Exploiting Partial Channel State Information for Secrecy over Wireless Channels

Matthieu R. Bloch and J. Nicholas Laneman

***Abstract*—In this paper, we investigate the effect of partial channel state information on the achievable secure communication rates and secret-key generation rates over ergodic fading channels. In particular, we establish lower bounds for the strong secrecy capacity and the strong secret-key capacity of ergodic and block-ergodic fading channels with partial Channel State Information at the Transmitter (CSIT). Our analysis sheds light on the usefulness of CSIT to harness the benefits of fading for secrecy and allows us to quantify the penalty incurred by lack of full CSIT. In particular, we illustrate numerically situations in which little CSIT is required to recover most of the benefits of fading and in which the legitimate terminals have an incentive to characterize their channel precisely.**

***Index Terms*—wireless fading channel; channels state information; secrecy capacity; secret-key capacity.**

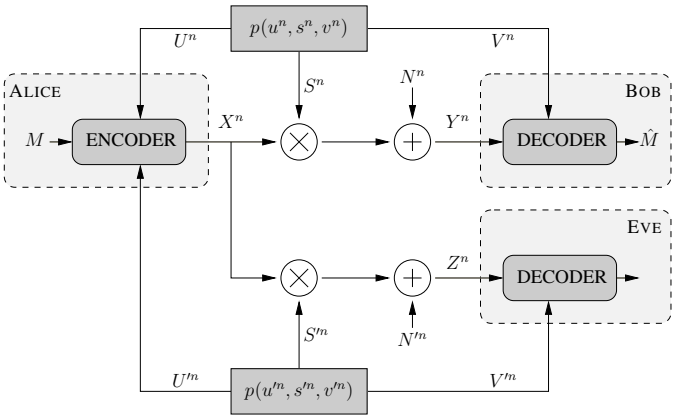

Fig. 1. Communication over a channel with imperfect CSI.

I. Introduction

The goal of achieving information-theoretic secrecy at the physical-layer of wireless channels has attracted much attention in recent years. The generalizations of the wiretap channel model [2] and of the secret-key generation model [3], [4] to various wireless channels [5]–[9] have highlighted the benefits of fading for secrecy and have even guided the design of some experimental systems [10], [11]. However, the ability to harness these benefits often relies on the knowledge of the channel statistics and even of the instantaneous realizations of the fading gains, which has hindered the acceptance of the information-theoretic models as credible cryptographic models. The analysis of models and the design of coding schemes that operate with little if no information about the eavesdropper are still in their early stages, see for instance [12].

In this paper, we do not address the problem of achieving secrecy without any information about eavesdroppers, but rather we study how much Channel State Information (CSI) is required to take advantage of fading. Specifically, we focus on ergodic fading channels with known statistics and we investigate the secure message rates and secret-key rates that can be obtained if there is only partial CSIT. In the extreme cases of perfect CSI and no CSI, the secrecy capacity and secret-key capacity have been studied for Single-Input Single Output (SISO) or Multiple-Input Multiple Output (MIMO) ergodic and block ergodic channels, see for instance [6], [7], [13]–[15]. However, to the best of our knowledge, few works analyze intermediate situations in which partial CSIT is available, for instance via a rate-limited feedback link. For simplicity, we focus in this paper on a SISO ergodic fading channel. The model and results bear some similarities with those of the concurrent work in [16], [17] and we draw similar conclusions regarding the usefulness of CSIT.

Strictly speaking, all the models studied in the remainder of the paper can be viewed as direct extensions of the discrete memoryless wiretap channels with causal CSI [18], [19], for which the secrecy capacity and secret-key capacity are often known; however, these results depend on auxiliary random variables and are not easily evaluated. In this paper, we extend these results by providing numerically computable expressions of achievable secure communication rates and secret-key capacity, which provide insight beyond that of the known single-letter expressions; we also establish strong secrecy rates by leveraging recent results on the secrecy capacity of arbitrary channels [20], [21]. Two of the main conclusions drawn from our analysis is that little CSIT is required to take advantage of fading and that legitimate terminals should try to precisely characterize their communication channel.

The remainder of the paper is organized as follows. Section II sets the notation and introduces the ergodic wireless channel with partial CSIT that we analyze. Section III presents our results for the secrecy capacity and secret-key capacity of the model. Section IV provides a numerical illustration of the results for a specific fading model. Finally, Section V offers some concluding remarks.

II. System Model

We consider the channel model illustrated in Figure 1, in which a legitimate transmitter (Alice) communicates with a legitimate receiver (Bob) in the presence of an eavesdropper (Eve). The channels are independent real-valued fading channels governed by stationary ergodic fading gains S^n and S'^n,

Matthieu R. Bloch is with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, and with the GT-CNRS UMI 2968, Metz, France. J. Nicholas Laneman is with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN. Parts of these results were presented at the 2009 Information Theory and Applications Workshop, San Diego, CA [1].

respectively, and corrupted by independent i.i.d. additive Gaussian noise N^n and N'^n with $N_i \sim \mathcal{N}(0,1)$, $N'_i \sim \mathcal{N}(0,1)$. We consider two models of fading. In the ergodic fading model, the fading gains change from one symbol to the next and the relations between input and outputs are given at each time instant i by

$$Y_i = \sqrt{S_i}X_i + N_i,$$
$$Z_i = \sqrt{S'_i}X_i + N'_i.$$

In the block-ergodic fading model, the fading gains remain constant over coherence intervals of length m, which we assume is large enough for asymptotic coding theorems to apply. The relations between input and outputs are given at each time instant i within coherence interval k by

$$Y_{k,i} = \sqrt{S_k}X_{k,i} + N_{k,i},$$
$$Z_{k,i} = \sqrt{S'_k}X_{k,i} + N'_{k,i}.$$

In the sequel, we often refer to the channel between Alice and Bob as the main channel and to the channel between Alice and Eve as the eavesdropper's channel.

Bob has access to his exact CSI and received Signal-to-Noise Ratio (SNR) $V_i \triangleq (S_i, S_i\mathbb{E}\left[X_i^2|U^i\right])$, while Eve has access to her exact CSI and received SNR $V'_i \triangleq (S'_i, S'_i\mathbb{E}\left[X_i^2|U'^i\right])$. Alice has access to causal CSI about both channels, which we denote by U_i and U'_i, respectively, which are deterministic functions of the CSI S_i and S'_i, respectively. This models, for instance, the situation in which the received SNR is estimated accurately at the receiver while the channel state is available to the transmitter through a rate-limited feedback link. The random variables corresponding to the first order joint distribution of $S_i, S'_i, U_i, U'_i, V_i, V'_i$ are simply denoted by S, S', U, U', V, V'. Finally, the transmitted symbols are subject to a long-term average power constraint $\frac{1}{n}\sum_{i=1}^n \mathbb{E}\left[X_i^2\right] \leqslant P$.

We consider two modes of operation over this channel. In the first mode, the objective is for Alice to transmit a message M reliably and secretly to Bob, in such a way that Eve obtains virtually no information about the message. Specifically, Alice uses a code defined as follows.

Definition 1. *An $(n, 2^{nR})$ code $\mathcal{C}_n$ consists of:*

- *a message set $\mathcal{M}_n \triangleq [\![1, 2^{nR}]\!]$;*
- *a set of stochastic encoding functions $f_i : \mathcal{M}_n \times \mathcal{U}^i \times \mathcal{U}'^i \to \mathcal{X}$ for $i[\![1, n]\!]$ used to transmit codeword symbols corresponding to a message m;*
- *a decoding function $g_n : \mathcal{Y}^n \times \mathcal{V}^n \to \mathcal{M}$ used to form an estimate $\hat{m}$ of the transmitter message.*

The reliability performance of the code is measured in terms of the probability of error $\mathbb{P}_e(\mathcal{C}_n) \triangleq \mathbb{P}\left[\hat{M} \neq M|\mathcal{C}_n\right]$ and the secrecy performance is measured in terms of the variational distance $\mathbb{S}(\mathcal{C}_n) \triangleq \mathbb{V}(p_{Z^nV'^nM}, p_{Z^nV'^n}p_M)$.[1]

A rate R is an achievable secure communication rate if there exists a sequence of $(n, 2^{nR})$ codes $\{\mathcal{C}_n\}$ such that

$$\lim_{n\to\infty} \mathbb{P}_e(\mathcal{C}_n) = \lim_{n\to\infty} \mathbb{S}(\mathcal{C}_n) = 0.$$

The supremum of achievable secure communication rates is the secrecy capacity C_s.

In the second mode, the objective is for Alice and Bob to extract a secret key from the channel randomness. In this case, we assume that there exists a public authenticated side channel of unlimited capacity over which they can communicate. Eve has access to all messages transmitted over this side channel but cannot tamper with them. Formally, a secret-key generation strategy is the following. [2]

Definition 2. *An $(n, 2^{nR})$ secrecy key generation strategy $\mathcal{S}_n$ consists of:*

- *a key set $\mathcal{K}_n \triangleq [\![1, 2^{nR}]\!]$;*
- *a set of encoding functions to create messages sent over the public channel, based on past messages; this messages are collectively denoted by $F \in \mathcal{F}$;*
- *a set of stochastic encoding functions f_i used to transmit symbols over the channel as a function of past messages and past state information;*
- *two decoding functions $f : \mathcal{F} \times \mathcal{X}^n \times \mathcal{U}^n \to \mathcal{K}_n$ and $g : \mathcal{F} \times \mathcal{Y}^n \times \mathcal{V}^n \to \mathcal{K}_n$ to estimate keys k and $\hat{k}$.*

The reliability performance is measured in terms of the probability of error $\mathbb{P}_e(\mathcal{S}_n) \triangleq \mathbb{P}\left[\hat{K} \neq K|\mathcal{S}_n\right]$ and the secrecy performance is measured in terms of the variational distance

$$\mathbb{S}(\mathcal{S}_n) \triangleq \mathbb{V}(p_{Z^nFV'^nK}, p_{Z^nV'^nF}p_K).$$

A rate R is an achievable secret-key rate if there exists a sequence of $(n, 2^{nR})$ strategies $\{\mathcal{S}_n\}$ such that

$$\lim_{n\to\infty} \mathbb{P}_e(\mathcal{S}_n) = \lim_{n\to\infty} \mathbb{S}(\mathcal{S}_n) = 0.$$

The supremum of achievable secure communication rates is the secret-key capacity C_{sk}.

III. Main Results

A. Secrecy Capacity

We first establish achievable secure communication rates for the ergodic model.

Proposition 1. *The strong secrecy capacity of an ergodic wireless channel with partial CSIT can be lower bounded according to*

$$C_s \geqslant \max_{\gamma} \mathbb{E}\left[\frac{1}{2}\log\left(\frac{1+S\gamma(U,U')}{1+S'\gamma(U,U')}\right)\right]$$

where γ is such that $\mathbb{E}[\gamma(U,U')] \leqslant P$.

Proof: Rather than establishing the result from first principles with a random coding argument, we rely on a lemma that establishes an n-letter expression for the the secrecy capacity of arbitrary wiretap channels. The proof is provided in Appendix A.

[1] This measure of secrecy is more stringent than the weak secrecy measure $\frac{1}{n}\mathbb{I}(M; Z^nV^nV'^n)$ [21].

[2] We refer the reader to [3] for a more explicit definition.

Lemma 1. *The strong secrecy capacity of an arbitrary wiretap channel with imperfect state information is*

$$C_s = \max_{\{W^n,T^n\}_{n=0}^{\infty}} \left(\text{p-limsup}_{n\to\infty} \frac{1}{n} I(W^n;Y^n|V^n) - \text{p-liminf}_{n\to\infty} \frac{1}{n} I(W^n;Z^n|V'^n) \right), \tag{1}$$

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

Following [22], we now consider a specific use of the CSI at the transmitter, according to which the transmitted symbol i is scaled by $\sqrt{\gamma(U_i,U_i')}$, where γ is a deterministic time-invariant function such that $\mathbb{E}[\gamma(U,U')] \leqslant P$. Upon denoting by X_i the transmitted symbol at time i, the situation is then as if X_i was transmitted over a new ergodic channel, without CSIT and full CSI at the receivers, characterized by

$$\begin{aligned} Y_i &= \sqrt{H_i} X_i + N_i \\ Z_i &= \sqrt{H_i'} X_i + N_i', \end{aligned} \tag{2}$$

with $H_i = S_i\gamma(U_i,U_i')$, $H_i' = S_i'\gamma(U_i,U_i)$, and subject to a power constraint $\frac{1}{n}\sum_{i=1}^n \mathbb{E}\left[X_i^2\right] \leqslant 1$. The secrecy capacity of the original channel is at least the secrecy capacity of the new one since it corresponds to a specific use of the CSI. We can then obtain an achievable rate for the new channel by substituting an appropriate choice of random processes in Eq. (1). Specifically, we set $W^n = T^n = X^n$, and we choose an i.i.d. process $X_i \sim \mathcal{N}(0,1)$. Substituting this in Eq. (1) we obtain

$$\begin{aligned} \frac{1}{n} I(T^n;Y^n|V^n) &= \frac{1}{n}\sum_{i=1}^n I(X_i;Y_i|V_i) \\ &= \frac{1}{n}\sum_{i=1}^n \frac{1}{2}\left(\log(1+H_i) - |N|_i^2 + \frac{|Y|_i^2}{1+H_i} \right), \end{aligned}$$

where we have used the fact that $Y_i \sim \mathcal{N}(0,1)$ conditioned on X_iV_i and $Y_i \sim \mathcal{N}(0,1+H_i)$ conditioned on V_i. The processes $\{V_i\}$ and $\{Y_i\}$ are stationary and ergodic by construction, so that $\frac{1}{n} I(T^n;Y^n|V^n)$ converges in probability to

$$\mathbb{E}\left[\log(1+H) - |N|^2 + \frac{|Y|^2}{1+H} \right] = \mathbb{E}[\log(1+S\gamma(U,U'))],$$

since $\mathbb{E}\left[|Y|^2/(1+H)\right] = \mathbb{E}\left[|N|^2\right] = 1$. Using similar arguments, we can also show that $\frac{1}{n} I(T^n;Z^n|V'^n)$ converges in probability to $\mathbb{E}[\log(1+S'\gamma(U,U'))]$. Consequently, Lemma 1 guarantees that the rate

$$\mathbb{E}[\log(1+S\gamma(U,U'))] - \mathbb{E}[\log(1+S'\gamma(U,U'))]$$

is an achievable strong secrecy rate. Maximizing over all choices of power allocation functions γ yields the desired result. ∎

Remark 1. *The achievable rate in Proposition 1 holds in the more general case in which the CSIT is a noisy version of the true CSI, and as long as the various CSIs remain jointly ergodic and stationary.*

If the transmitter has perfect CSI about both channels ($U = S$ and $U' = S'$), the lower bound in Proposition 1 coincides with the secrecy capacity. In this case, the optimal power allocation function γ does not depend on the fading statistics and can be derived in closed-form, as was already obtained in [6] with a completely different proof. If the transmitter has no CSI (U independent of S and U' independent of S'), the lower bound is maximized by a constant power allocation γ; whether the lower bound is positive or not then depends on the statistics of the fading and, in particular, it is zero if the fading statistics are identical on both channels.

We now establish achievable secure communication rates for the block-ergodic model.[3]

Proposition 2. *The strong secrecy capacity of a block-ergodic wireless channel can be lower bounded according to*

$$C_s \geqslant \mathbb{E}\left[\left[\mathbb{E}\left[\frac{1}{2}\log\left(\frac{1+S\gamma(U,U')}{1+S'\gamma(U,U')} \right) \middle| UU' \right] \right]^+ \right]$$

where γ *is such that* $\mathbb{E}[\gamma(U)] \leqslant P$ *and* $[x]^+ \triangleq \max(x,0)$*.*

Proof: Consider a fixed power allocation function γ such that $\mathbb{E}[\gamma(U,U')] \leqslant P$. As for the proof of Proposition 1, we construct a new block-ergodic wiretap channel without CSI at the transmitter and full CSI at the receivers Setting $H_i \triangleq S_i\gamma(u,u')$ and $H_i' \triangleq S_i'\gamma(u,u')$, the relations between input and outputs in coherence interval k in which the CSIT is (u,u') are

$$\begin{aligned} Y_{k,i} &= \sqrt{H_i} X_{k,i} + N_{k,i} \\ Z_{k,i} &= \sqrt{H_i'} X_{k,i} + N_{k,i}', \end{aligned} \tag{3}$$

subject to the constraint $\frac{1}{mn}\sum_{i=1}^k \sum_{j=1}^n \mathbb{E}\left[X_{k,i}^2\right] \leqslant 1$. We then note that, because the CSIT U_i is a deterministic function of the fading gains S_i and because the legitimate receiver knows the fading gain and the exact received SNR, it can recover $\gamma(u,u')$ if a constant-power code is used. In this case, Alice and Bob can effectively demultiplex the channel into parallel sub-channels, each characterized by a different value of u,u'. Letting $R_s(u,u')$ denote an achievable secure communication rate for the channel characterized by (u,u'), the stationarity and ergodicity of the fading ensures that

$$C_s \geqslant \iint dudu' p(u,u') R_s(u,u'). \tag{4}$$

We then construct an appropriate process to substitute in Eq. (1) as follows. We set $W^n = T^n = X^n$ and we let $\epsilon > 0$ and $N \in \mathbb{N}^*$. We choose for $\{X_i\}$ a process that consists of i.i.d. codewords C^m of length m stemming from a constant-rate constant-power code for the main channel in Eq. (3). By the channel coding theorem, we know that the code can be chosen with rate $C_B - \epsilon$ and probability of error ϵ, where C_B denotes the capacity of the main channel in Eq. (3). Since the process is memoryless by block, the information density $\frac{1}{n} I(T^n;Y^n|V^n)$ converges in probability

[3] This result corrects an error in the statement of [1, Proposition 2].

to $\frac{1}{m}\mathbb{I}(C^m;Y^m|V^m)$, which is lower bounded as follows.

$$\begin{aligned}\frac{1}{m}\mathbb{I}(C^m;Y^m|V^m) &= \frac{1}{m}\mathbb{H}(C^m) - \frac{1}{N}\mathbb{H}(C^m|Y^mV^m) \\ &\geqslant \frac{1}{m}\mathbb{H}(C^m) - \frac{1}{m} - \epsilon(C_B-\epsilon), \quad (5)\end{aligned}$$

where the last line follows from Fano's inequality. We now turn our attention to the information density $\frac{1}{n}I(T^n;Z^n|V'^n)$. As earlier, it converges in probability to $\frac{1}{m}\mathbb{I}(C^m;Z^m|V'^m)$, which is upper bounded as

$$\frac{1}{m}\mathbb{I}(C^m;Z^m|V'^m) \leqslant C_E \quad (6)$$

where C_E denotes the capacity of the eavesdropper's channel in Eq. (3). In addition, we have

$$\frac{1}{m}\mathbb{I}(C^m;Z^m|V'^m) \leqslant \frac{1}{n}\mathbb{H}(C^n)\,. \quad (7)$$

Combining Eq. (5), Eq. (6), and Eq. (7), we obtain

$$\begin{aligned}&\operatorname*{p-liminf}_{n\to\infty}\frac{1}{n}I(T^n;Y^n|V^n) - \operatorname*{p-limsup}_{n\to\infty}\frac{1}{n}I(T^n;Z^n|V'^n) \\ &\geqslant \frac{1}{m}\mathbb{H}(C^m) - \frac{1}{N} - \epsilon(C_B-\epsilon) - \min(C_E, \frac{1}{m}\mathbb{H}(C^m)) \\ &= \left[\frac{1}{m}\mathbb{H}(C^m) - C_E\right]^+ - \frac{1}{N} - \epsilon(C_B-\epsilon) \\ &\geqslant [C_B - C_E - \epsilon]^+ - \frac{1}{N} - \epsilon(C_B-\epsilon).\end{aligned}$$

Since ϵ and N are arbitrary, we obtain $C_s \geqslant [C_B - C_E]^+$. Finally, note that the capacity of the channels characterized by Eq. (3) is obtained for a constant power allocation, so that

$$\begin{aligned}C_B &= \mathbb{E}\left[\frac{1}{2}\log(1+S\gamma(u,u'))\right] \\ C_E &= \mathbb{E}\left[\frac{1}{2}\log(1+S'\gamma(u,u'))\right]\end{aligned}$$

Going back to Eq. (4), we obtain

$$C_s \geqslant \mathbb{E}\left[\left[\mathbb{E}\left[\frac{1}{2}\log\left(\frac{1+S\gamma(U,U')}{1+S'\gamma(U,U')}\right)\middle|UU'\right]\right]^+\right]$$

■

The lower bound given in Proposition 2 is always larger than that of Proposition 1 because the expectation to optimize is always positive. In addition, as already noted in [7], the achievable rates are positive even in the absence of CSIT about the eavesdropper's channel (U' independent of S') as long as $\mathbb{P}[S > S'] > 0$; 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 possible. We stress that this powerful result is tightly related to the specific nature of the block ergodic fading.

B. Secret-Key Capacity

We now turn our attention to the problem of secret-key generation over the ergodic and block-ergodic models.

Proposition 3. *The strong secret-key capacity of an ergodic wireless channel can be lower bounded according to*

$$C_{sk} \geqslant \max_{\gamma}\mathbb{E}\left[\frac{1}{2}\log\left(\frac{1+S'\gamma(U,U')+S\gamma(U,U')}{1+S'\gamma(U,U')}\right)\right]$$

where γ is such that $\mathbb{E}[\gamma(U)] \leqslant P$.

Proof: We first transform the original channel into a new channel with no CSIT characterized by Eq. (2), as done in the proofs in Proposition 1. For this channel, Alice sends i.i.d. random symbols X_i generated according to $\mathcal{N}(0,1)$. This transforms the channel into a specific source model for key generation [3], in which the components $YV \to X \to ZV'$ form a Markov chain. In this case, the secret-key capacity is known and given by $\mathbb{I}(X;YV|ZV') = \mathbb{I}(X;Y|ZVV')$ since V is independent of X. Hence we have,

$$\begin{aligned}C_{sk} &\geqslant \mathbb{I}(X;Y|ZVV') \\ &= h(Y|ZVV') - h(Y|ZXVV') \\ &= h(YZ|VV') - h(Z|VV') - h(N) \\ &= \mathbb{E}\left[\frac{1}{2}\log\left((2\pi e)^2(1+\gamma(U,U')(S+S'))\right)\right] \\ &\qquad - \mathbb{E}\left[\frac{1}{2}\log\left((2\pi e)(1+\gamma(U,U')S')\right)\right] - \frac{1}{2}\log(2\pi e) \\ &= \mathbb{E}\left[\frac{1}{2}\log\left(\frac{1+S'\gamma(U,U')+S\gamma(U,U')}{1+S'\gamma(U,U')}\right)\right].\end{aligned}$$

Maximizing over γ establishes the lower bound on C_{sk}.

■

Remark 2. *Proposition 3 also holds for block-ergodic channel. Note that having longer coherence intervals does not improve the secret-key capacity.*

IV. Numerical Example

The results established in Section III still depend on an optimization over all possible power allocation functions γ. One can therefore try to perform an optimization to compute the various bounds. Without perfect CSIT, the objective functions given in Proposition 1 and Proposition 2 are not concave functions of the power allocation γ, which means that the Karush-Kuhn-Tucker conditions are only necessary conditions. Nevertheless, the optimization of the lower bound in Proposition 1 can be performed numerically using the following lemma.

Lemma 2. *Define the function $f_{uu'}(\gamma)$ as*

$$f_{uu'}(\gamma) \triangleq \iint \frac{s-s'}{(1+s\gamma(u,u'))(1+s'\gamma(u,u'))}p(s|u)p(s'|u')dsds'.$$

Assuming there exists (u_o,u_0') with $p(u_0,u_0') > 0$ such that $\mathbb{E}[S-S'|u_0,u_0'] > 0$, then $\gamma(u,u')$ defined as

$$\gamma(u,u') \triangleq \begin{cases} f_{uu'}^{-1}(\lambda) & \text{if } 0 \leqslant \lambda \leqslant \mathbb{E}[S-S'|u,u'], \\ 0 & \text{else.}\end{cases}$$

is a power allocation under power constraint

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

Proof: One can check that if there exists (u_o, v_0) with $p(u_0, u_0') > 0$ such that $\mathbb{E}[S - T|u_0, v_0] > 0$, then using the entire power P is optimal. Then, by forming the Lagrangian $\mathcal{L}$ as follows

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

and by using the Karush-Kuhn-Tucker conditions with respect to the function $\gamma(u, v)$, we obtain the desired result. ∎

By varying λ, Lemma 2 provides the optimal power allocation for all power constraints P. Since $\lambda \geqslant 0$, notice that $\gamma(u, v) = 0$ whenever $\mathbb{E}[S|u, v] \leqslant \mathbb{E}[T|u, v]$, 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 lower bound in Proposition 2 can be evaluated with a similar procedure.

The objective function in Proposition 3 is a concave function of the power allocation function γ. Following the same approach as in Lemma 2, one can claim to identify the optimal power allocation function. In the case of perfect CSIT, one can then identify the power allocation in closed form, which does not depend on the channel statistics. We report it here for completeness.

Lemma 3. *Define*

$$g(s,s') \triangleq \frac{1}{2}\left(-\left(\frac{1}{s'}+\frac{1}{s+s'}\right)+\sqrt{\left(\frac{1}{s'}-\frac{1}{s+s'}\right)\left(\frac{4}{\lambda}+\frac{1}{s'}-\right.\right.$$

Then, the power allocation $\gamma(s, s') = g(s, s')\mathbf{1}\{g(s, s') > 0\}$ *is the optimal power allocation for power* $P = \mathbb{E}[\gamma(S, S')]$.

We now illustrate the above results with a numerical example. We consider a channel for which $\{S_i\}_{i\geqslant 1}$ and $\{S_i'\}_{i\geqslant 1}$ are independent i.i.d. processes with S_i and S_i uniformly distributed over $[0, 2]$. Receivers have perfect knowledge of their own instantaneous received SNRs, and U (resp. U') is a uniformly quantized version of S (resp. S') obtained with N_m (resp. N_e) intervals.

Figure 2 illustrates the impact of quantized CSI on achievable secure communication rates when the transmitter has the same precision on the eavesdropper and legitimate receiver CSIT ($N \triangleq N_m = N_e$). As expected, the penalty imposed by quantization vanishes as the precision increases. Interestingly, only one bit of quantization closes most of the gap between no CSIT and full CSIT, 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

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

Based on the expression above, and using the approximation $\sum_{k=1}^{N-1} k\ln k \approx \int_{1/2}^{n-1/2} dx x\ln x$, one can also show that

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

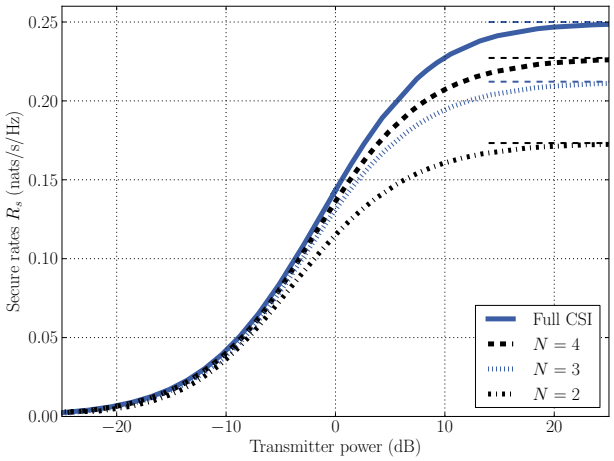

Fig. 2. Impact of quantized CSI on achievable secure communication rates. Legend indicates the number of intervals N used for uniform quantization. Thin horizontal lines indicate asymptotic values.

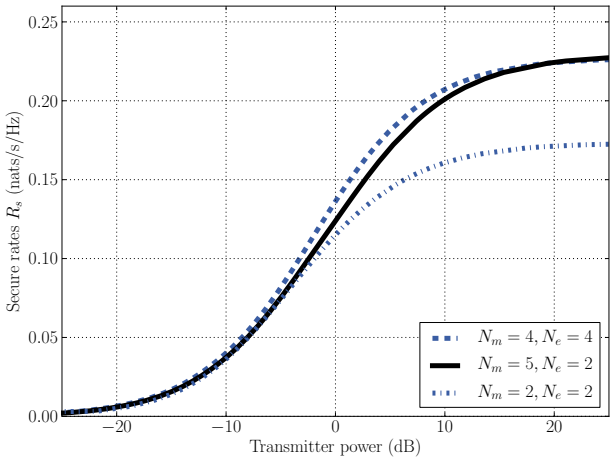

Fig. 3. Impact of asymmetric quantized CSI on achievable secure rates. Legend indicates the number of intervals N_m and N_e used for uniform quantization.

which confirms the observations made form the simulations.

Figure 3 shows the impact of unequal precision for CSI of the legitimate receiver's channel and eavesdropper's channel. Interestingly, the lack of precision on the eavesdropper's CSIT can be somewhat compensated by increasing the precision of the legitimate receiver's CSIT. 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.

Figure 4 illustrates the impact of quantized CSI on the achievable secret-key rates. Quantized CSI inflicts a negligible penalty across the entire range of SNRs and, in particular, achieves the full CSI performance in the high-SNR regime.

V. Conclusion

Our analysis of the secrecy of wireless channels with partial CSIT shows that little CSIT is needed to take advantage of the fading of ergodic wireless channels. Our simulations show that, in the case of secure communication, partial CSIT inflicts

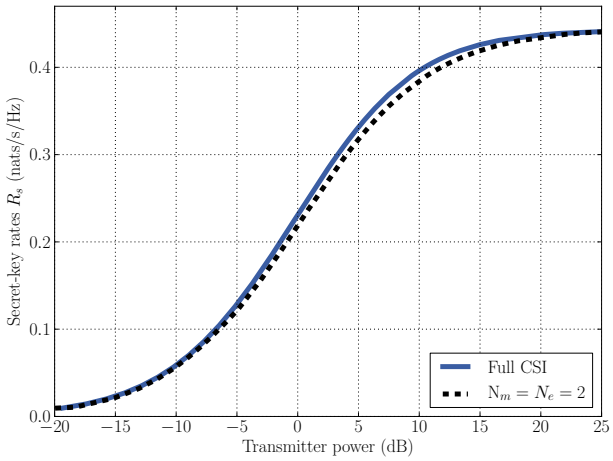

Fig. 4. Impact of quantized CSI on achievable secret-key rates rates. Legend indicates the number of intervals N used for uniform quantization.

a penalty across the whole SNR range; in contrast, in the case of secret-key generation, the penalty incurred by partial CSIT disappears in the high SNR regime.

Interestingly, our results suggest that the legitimate terminals should try to characterize their own channel precisely. A good precision on the CSIT for the main channel allows the transmitter to better identify the fading realizations that are detrimental for secrecy, which in turn translates into higher secrecy rates.

An important aspect that we have not addressed is the "cost" of CSI. Our model considers that CSI is obtained for free whereas in reality this may come at the expense of resources, such as bandwidth for a reverse link. The analysis of the trade-off between channel estimation and communication will be the subject of future investigations.

Appendix A
Proof of Lemma 1

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 $T_i \in \mathcal{X}^{|\mathcal{U}_m|^i \times |\mathcal{U}_e|^i}$ and whose output are the pairs $(Y_i, V_{m,i})$ and $(Y_i, V_{e,i})$. A code $\mathcal{C}$ for the new channel is a set

$$\mathcal{C} = \{t^n(m) = (t_1(m), \dots, t_n(m)) : m \in \mathcal{M}, \\ t_i(m) \in \mathcal{X}^{|\mathcal{U}_m|^i \times |\mathcal{U}_e|^i}\},$$

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

$$p(y^n, z^n, v_m^n, v_e^n | t^n) = \sum_{s_m^n, s_e^n, u_m^n, u_e^n} p(y^n, z^n | t^n(u_m^n, u_e^n), s_m^n, s_e^n) p(u_m^n, u_e^n, v_m^n, v_e^n, s_m^n, s_e^n)$$

This new channel is strictly equivalent to the original one it terms of capacity. We also know that the secrecy capacity of an arbitrary wiretap channel is The secrecy capacity of a wiretap channel $\left(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \left\{p_{Y^n Z^n | X^n}(y^n, z^n | x^n)\right\}_{n=1}^{\infty}\right)$ is

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

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

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

Specializing this information-spectrum formula to the equivalent channel yields the desired result. The proof can be extended to continuous alphabets $\mathcal{U}_m$ and $\mathcal{U}_e$ using discrete approximations.

References

[1] M. Bloch and J. N. Laneman, "Information-spectrum methods for information-theoretic security," in *Proc. Information Theory and Applications Workshop*, San Diego, CA, February 2009, pp. 23–28, (invited).

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

[3] 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.

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

[5] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, September 2007.

[6] 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, 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, October 2008.

[8] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[9] 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.

[10] H. Imai, K. Kobara, and K. Morozov, "On the possibility of key agreement using variable directional antenna," in *Proc. of 1st Joint Workshop on Information Security*, Sookmyung Women's University, Korea, 2006, pp. 153–157.

[11] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[12] X. He and A. Yener, "Providing secrecy when the eavesdropper channel is arbitrarily varying: A case for multiple antennas," in *Proc. 48th Annual Allerton Conf. Communication, Control, and Computing (Allerton)*, 2010, pp. 1228–1235.

[13] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The misome wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[14] T. F. Wong, M. Bloch, and J. M. Shea, "Secret Sharing over Fast-Fading MIMO Wiretap Channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 506 973/1–17, 2009.

[15] A. Agrawal, Z. Rezki, A. J. Khisti, and M. Alouini, "Noncoherent capacity of secret-key agreement with public discussion," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 565–574, 2011.

[16] Z. Rezki, A. Khisti, and M. Alouini, "On the ergodic secrecy capacity of the wiretap channel under imperfect main channel estimation," in *Proc. Conf Signals, Systems and Computers (ASILOMAR) Record of the Forty Fifth Asilomar Conf*, 2011, pp. 952–957.

[17] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the ergodic secret message capacity of the wiretap channel with finite-rate feedback," in *Proc. (ISIT) Symp. IEEE Int Information Theory*, 2012, pp. 239–243.

[18] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key agreement with channel state information at the transmitter," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 672–681, 2011.

[19] Y.-K. Chia and A. El Gamal, "Wiretap channel with causal state information," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2838–2849, 2012.

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

[21] 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, pp. 818–825.

[22] 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.