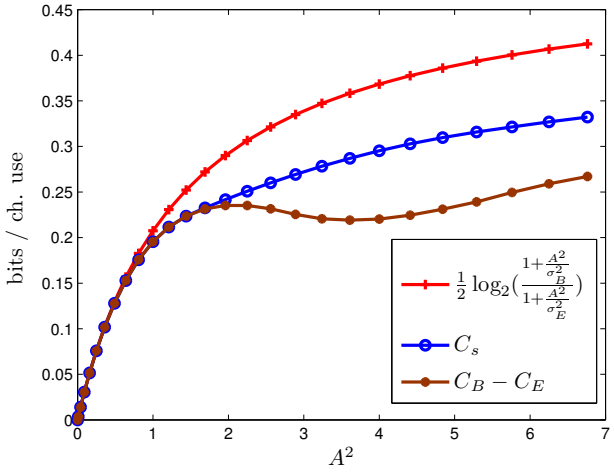

Fig. 3. The secrecy capacity for $\sigma_B^2 = 1$ and $\sigma_E^2 = 2$ versus the square of the amplitude constraint A.

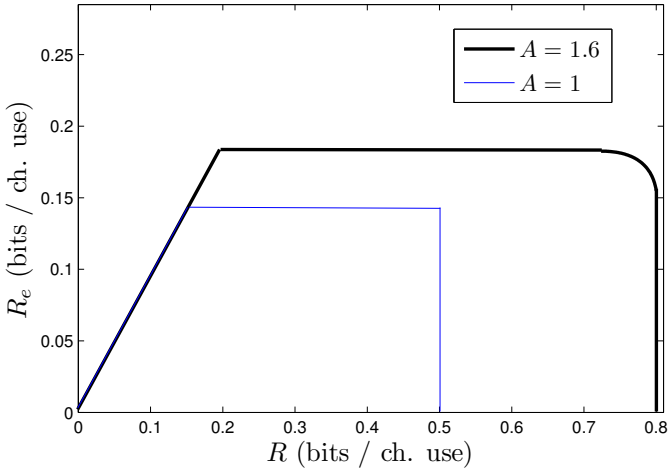

Fig. 4. The rate-equivocation regions for $\sigma_B^2 = 1$ and $\sigma_E^2 = 1.6$ under amplitude constraints $A = 1$ and $A = 1.6$.

respect to the amplitude constraint A for $\sigma_B^2 = 1$ and $\sigma_E^2 = 2$. We observe in Fig. 3 that the increase rate of both the secrecy capacity under a peak power constraint A and the secrecy capacity under an average power constraints A^2 are similar. A similar observation was made by Smith [4] for the capacities under a peak power constraint and under an average power constraint. Moreover, in Fig. 3, we also plot the difference between the legitimate user's and the eavesdropper's capacities, i.e., $C_B - C_E$, which in general, provides a lower bound for the secrecy capacity C_s. On the other hand, 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.

In Fig. 4, we plot the entire rate-equivocation region of the wiretap channel when $\sigma_B^2 = 1$ and $\sigma_E^2 = 1.6$ for two different values of A. When $A = 1$, it is clear from Fig. 4 that both the secrecy capacity and the capacity can be attained simultaneously. In particular, for $A = 1$, the binary input distribution located at $\pm A$ achieves both the capacity and the secrecy capacity, i.e., the optimal input distributions for the secrecy capacity and the capacity are identical. In other words, when $A = 1$, the transmitter can communicate with the legitimate user at the capacity while achieving the maximum equivocation at the same time. On the other hand, when $A = 1.6$, the secrecy capacity and the capacity cannot be achieved simultaneously. In particular, for $A = 1.6$, the binary input distribution located at $\pm A$ achieves the capacity, while a ternary distribution located at $x = \pm 1.6$ and $x = 0$ with probability masses 0.358 at ± 1.6 and 0.284 at 0 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 the equivocation in the sense that, to increase the communication rate, we should compromise from the equivocation of this communication, and to increase the achieved equivocation, we should compromise from the communication rate. This result is in contrast with the average power constraint case, where irrespective of the average power constraint, both the secrecy capacity and the capacity can be simultaneously achieved by a Gaussian distribution with full power.

VI. Conclusion

In this paper, we study the Gaussian wiretap channel under a peak power constraint. We show that the boundary of the entire rate-equivocation region is achieved by input distributions that have finite support. We prove this result by using the methodology in [4] for our setting. An interesting aspect that our result reveals is that, unlike the average power constrained Gaussian wiretap channel, under a peak power constraint, the secrecy capacity and the capacity cannot be obtained simultaneously in general, i.e., there is a tradeoff between the rate and equivocation for the peak power constrained case.

References

[1] A. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journal*, vol. 54, pp. 1355–1387, October 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. on Inform. Theory*, vol. 24, pp. 339–348, May 1978.

[3] S. K. Leung-Yan-Cheung and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. on Inform. Theory*, vol. 24, pp. 451–456, July 1978.

[4] J. G. Smith, "The information capacity of amplitude and variance-constrained scalar Gaussian channels," *Information and Control*, vol. 18, pp. 203–219, April 1971.

[5] S. Shamai and I. Bar-David, "The capacity of average and peak-power-limited quadrature Gaussian channels," *IEEE Trans. on Information Theory*, vol. 41, pp. 1060–1071, July 1995.

[6] I. Abu-Faycal, M. Trott, and S. Shamai, "The capacity of discrete-time memoryless rayleigh fading channels," *IEEE Trans. on Information Theory*, vol. 47, pp. 1290–1301, May 2001.

[7] M. C. Gursoy, H. V. Poor, and S. Verdu, "The noncoherent Rician fading channel part-I: Structure of the capacity achieving input," *IEEE Trans. Wireless Commun.*, vol. 4, pp. 2193–2206, September 2005.

[8] T. H. Chan, S. Hranilovic, and F. Kschischang, "Capacity-achieving probability measure for conditionally Gaussian channels with bounded inputs," *IEEE Trans. Inform. Theory*, vol. 51, pp. 2073–2088, June 2005.

[9] L. Zhang and D. Guo, "Capacity of Gaussian channels with duty cycle and power constraints," in *IEEE ISIT*, July 2011.

[10] A. Tchamkerten, "On the discreteness of capacity achieving distributions," *IEEE Trans. on Information Theory*, vol. 50, pp. 2273–2278, November 2004.