Information-Spectrum Methods for Information-Theoretic Security

Matthieu Bloch and J. Nicholas Laneman
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN, 46556, USA
Email: {mbloch1, jnl}@nd.edu

***Abstract*—We investigate the potential of an information-spectrum approach to information-theoretic security. We show how this approach provides conceptually simple yet powerful results that can be used to investigate complex communication scenarios. In particular, we illustrate the usefulness of information-spectrum methods by analyzing the effect of channel state information (CSI) on the secure rates achievable over wiretap channels. We establish a formula for secrecy capacity, which we then specialize to compute achievable rates for ergodic fading channels in the presence of imperfect CSI. Our results confirm the importance of having some knowledge about the eavesdropper's channel, but also show that imperfect CSI does not necessarily preclude security.**

I. Introduction

Renewed interest in information-theoretic security has led to numerous extensions of the wiretap channel model, which was initially introduced by Wyner [1] and generalized by Csiszár and Körner [2]. The salient features unveiled by recent contributions are probably the benefit of feedback [3], [4], interference, and jamming [5], and the usefulness of fading in wireless environment [6], [7], [8].

These information-theoretic results strongly advocate for the use of physical-layer schemes to provide security, but it is fair to acknowledge that there exist several conceptual issues that hinder the acceptance of the wiretap channel as a credible cryptographic model. First, security with respect to the eavesdropper is often assessed in terms of a mutual information rate (*weak secrecy*), which is known to be unsatisfactory from a cryptographic perspective. Second, the model ignores the need for authentication of the legitimate parties, the possibility of a malicious (not purely passive) eavesdropper, and the imperfections of the channel state information (CSI) available at the transmitter.

The aforementioned issues are often dismissed under the assumption that the adversary is "honest but curious", that is he abides by a predefined protocol but attempts to extract as much information as he can from his available observations. Nevertheless, there is probably a need for more sophisticated mathematical tools that are powerful enough to handle some of the conceptual issues, yet simple enough to remain tractable. As discussed in [9], information-spectrum methods [10] offer a promising framework to study complicated wiretap channel models. In this work, we further investigate the usefulness of the information-spectrum approach and we analyze achievable rates of secure communication in the presence of partial or noisy CSI. Although we do not obtain an exact expression for secrecy capacity, our results highlight the critical role of CSI for security. Our approach draws on [11] and exploits the general formula for secrecy capacity obtained via the information-spectrum approach [9], [12] to significantly simplify the analysis.

The remainder of the paper is organized as follows. In Section II, we introduce notation and basic definitions, and we recall known facts about general wiretap channels. In Section III, we introduce a generic model of wiretap channel with causal channel state information and we provide a general (but likely incomputable) formula for secrecy capacity. In Section IV, we investigate various Gaussian ergodic fading channels with imperfect CSI, and we illustrate our results with a numerical example.

II. Preliminaries

A. Notation and basic definitions

First, a word about notation and definitions. Consider two random variables X and Y taking values in alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively. Sample values of X and Y are denoted by x and y, respectively, the joint probability law is denoted by $p_{\mathsf{XY}}(\mathsf{x},\mathsf{y})$, and the marginal probabilities are denoted by $p_{\mathsf{X}}(\mathsf{x})$ and $p_{\mathsf{Y}}(\mathsf{y})$, respectively. The expectation of X is denoted by $\mathbb{E}_{\mathsf{X}}[\mathsf{X}]$, and unless mentioned otherwise, alphabets are assumed to be abstract alphabets, including countably infinite or continuous alphabets. The *mutual information* between X and Y is the random variable $\mathrm{I}(\mathsf{X};\mathsf{Y}) := \log \frac{p_{\mathsf{XY}}(\mathsf{X},\mathsf{Y})}{p_{\mathsf{X}}(\mathsf{X})p_{\mathsf{Y}}(\mathsf{Y})}$. Note that the average of the mutual information random variable is the usual *average mutual information* $\mathbb{I}(\mathsf{X};\mathsf{Y})$. The *variational distance* between two random variables $\mathsf{X} \in \mathcal{X}$ and $\mathsf{X}' \in \mathcal{X}$ is defined as

$$d\left(p_{\mathsf{X}}, p_{\mathsf{X}'}\right) = \sum_{\mathsf{x}\in\mathcal{X}} \left|p_{\mathsf{X}}(\mathsf{x}) - p_{\mathsf{X}'}(\mathsf{x})\right|.$$

For a given sequence $\{\mathsf{X}_n\}_{n=1}^{\infty}$ of random variables, the lim-sup and lim-inf in probability are defined as

$$\operatorname*{p-limsup}_{n\to\infty} \mathsf{X}^n := \inf\left\{\alpha : \lim_{n\to\infty} \mathbb{P}[\mathsf{X}^n > \alpha] = 0\right\},$$

and

$$\operatorname*{p-liminf}_{n\to\infty} \mathsf{X}^n := \sup\left\{\beta : \lim_{n\to\infty} \mathbb{P}[\mathsf{X}^n < \beta] = 0\right\},$$

respectively. These two quantities play a central role in information-spectrum methods.

B. General wiretap channel

A general wiretap channel is denoted by $\left(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \left\{p_{\mathsf{Y}^n\mathsf{Z}^n|\mathsf{X}^n}(\mathsf{y}^n, \mathsf{z}^n|\mathsf{x}^n)\right\}_{n=1}^{\infty}\right)$ and consists of an arbitrary input alphabet $\mathcal{X}$, two arbitrary output alphabets $\mathcal{Y}$ and $\mathcal{Z}$, and a sequence of transition probabilities $\left\{p_{\mathsf{Y}^n\mathsf{Z}^n|\mathsf{X}^n}(\mathsf{y}^n, \mathsf{z}^n|\mathsf{x}^n)\right\}_{n=1}^{\infty}$. By convention, the channel $\left(\mathcal{X}, \mathcal{Y} \left\{p_{\mathsf{Y}^n|\mathsf{X}^n}(\mathsf{y}^n|\mathsf{x}^n)\right\}_{n=1}^{\infty}\right)$ is called the *legitimate receiver's channel*, and the channel $\left(\mathcal{X}, \mathcal{Z}, \left\{p_{\mathsf{Z}^n|\mathsf{X}^n}(\mathsf{z}^n|\mathsf{x}^n)\right\}_{n=1}^{\infty}\right)$ is called the *eavesdropper's channel*.

Definition 1: Am $\left(n, \lceil 2^{nR}\rceil, \epsilon_n\right)$ code for a general wiretap channel consists of the following.

- a set $\mathcal{M}_n = \left\{1, \ldots, \lceil 2^{nR}\rceil\right\}$;
- a stochastic encoding function $f_n : \mathcal{M}_n \to \mathcal{X}^n$;
- a decoding function $g_n : \mathcal{Y}^n \to \mathcal{M}_n$,

such that the average probability of error satisfies $\mathbb{P}[g_n(\mathsf{Y}^n) \neq \mathsf{M}] \leq \epsilon_n$, and $d(p_{\mathsf{M}\mathsf{Z}^n}, p_{\mathsf{M}}p_{\mathsf{Z}^n}) \leq \delta_n$.

A rate R is achievable is there exists a sequence of $\left(n, \lceil 2^{nR}\rceil, \epsilon_n\right)$ codes with

$$\lim_{n\to\infty} \epsilon_n = 0, \qquad \lim_{n\to\infty} \delta_n = 0,$$

and the *secrecy capacity* C_s is defined as the supremum of all achievable rates. It can be shown that the secrecy capacity of a general channel is given by the following theorem.

Theorem 1 ([9], [12]): The secrecy capacity of a wiretap channel $\left(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \left\{p_{\mathsf{Y}^n\mathsf{Z}^n|\mathsf{X}^n}(\mathsf{y}^n, \mathsf{z}^n|\mathsf{x}^n)\right\}_{n=1}^{\infty}\right)$ is

$$C_s = \max_{\{\mathsf{V}^n, \mathsf{X}^n\}_{n=1}^{\infty}} \left(\text{p-liminf}_{n\to\infty} \frac{1}{n}\mathrm{I}(\mathsf{V}^n; \mathsf{Y}^n) - \text{p-limsup}_{n\to\infty} \frac{1}{n}\mathrm{I}(\mathsf{V}^n; \mathsf{Z}^n)\right),$$

where the process $\{\mathsf{V}^n, \mathsf{X}^n\}_{n=1}^{\infty}$ satisfies

$$\mathsf{V}^n \to \mathsf{X}^n \to \mathsf{Z}^n\mathsf{Y}^n \quad \forall n \in \mathbb{N}^*.$$

Notice that this general formula for secrecy capacity resembles that obtained for discrete memoryless channels. We also emphasize that secrecy with respect to the eavesdropper is assessed in terms of the variational distance, which is a stronger criterion than weak secrecy.

III. Wiretap Channel with Imperfect State Information

As an illustration of the usefulness of the information-spectrum approach to secrecy capacity, we investigate wiretap channels with imperfect state information. The perfect knowledge of channel state information is implicit in the early work of Wyner and Csiszár and Körner, and it is arguably not a critical issue for static channels whose parameters remain constant over time; however, if the channel parameters vary over time, the availability of perfect CSI becomes somewhat questionable. Legitimate parties can always cooperate to characterize their communication channel precisely, but it is doubtful that an adversary would do so; additionally, even if all players cooperate, CSI is usually available through side-channels that are either noisy or rate-limited. With the notable exception of [6], [7], few contributions have considered the effect of channel state information on security. The model used in [7] is a block-ergodic fading model in which the ergodicity makes it possible to code across many realizations of the eavesdropper's fading, thereby completely removing the need for CSI about the eavesdropper's channel. The authors of [6] investigate a quasi-static fading model and provide simple bounds on the probability of secrecy outage in the presence of noisy CSI.

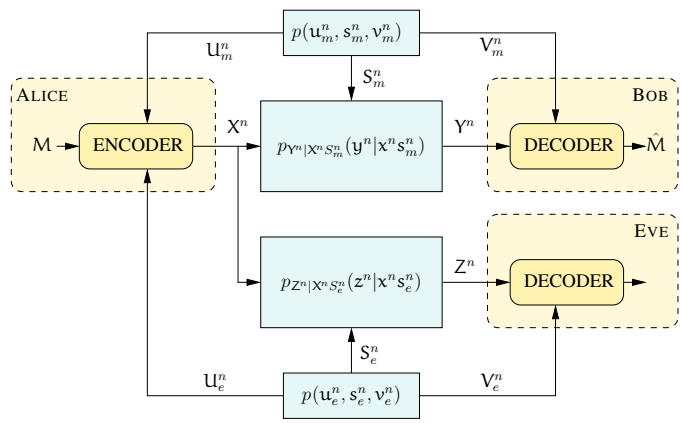

Fig. 1. Wiretap channel with channel state information.

Here, we consider the channel model illustrated in Figure 1, with input alphabet $\mathcal{X}$, and output alphabets $\mathcal{Y}$ and $\mathcal{Z}$ to the legitimate receiver and eavesdropper, respectively. We assume that the legitimate receiver's channel is governed by a state S_m^n, and the eavesdropper's channel is governed by another state S_e^n. For all $n \geq 0$, the transition probabilities are assumed to be of the form

$$p_{\mathsf{Y}^n\mathsf{Z}^n|\mathsf{X}^n\mathsf{S}_m^n\mathsf{S}_e^n}(\mathsf{y}^n, \mathsf{z}^n|\mathsf{x}^n, \mathsf{s}_m^n, \mathsf{s}_e^n) = p_{\mathsf{Y}^n|\mathsf{X}^n\mathsf{S}_m^n}(\mathsf{y}^n|\mathsf{x}^n, \mathsf{s}_m^n)\, p_{\mathsf{Z}^n|\mathsf{X}^n\mathsf{S}_e^n}(\mathsf{z}^n|\mathsf{x}^n\mathsf{s}_e^n).$$

The transmitter is provided with *causal* CSI U_m^n and U_e^n about the legitimate user's channel an eavesdropper's channel, who respectively obtain CSI V_m^n and V_e^n about their own channel[1]. The form of the transition probabilities is appropriate to model situations in which receivers report back CSI to the transmitter. A more general model would consider transition probabilities that do not factorize as above, but this approach is not pursued here; however, we emphasize that S_m and S_e need not be independent, but we assume that $(\mathsf{U}_{m,n}, \mathsf{S}_{m,n}, \mathsf{V}_{m,n}, \mathsf{U}_{e,n}, \mathsf{S}_{e,n}, \mathsf{V}_{e,n})$ is independent of past inputs X^{n-1}.

Definition 2: An $\left(n, \lceil 2^{nR}\rceil, \epsilon_n, \delta_n\right)$ wiretap code of such a channel consists of the following.

- a set $\mathcal{M}_n = \{1, \ldots, \lceil 2^{nR}\rceil\}$;

[1]By writing $\mathsf{V}_e^n = (\mathsf{V}_e^n, \mathsf{V}_m^n)$, we can consider situations in which the eavesdropper knows what the legitimate receiver receives.

- a set of stochastic encoding functions $f_i : \mathcal{M}_n \times \mathcal{U}_e^i \times \mathcal{U}_m^i \to \mathcal{X}$ for $i \in \{1, \ldots, n\}$;
- a decoding function $g_n : \mathcal{Y}^n \times \mathcal{V}_m^n \to \mathcal{M}_n$,

such that the average probability or error satisfies $\mathbb{P}[g_n(\mathsf{Y}^n) \neq \mathsf{M} | \mathsf{X}^n = f_n(\mathsf{M})] \leq \epsilon_n$ and the variational distance $d(p_{\mathsf{M}\mathsf{Z}^n}, p_{\mathsf{M}} p_{\mathsf{Z}^n}) \leq \delta_n$.

A rate R is achievable if there exists a sequence of $\left(n, \lceil 2^{nR} \rceil, \epsilon_n, \delta_n\right)$ codes such that

$$\lim_{n\to\infty} \epsilon_n = \lim_{n\to\infty} \delta_n = 0,$$

and secrecy capacity is defined as the supremum of all achievable rates.

The following theorem provides a generic formula for secrecy capacity in terms of the lim-sup in probability and lim-inf in probability of information-density rates.

Theorem 2: The secrecy capacity of an arbitrary wiretap channel with channel state information is given by

$$C_s = \max_{\{\mathsf{R}^n, \mathsf{T}^n\}_{n=0}^{\infty}} \left(\text{p-limsup}_{n\to\infty} \frac{1}{n} \mathrm{I}(\mathsf{R}^n; \mathsf{Y}^n | \mathsf{V}_m^n) - \text{p-liminf}_{n\to\infty} \frac{1}{n} \mathrm{I}(\mathsf{R}^n; \mathsf{Z}^n | \mathsf{V}_e^n) \right), \quad (1)$$

where $\{\mathsf{R}^n, \mathsf{T}^n\}_{n=0}^{\infty}$ is such that $\mathsf{R}^n \to \mathsf{T}^n \to \mathsf{X}^n \to \mathsf{Y}^n \mathsf{Z}^n$ for all n.

Proof: The proof is based on the same arguments as in [13]. Assuming that $\mathcal{U}_m$ and $\mathcal{U}_e$ are finite, the channel is transformed into an equivalent one without CSI at the transmitter and receivers, whose input symbol is a vector $\mathsf{T}_i \in \mathcal{X}^{|\mathcal{U}_m|^i \times |\mathcal{U}_e|^i}$ and whose output are the pairs $(\mathsf{Y}_i, \mathsf{V}_{m,i})$ and $(\mathsf{Y}_i, \mathsf{V}_{e,i})$. A code $\mathcal{C}$ for the new channel is a set

$$\mathcal{C} = \{\mathsf{t}^n(\mathsf{m}) = (\mathsf{t}_1(\mathsf{m}), \ldots, \mathsf{t}_n(\mathsf{m})) : \mathsf{m} \in \mathcal{M}, \mathsf{t}_i(\mathsf{m}) \in \mathcal{X}^{|\mathcal{U}_m|^i \times |\mathcal{U}_e|^i}\},$$

and at each time i, the channel input is the component of the vector $\mathsf{t}_i(\mathsf{m})$ indexed by $(\mathsf{u}_m^i, \mathsf{u}_e^i)$. An input process $\{\mathsf{T}^n\}_{n=0}^{\infty}$ is entirely characterized by a set of probabilities $\{p_{\mathsf{T}^n}(\mathsf{t}^n)\}_{n=0}^{\infty}$, and the transition probability of the new channel is

$$p(\mathsf{y}^n, \mathsf{z}^n, \mathsf{v}_m^n, \mathsf{v}_e^n | \mathsf{t}^n) = \sum_{\mathsf{s}_m^n, \mathsf{s}_e^n, \mathsf{u}_m^n, \mathsf{u}_e^n} p(\mathsf{y}^n, \mathsf{z}^n | \mathsf{t}^n(\mathsf{u}_m^n, \mathsf{u}_e^n), \mathsf{s}_m^n, \mathsf{s}_e^n) \, p(\mathsf{u}_m^n, \mathsf{u}_e^n, \mathsf{v}_m^n, \mathsf{v}_e^n, \mathsf{s}_m^n, \mathsf{s}_e^n).$$

This new channel is strictly equivalent to the original one it terms of capacity; therefore, applying the information-spectrum formula of Theorem 1 yields the desired result. The proof can be extended to continuous alphabets $\mathcal{U}_m$ and $\mathcal{U}_e$ using discrete approximations. ■

Despite its generality, the above result can hardly be evaluated numerically because the maximization in Equation (1) is performed over all possible input processes; nevertheless, by restricting processes $\{\mathsf{T}^n\}_{n=0}^{\infty}$ to simpler classes (for instance, memoryless processes), it is possible, in most situations, to obtain computable achievable rates. By substituting appropriate processes in (1), we can turn the determination of achievable rates into a simpler optimization problem.

IV. Gaussian Wiretap Fading Channels

In this section, we specialize the general results of Theorem 2 to Gaussian wiretap fading channels with various types of fading. We briefly derive known achievable rates for block-ergodic fading without eavesdropper CSI [7] and discuss the effect of partial CSI and imperfect CSI on secure communication rates. Throughout the remainder of the paper, we consider a real Gaussian fading channel for which the observations of the legitimate receiver and the eavesdropper are given by

$$\mathsf{Y}_i = \sqrt{\mathsf{S}_{m,i}} \mathsf{X}_i + \mathsf{N}_{m,i},$$
$$\mathsf{Z}_i = \sqrt{\mathsf{S}_{e,i}} \mathsf{X}_i + \mathsf{N}_{e,i},$$

where $\{\mathsf{N}_{m,i}\}_{i\geq 1}$ and $\{\mathsf{N}_{e,i}\}_{i\geq 1}$ are sequences of i.i.d. zero-mean unit variance Gaussian random variables.

A. Ergodic fading with perfect CSIR and imperfect CSIT

In this section, we assume CSIs U_m and U_e available at the transmitter are imperfect versions of the actual fading realizations $\mathsf{S}_{e,i}$ and $\mathsf{S}_{m,i}$, but receivers have perfect knowledge of their instantaneous received signal-to-noise ratio (SNR), that is

$$\mathsf{V}_{m,i} = \mathsf{S}_{m,i} \mathbb{E}\left[\mathsf{X}_i^2 | \mathsf{U}_{e,i}, \mathsf{U}_{m,i}\right],$$
$$\text{and} \quad \mathsf{V}_{e,i} = \mathsf{S}_{e,i} \mathbb{E}\left[\mathsf{X}_i^2 | \mathsf{U}_{e,i}, \mathsf{U}_{m,i}\right].$$

Proposition 1: The following rates are achievable with imperfect CSI at transmitter and perfect CSI at receiver.

$$R_s < \max_{\gamma} \mathbb{E}_{\mathsf{S}_m \mathsf{S}_e \mathsf{U}_m \mathsf{U}_e} \left[\frac{1}{2} \log \left(\frac{1 + \mathsf{S}_m \gamma(\mathsf{U}_m, \mathsf{U}_e)}{1 + \mathsf{S}_e \gamma(\mathsf{U}_m, \mathsf{U}_e)} \right) \right], \quad (2)$$

where S_m, S_e, U_m, and U_e are random variables whose distribution is the first order distribution of the corresponding ergodic processes and γ is a deterministic function such that $\mathbb{E}_{\mathsf{U}_m \mathsf{U}_e}[\gamma(\mathsf{U}_m, \mathsf{U}_e)] \leq P$.

Sketch of proof: Following [11], we consider a new channel with input T_i defined as

$$\begin{aligned} \mathsf{Y}_i &= \sqrt{\mathsf{H}_{m,i}} \mathsf{T}_i + \mathsf{N}_{m,i} \\ \mathsf{Z}_i &= \sqrt{\mathsf{H}_{e,i}} \mathsf{T}_i + \mathsf{N}_{e,i}, \end{aligned} \quad (3)$$

where $\mathsf{H}_{m,i} = S_{m,i} \gamma(\mathsf{U}_{m,i}, \mathsf{U}_{e,i})$, $\mathsf{H}_{e,i} = S_{e,i} \gamma(\mathsf{U}_{m,i}, \mathsf{U}_{e,i})$, and γ is a deterministic time-invariant function such that $\mathbb{E}[\gamma(\mathsf{U}_m, \mathsf{U}_e)] \leq P$. The input of the channel should satisfy the power constraint $\mathbb{E}\left[\mathsf{T}_n^2\right] \leq 1$. Clearly, the capacity of the original channel is at least the capacity of the new one as it corresponds to a specific use of the CSI at the transmitter. We can again apply the general formula of secrecy capacity to this new channel, and choose $\mathsf{T}_i \sim \mathcal{N}(0, 1)$. For this choice, we obtain $\mathsf{Y}_i | \mathsf{T}_i \mathsf{V}_{m,i} \sim \mathcal{N}(0, 1)$ and $\mathsf{Y}_i | \mathsf{V}_{m,i} \sim \mathcal{N}(0, 1 + \mathsf{H}_{m,i})$;

substituting this densities in the information density rate of the legitimate receiver's channel, we obtain

$$\frac{1}{n}\mathrm{I}(\mathsf{T}^n;\mathsf{Y}^n|\mathsf{V}_m^n) = \frac{1}{n}\sum_{i=1}^{n}\frac{1}{2}\left(\log(1+\mathsf{H}_{m,i}) - \mathsf{N}_{m,i}^2 + \frac{\mathsf{Y}_i^2}{1+\mathsf{H}_{m,i}}\right)$$

Using the ergodicity and stationarity of the H_m and S_m, the above quantity can be shown to converge in probability to

$$\mathbb{E}_{\mathsf{H}_m}[\log(1+\mathsf{H}_m)] = \mathbb{E}_{\mathsf{S}_m\mathsf{U}_m,\mathsf{U}_e}[\log(1+S_m\gamma(\mathsf{U}_m,\mathsf{U}_e)],$$

where $\mathsf{S}_m, \mathsf{U}_m, \mathsf{U}_e$ have the same first-order distribution as the corresponding processes. Repeating the same argument for the eavesdropper's channel, we obtain the desired result. ■

The function γ controls the power allocated for each realization of the CSI $(\mathsf{U}_m, \mathsf{U}_e)$ observed by the transmitter. The simple form of (2) allows us to solve the optimization exactly, as given by the following lemma.

Lemma 1: Let the function $f_{uv}(\gamma)$ be defined as

$$f_{uv}(\gamma) = \iint \frac{s-t}{(1+s\gamma(u,v))(1+t\gamma(u,v))}p(s|u)p(t|v)dsdt.$$

Then, $\gamma(u,v)$ defined as

$$\gamma(u,v) = \begin{cases} f_{uv}^{-1}(\lambda) & \text{if } 0 \le \lambda \le \mathbb{E}[\mathsf{S}-\mathsf{T}|u,v], \\ 0 & \text{else.} \end{cases}$$

is the optimal power allocation under power constraint

$$P(\lambda) = \sum_{u,v} p(u,v)\gamma(u,v).$$

Proof: By forming the Lagrangian $\mathcal{L}$ as follows

$$\mathcal{L} = \sum_{u,v} p(u,v)\iint \log\left(\frac{1+s\gamma(u,v)}{1+t\gamma(u,v)}\right)p(s|u)p(t|v)dsdt - \lambda\sum_{u,v}p(u,v)\gamma(u,v)$$

and by using the Karush-Kuhn-Tucker conditions with respect to the function $\gamma(u,v)$, we obtain the desired result. Under the assumption that there exists $(\mathsf{u}_o, \mathsf{v}_0)$ such that $\mathbb{E}[\mathsf{S}-\mathsf{T}|\mathsf{u}_0,\mathsf{v}_0] > 0$, it can be shown that using the full power P is optimal. ■

By varying λ, Lemma 1 provides the optimal power allocation for all power constraints P. Since $\lambda \ge 0$, notice that $\gamma(u,v) = 0$ whenever $\mathbb{E}[\mathsf{S}|u,v] \le \mathbb{E}[\mathsf{T}|u,v]$, which is consistent with the intuition that no power should be allocated when the eavesdropper's channel is expected to be better than the legitimate receiver's channel.

The situations in which the transmitter has perfect CSI or no CSI are special cases of the above analysis. If the transmitter has perfect CSI about both channels ($\mathsf{U}_m^n = \mathsf{S}_m^n$,$\mathsf{U}_e^n = \mathsf{S}_e^n$), the optimal power allocation does not depend on fading statistics and can be derived in closed-form; using Lemma 1, we obtain

$$\gamma(u,v) = \begin{cases} \left\{\frac{1}{\lambda}-\frac{1}{u}\right\}^+ & \text{if } u>0, v=0 \\ \frac{1}{2}\left\{-\left(\frac{1}{v}+\frac{1}{u}\right)+\sqrt{\left(\frac{1}{v}-\frac{1}{u}\right)\left(\frac{4}{\lambda}+\frac{1}{v}-\frac{1}{u}\right)}\right\}^+ & \text{if } u,v>0, \\ 0 & \text{otherwise,} \end{cases}$$

which is what was already obtained in [8], albeit with a completely different approach. If the transmitter has no CSI (U_m^n independent of S_m^n and U_e^n independent of S_e^n), the achievable rates in (2) are maximized by a constant power allocation. Whether these rates are strictly positive or not depends on the statistics of the fading S_m^n and S_e^n and of the noise N_m^n and N_e^n; in particular, rates are zero when the fading and noise statistics are identical on both channels.

B. Numerical examples

We now illustrate the above result with a numerical example. We consider a wiretap channel for which $\{\mathsf{S}_{m,i}\}_{i\ge1}$ and $\{\mathsf{S}_{e,i}\}_{i\ge1}$ are i.i.d. processes with $\mathsf{S}_{m,i}$ and $\mathsf{S}_{e,i}$ uniformly distributed over $[0,2]$. Receivers have perfect knowledge of their own instantaneous received SNRs, and U_m (resp. U_e) is a uniformly quantized version of S_m (resp. S_e) obtained with N_m (resp. N_e) intervals. This situation clearly satisfies the condition of Lemma 1 if $N_m, N_e \ge 2$, which allows us to find the optimal power allocation.

Figure 2 illustrates the impact of quantized CSI on achievable rates when the transmitter has the same precision on the eavesdropper and legitimate receiver CSI ($N_m = N_e := N$). As expected, the penalty imposed by quantization vanishes as the precision increases. Interestingly, only one bit of feedback closes most of the gap between no CSI and full CSI, and the rate gain becomes marginal for more that five quantization intervals. At low SNR (less than 0dB), precision seems even less critical and one bit of feedback is sufficient. In the high SNR regime, the asymptotic limits of achievable secure rates can be computed exactly and are given by

$$R_s^{\lim} = \frac{N(N-1)\log N - 2\sum_{k=1}^{N-1}k\log k}{2N^2}$$

Based on the expression above, one can also show that

$$R_s^{\lim} = \frac{1}{4} - \frac{\log N}{8N^2} + o\left(\frac{\log N}{N^2}\right) \quad \text{as} \quad N\to\infty.$$

Figure 3 shows the impact of asymmetric precision of CSI for the legitimate receiver's channel and eavesdropper's channel. Interestingly, the lack of precision on the eavesdropper's CSI can be somewhat compensated by increasing the precision of the legitimate receiver's CSI. For instance, the rates attained with $N_m = 5$ quantization intervals for the legitimate receiver and $N_e = 2$ quantization intervals for the eavesdropper are close to those attained with $N_m = N_e = 2$ for both channels.

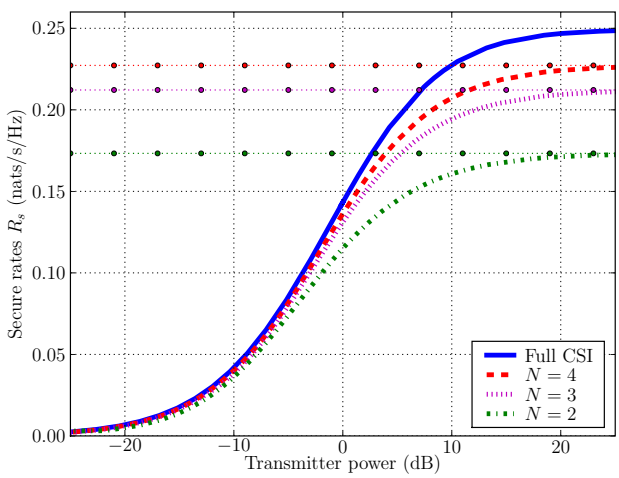

Fig. 2. Impact of quantized CSI on achievable secure rates. Legend indicates the number of intervals N used for uniform quantization. Thin horizontal lines indicate asymptotic values.

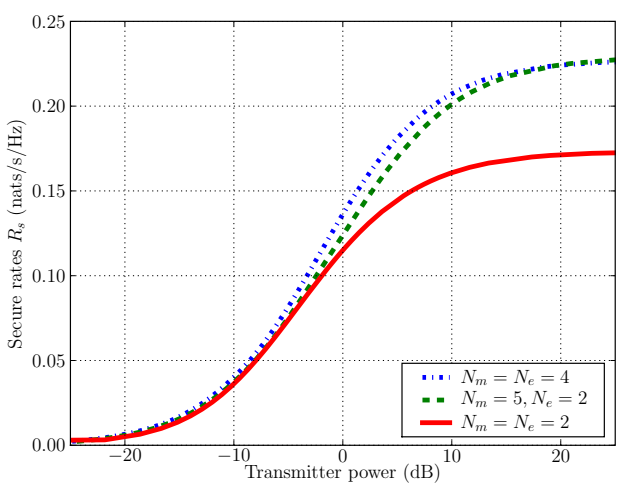

Fig. 3. Impact of asymmetric quantized CSI on achievable secure rates. Legend indicates the number of intervals N_m and N_e used for uniform quantization.

C. Block-ergodic fading

In this section, we consider the fading model used in [7]. We assume that both channel experience *block fading*, where the channel gains $\mathsf{S}_{m,i}$ and $\mathsf{S}_{e,i}$ remain constant over a coherence interval and are independent from one interval to another. Additionally, the duration of each coherence interval is sufficiently long to allow asymptotic coding results to hold. For this mode, we have the following generalization of [7, Theorem 2].

Proposition 2: The following rates R_s are achievable for the block-ergodic fading model.

$$R_s < \max_{\gamma} \mathbb{E}_{\mathsf{S}_m \mathsf{S}_e \mathsf{U}_m \mathsf{U}_e} \left[\left\{ \frac{1}{2} \log \left(\frac{1 + \mathsf{S}_m \gamma(\mathsf{U}_m, \mathsf{U}_e)}{1 + \mathsf{S}_e \gamma(\mathsf{U}_m, \mathsf{U}_e)} \right) \right\}^+ \right], \quad (4)$$

where $\{x\}^+ = \max(x, 0)$.

Sketch of proof: As in the proof of Proposition 1, we consider the new channel defined by (3); however, we use a different random process to evaluate (1). Let us first consider the information density $\frac{1}{km}\mathrm{I}\big(\mathsf{T}^{km}; \mathsf{Y}^{km} | \mathsf{V}_m^{km}\big)$ taken over k coherence intervals of m symbols each. We consider a specific process T_0^{km} such that over each coherence interval $j \in \{1, \ldots, k\}$, $\mathsf{T}_0^{(j)m}$ is a codeword chosen uniformly at random from *independent* codebooks achieving reliable communication. Therefore, we have

$$\frac{1}{km}\mathrm{I}\big(\mathsf{T}_0^{km}; \mathsf{Y}^{km} | \mathsf{V}_m^{km}\big) = \frac{1}{k}\sum_{j=0}^{k} \frac{1}{m}\mathrm{I}\Big(\mathsf{T}^{(j)m}; \mathsf{Y}^{(j)m} | \mathsf{V}_m^{(j)m}\Big)$$

From [10, Theorem 3.2.3], we know that each information density in the sum converges in probability to the rate of the code, which can be arbitrarily close to $\frac{1}{2}\log(1 + \mathsf{h}_m^{(j)})$. Using the ergodicity and stationarity of the block-ergodic fading process, the information density can be shown to converge in probability to

$$\mathbb{E}_{\mathsf{S}_m \mathsf{S}_e \mathsf{U}_m \mathsf{U}_e} \left[\frac{1}{2} \log\left(1 + \mathsf{H}_m\right) \right]. \quad (5)$$

Let us now consider the information density $\frac{1}{km}\mathrm{I}\big(\mathsf{T}_0^{km}; \mathsf{Z}^{km} | \mathsf{V}_e^{km}\big)$. Over each coherence interval, we have

$$\begin{aligned} \frac{1}{m}\mathrm{I}\Big(\mathsf{T}_0^{(j)m}; \mathsf{Z}^m | \mathsf{V}_e^m\Big) &= \frac{1}{m} \log \frac{p\Big(\mathsf{T}_0^{(j)m} | \mathsf{Z}^m\Big)}{p\Big(\mathsf{T}_0^{(j)m}\Big)} \\ &\leq -\frac{1}{m} \log p\Big(\mathsf{T}_0^{(j)m}\Big), \end{aligned}$$

and the last term is simply the rate of the code. Also, over each coherence interval, the information density cannot exceed the capacity of the eavesdropper channel given by $\frac{1}{2}\log(1 + \mathsf{h}_e^{(j)})$. Hence, using the ergodicity and stationarity of the block-fading process, we can show that $\frac{1}{km}\mathrm{I}\big(\mathsf{T}_0^{km}; \mathsf{Z}^{km} | \mathsf{V}_e^{km}\big)$ is upper-bounded by a term that converges in probability to

$$\min\left(\mathbb{E}_{\mathsf{S}_m \mathsf{S}_e \mathsf{U}_m \mathsf{U}_e} \left[\frac{1}{2} \log\left(1 + \mathsf{H}_m\right) \right], \mathbb{E}_{\mathsf{S}_m \mathsf{S}_e \mathsf{U}_m \mathsf{U}_e} \left[\frac{1}{2} \log\left(1 + \mathsf{H}_e\right) \right] \right) \quad (6)$$

Combining (5) and (6), substituting the definition of H_m and H_m, and optimizing over all possible functions γ, we obtain the desired result. ■

Because the expectation to optimize in (4) is always positive, the set of functions γ that yield non-zero rates is larger than for (2). In particular, we see that, even in the absence of CSI about the eavesdropper's channel at the transmitter (U_e^n

independent of S_e^n), the achievable rates are strictly positive if $\mathbb{P}_{S_m S_e}[S_m > S_e] > 0$; therefore, even for situations in which the legitimate receiver's channel has a lower average SNR than the eavesdropper's channel, secure communication at non-zero rates is always possible. We stress that this powerful result is tightly related to the specific type of block fading considered here, and it is doubtful that similar conclusions hold in other situations.

The method used to find the optimal function γ in the previous section (Lemma 1) can be applied directly here; in particular, the same conclusions can be drawn in terms of the impact of CSI precision on secrecy capacity.

V. Conclusion

As an illustration of the usefulness of information-spectrum techniques for information-theoretic security, we have investigated wiretap channels with imperfect CSI. In particular, we have characterized achievable secrecy rates for Gaussian fading channels in the presence of imperfect information about the legitimate receiver's channel and eavesdropper's channel. Although we do not have outer bounds on the secrecy capacity of such channels, our achievable rates match the secrecy capacity in the case of perfect CSI. As expected, our results also confirm the importance of having some information about the eavesdropper's channel. Although this strong requirement may limit the scope of information-theoretic schemes, we emphasize that the precision of CSI available at the transmitter seems less critical. Finally, we point out that our model implicitly assumes the existence of feedback channels that convey channel state information back to the transmitter. It is well known that feedback can increase secrecy capacity [3], [4], and it is not clear whether using these channels to transmit channel state information is necessarily the optimal strategy to maximize secrecy capacity.

Acknowledgment

This research has been supported in part by the NSF CAREER grant CCF05-46618.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, October 1975.

[2] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[4] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[5] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[6] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[7] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[8] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[9] M. Bloch and J. N. Laneman, "On the secrecy capacity of arbitrary wiretap channels," in *Proceedings of 46th Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 2008.

[10] T. S. Han, *Information-Spectrum Methods in Information Theory*. Springer, 2002.

[11] G. Caire and S. Shamai, "On the capacity of some channels with channel state information," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 2007–2019, 1999.

[12] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, April 2006.

[13] C. E. Shannon, "Channels with side information at the transmitter," *IBM Journal of Research and Development*, vol. 2, no. 4, pp. 289–293, October 1958.