On Secrecy Capacity of Fast Fading Multiple Input Wiretap Channels with Statistical CSIT

Shih-Chun Lin *Member, IEEE* and Pin-Hsun Lin *Member, IEEE*

Abstract

We consider the secure transmission in ergodic fast Rayleigh fading multiple-input single-output single-antenna-eavesdropper (MISOSE) wiretap channels. We assume that the statistics of both the legitimate and eavesdropper channels are the only available channel state information at the transmitter (CSIT). By introducing a new secrecy capacity upper bound, we prove that the secrecy capacity is achieved by the Gaussian input without prefixing. To attain this result, we form another MISOSE channel for upper-bounding by relaxing the equivocation constraint, and tighten the bound by carefully selecting correlations between the legitimate and eavesdropper channel gains. The resulting upper bound is tighter than the others in the literature which are based on modifying the correlation between the noises at the legitimate receiver and eavesdropper. Next, we fully characterize the secrecy capacity by showing that the optimal channel input covariance matrix is a scaled identity matrix. The key to solve such a stochastic optimization problem is by exploiting the completely monotone property of the secrecy capacity. Finally, we prove that with only statistical CSIT of both channels, the capacity will neither scale with SNR nor the number of antenna. Our numerical results also match these observations and further confirm that having the legitimate CSIT (realizations) is very beneficial to increase the secrecy capacity.

I. Introduction

Traditionally, the security of data transmission has been ensured by the key-based enciphering. However, for secure communications in wireless networks, the key distributions and

Manuscript received Mar. 2012; revised Jun. and Aug. 2012; accepted Nov.26, 2012. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. K.C. Teh.

S.-C. Lin is with the Department of Electronic and Computer Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan, 10607 (e-mail: sclin@mail.ntust.edu.tw), P.-H. Lin is with the Smart Wireless Laboratory, Wireless Network Research Institute, National Institute of Information and Communications Technology (NICT), Yokosuka Kanagawa, Japan 239-0847, (e-mail: pslin@nict.go.jp)

This work was supported by the National Science Council, Taiwan, R.O.C., under Grants NSC 101-2221-E-027-085-MY3 and 100-2628-E-007-025-MY3.

managements may be challenging tasks [1]. The physical-layer security introduced in [2] [3] is appealing due to its keyless nature. One of the fundamental problems for physical-layer security is characterizing the secrecy capacity for wiretap channels. The secrecy capacity is the maximum achievable secrecy rate between a transmitter and a legitimate receiver, with a perfect secrecy constraint imposed to make no information be available by an eavesdropper [2] [3]. In the wireless environments where each node has single antenna, the time-varying characteristics of fading channels can also be exploited to enhance the secrecy capacity [4] [5]. Further enhancements are attainable by employing multiple antennas at each node, e.g., in [6] [7] [8]. However, to show the secrecy capacity results as in [4], [6]–[8], at least the perfect knowledge of the legitimate receiver's channel state information at the transmitter (CSIT) is required. Because of the limited feedback bandwidth and the delay caused by the channel estimation, it may be hard to track the channel coefficients if they vary rapidly. Thus for fast-fading channels, it is more practical to consider the case with only partial CSIT of the legitimate channel [5] [9] [10]. In this case, when the transmitter has multiple antennas, only some lower and upper bounds of the secrecy capacity are known [9] [10], while the secrecy capacity is unknown. Although the general secrecy capacity formula was shown in [2], the optimal selection of the auxiliary random variable for prefixing in this formula is *still unknown*.

In this correspondence, we consider one important scenario of partial CSIT, i.e., the transmitter only knows the statistics of both the legitimate and eavesdropper channels but not the realizations of them. Under this scenario, we derive the secrecy capacity of the ergodic fast-fading, multiple-input single-output single-antenna-eavesdropper (MISOSE) wiretap channels, where the transmitter has multiple antennas while the legitimate receiver and eavesdropper each has a single antenna. Both the coefficients of the legitimate and eavesdropper channels are Rayleigh fading. We first propose a new secrecy capacity upper bound, which is tighter than that in [10], to prove that the transmission scheme in [9] is secrecy-capacity achieving, which is based on [2] with Gaussian input but *without prefixing*. Then we *analytically* solve the optimal channel input covariance matrix to fully characterize the secrecy capacity, while such an optimization problem was solved *numerically* in [9] without guaranteeing the optimality. To attain it, we first transform the secrecy capacity in an equivalent form to exploit the completely monotone property [11] of it. With this property, we then use the majorization theory [12] and the stochastic ordering theory [11] to solve this complicated stochastic covariance matrix optimization problem. More detailed

comparisons between our results and those in [4], [5], [8]–[10] can be found in discussions in Section III.

II. System Model

In the considered MISOSE wiretap channel, as shown in Figure 1, we study the problem of reliably communicating a secret message w from the transmitter to the legitimate receiver subject to a constraint on the information attainable by the eavesdropper (in upcoming (4)). The received signals y and z at the legitimate receiver and eavesdropper (each with a single antenna) from the transmitter (with multiple antennas), can be represented respectively as *

$$y = \mathbf{h}^H \mathbf{x} + n_y, \tag{1}$$

$$z = \mathbf{g}^H \mathbf{x} + n_z, \tag{2}$$

where $\mathbf{x}$ is an $N_T \times 1$ complex vector representing the transmitted vector signal with N_T being the number of transmit antennas, while n_y and n_z are independent and identically distributed (i.i.d.) circularly symmetric additive white Gaussian noise with zero mean and unit variance at the legitimate receiver and eavesdropper, respectively. In (1) and (2), $\mathbf{h}$ and $\mathbf{g}$ are both $N_T \times 1$ complex vectors, and represent the channels from the transmitter to the legitimate receiver and eavesdropper, respectively.

In this work, the channels are assumed to be fast Rayleigh fading, i.e.,

$$\mathbf{h} \sim CN(0, \sigma_{\mathbf{h}}^2 \mathbf{I}) \text{ and } \mathbf{g} \sim CN(0, \sigma_{\mathbf{g}}^2 \mathbf{I}),$$

respectively, while the channel coefficients change in each symbol time. We assume that $\mathbf{h}$, $\mathbf{g}$, n_y and n_z are independent. We also assume that the legitimate receiver knows the instantaneous channel state information of $\mathbf{h}$ perfectly, while the eavesdropper knows those of $\mathbf{h}$ and $\mathbf{g}$ perfectly. As for the CSIT, only the distributions of $\mathbf{h}$ and $\mathbf{g}$ are known at the transmitter, while the realizations of $\mathbf{h}$ and $\mathbf{g}$ are unknown. In addition, the transmitter is subjected to a power constraint

*In this correspondence, $\|\mathbf{a}\|$ is the vector norm of vector $\mathbf{a}$. The trace and complex conjugate transpose of matrix $\mathbf{A}$ is denoted by $\mathrm{Tr}(\mathbf{A})$ and $\mathbf{A}^{\mathrm{H}}$, respectively. Also $\mathrm{diag}(\mathbf{a})$ denotes the diagonal matrix formed by vector $\mathbf{a}$ and $\mathbf{I}$ is the identity matrix. The zero-mean complex Gaussian random vector with covariance matrix $\mathbf{\Sigma}$ is denoted as $CN(0,\Sigma)$. For random variables (vectors) A and B, $p(A)$ is the probability distribution function (p.d.f.) of A, $I(A;B)$ denotes the mutual information between A and B while $h(A|B)$ denotes the conditional differential entropy. We use $A \to B \to C$ to represent that A, B, and C form a Markov chain. All the logarithm operations are of base 2 such that the unit of rates is in bit.

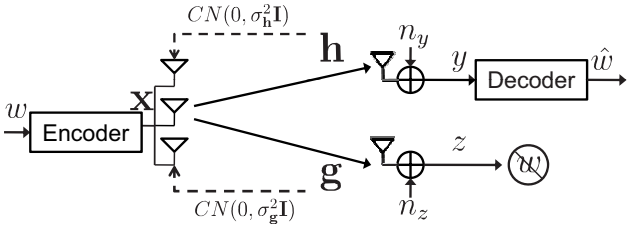

Fig. 1. Fast Rayleigh fading MISOSE wiretap channel with statistical CSIT.

as

$$\mathrm{Tr}(\Sigma_{\mathbf{x}}) \leq P, \tag{3}$$

where $\Sigma_{\mathbf{x}}$ is the covariance matrix of $\mathbf{x}$ in (1) and (2).

The perfect secrecy and secrecy capacity are defined as follows. Consider a $(2^{NR},N)$-code with an encoder that maps the message $w \in \mathcal{W}_N = \{1,2,\ldots,2^{NR}\}$ into a length-N codeword, and a decoder at the legitimate receiver that maps the received sequence y^N (the collections of y over the code length N) from the legitimate channel (1) to an estimated message $\hat{w} \in \mathcal{W}_N$. We then have the following definitions. As [1] [3] [4], the equivocation under perfect secrecy requirement is measured by $I(w;z^N,\mathbf{h}^N,\mathbf{g}^N)/N$, which is based on all the information $(z^N,\mathbf{h}^N,\mathbf{g}^N)$ that the eavesdropper can obtain. Here z^N, $\mathbf{h}^N$, and $\mathbf{g}^N$ are the collections of z, $\mathbf{h}$, and $\mathbf{g}$ over the code length N, respectively.

Definition 1 (Secrecy Capacity [1] [3] [4]) *Perfect secrecy is achievable with rate R if, for any* $\varepsilon > 0$*, there exists a sequence of* $(2^{NR},N)$*-codes and an integer* N_0 *such that for any* $N > N_0$

$$\begin{aligned} R_e = h(w|z^N,\mathbf{h}^N,\mathbf{g}^N)/N \geq R-\varepsilon, \\ \text{and} \quad \Pr(\hat{w} \neq w) \leq \varepsilon, \end{aligned} \tag{4}$$

where R_e *in* (4) *is the equivocation rate and w is the secret message. The* **secrecy capacity** C_s *is the supremum of all achievable secrecy rates.*

III. Secrecy capacity of the MISOSE fast Rayleigh fading wiretap channel

In this section, we fully characterize the secrecy capacity of the MISOSE fast Rayleigh fading channel in the upcoming Theorem 1. Before that, we present the following Lemma 1 which shows

that transmitting Gaussian $\mathbf{x}$ without prefixing as [9] is capacity achieving. By introducing new bounding techniques, we obtain a tighter secrecy capacity upper bound than that in [10] to attain the secrecy capacity. To derive the upper bound, we form a degraded MISOSE channel of (1)(2) with a equivocation constraint less stringent than (4) by hiding the legitimate channel to the eavesdropper (in the upcoming (6)), and tighten the upper bound by carefully introducing correlations to the channels $\mathbf{h}$ and $\mathbf{g}$ (in the upcoming (8)).

Lemma 1 *For the MISOSE fast Rayleigh fading wiretap channel* (1)(2) *with the statistical CSIT of* $\mathbf{h}$ *and* $\mathbf{g}$*, using Gaussian* $\mathbf{x}$ *without prefixing is the optimal transmission strategy, and the non-zero secrecy capacity* C_s *is obtained only when* $\sigma_{\mathbf{h}} > \sigma_{\mathbf{g}}$*, which is*

$$C_s = \max_{\Sigma_{\mathbf{x}}} \left(\mathbb{E}_{\mathbf{h}} \left[\log \left(1 + \mathbf{h}^H \Sigma_{\mathbf{x}} \mathbf{h} \right) \right] - \mathbb{E}_{\mathbf{g}} \left[\log \left(1 + \mathbf{g}^H \Sigma_{\mathbf{x}} \mathbf{g} \right) \right] \right), \tag{5}$$

where $\Sigma_{\mathbf{x}}$ *is the covariance matrix of the Gaussian channel input* $\mathbf{x}$ *subject to* (3)*, while* $\mathbf{h} \sim CN(0, \sigma_{\mathbf{h}}^2 \mathbf{I})$ *and* $\mathbf{g} \sim CN(0, \sigma_{\mathbf{g}}^2 \mathbf{I})$.

Proof: From [9], we know that the right-hand-side (RHS) of (5) is achievable and serves as a secrecy capacity lower-bound. Now we present our new secrecy capacity upper bound which matches the RHS of (5). The key to establish such an upper bound is to form a better MISOSE channel than (1)(2) in terms of having higher secrecy capacity. First, we consider a better channel where the eavesdropper does not know the realizations of $\mathbf{h}$, and the equivocation constraint (4) becomes

$$R_e = h(w|z^N, \mathbf{g}^N)/N \geq R - \varepsilon. \tag{6}$$

Note that since $h(w|z^N, \mathbf{g}^N) \geq h(w|z^N, \mathbf{h}^N, \mathbf{g}^N)$ [13], we know that the MISOSE under equivocation constraint (6) will have higher secrecy capacity compared with the MISOSE under original constraint (4). Now as in [14], equivalently, we can respectively treat the output of the legitimate channel as $(y, \mathbf{h})$ while that of the eavesdropper channel as $(z, \mathbf{g})$. From [1, Lemma 2.1], the secrecy capacity under constraint (6) is only related to the marginal distributions $p(y, \mathbf{h}|\mathbf{x})$ and $p(z, \mathbf{g}|\mathbf{x})$. Then two MISOSE channels have the same secrecy capacity under constraint (6) if the two legitimate channels have the same transition p.d.f. $p(y', \mathbf{h}'|\mathbf{x}) = p(y, \mathbf{h}|\mathbf{x})$ while the two eavesdropper channels are identical.

Here we introduce our same marginal legitimate channel $p(y',\mathbf{h}'|\mathbf{x})$ for (1), which is formed by replacing $\mathbf{h}$ in y with $\mathbf{h}' = (\sigma_{\mathbf{h}}/\sigma_{\mathbf{g}})\mathbf{g}$ as

$$\begin{aligned} y' &= (\mathbf{h}')^H\mathbf{x} + n_y \\ &= (\sigma_{\mathbf{h}}/\sigma_{\mathbf{g}})\mathbf{g}^H\mathbf{x} + n_y. \end{aligned} \tag{7}$$

Since $\mathbf{x}$ is independent of $\mathbf{h}$ and $\mathbf{g}$ due to our CSIT assumption, both $\mathbf{h}'$ and $\mathbf{h}$ have the same conditional distributions condition on $\mathbf{x}$ (which equals to $CN(0,\sigma_{\mathbf{h}}^2\mathbf{I})$). Then we know that $p(y',\mathbf{h}'|\mathbf{x})$=$p(y,\mathbf{h}|\mathbf{x})$. From (7), we will focus on the following MISOSE channel under the equivocation constraint (6)

$$\begin{aligned} y'' &= \mathbf{g}^H\mathbf{x} + (\sigma_{\mathbf{g}}/\sigma_{\mathbf{h}})n_y, \\ z &= \mathbf{g}^H\mathbf{x} + n_z. \end{aligned} \tag{8}$$

Again from [1, Lemma 2.1], the secrecy capacity C_s'' of the above degraded MISOSE channel is equal to that of the original channel (1)(2) under equivocation constraint (6) with $\mathbf{h}$ hidden from the eavesdropper. And thus C_s'' serves as an upper-bound of the secrecy capacity C_s of the original channel (1)(2) under equivocation constraint (4), where $\mathbf{h}$ is revealed to the eavesdropper.

Now we can upper-bound the secrecy capacity C_s by C_s'' as follows. As in [15], we treat $(y'',\mathbf{g})$ and $(z,\mathbf{g})$ respectively as the outputs of the legitimate and the eavesdropper channels in (8), and by applying the results in [2],

$$C_s \le C_s'' = \max_{p_{(U,\mathbf{x})}} I(U;y'',\mathbf{g}) - I(U;z,\mathbf{g}), \tag{9}$$

where U in (9) is an auxiliary random variable for prefixing, which forms the Markov chain $U \to \mathbf{x} \to (y'',z,\mathbf{g})$. When $\sigma_{\mathbf{g}} < \sigma_{\mathbf{h}}$, the MISOSE channel (8) given $\mathbf{g}$ is degraded [13], i.e., $\mathbf{x} \to y'' \to z$. Thus from [7], we can rewrite the RHS of (9) as

$$\begin{aligned} C_s &\le \max_{p_{\mathbf{x}}} I(\mathbf{x};y''|z,\mathbf{g}) \\ &= \max_{p_{\mathbf{x}}} I(\mathbf{x};y''|\mathbf{g}) - I(\mathbf{x};z|\mathbf{g}). \end{aligned} \tag{10}$$

Note that the covariance matrix of $\mathbf{x}$ does not change with the realization of $\mathbf{g}$. Then from [6], we know that Gaussian $\mathbf{x}$ is optimal for the upper bound in (10). After substituting Gaussian $\mathbf{x}$

with covariance matrix $\Sigma_{\mathbf{x}}$ into the upper bound (10), we can find that it matches the RHS of (5) when $\sigma_{\mathbf{g}} < \sigma_{\mathbf{h}}$. Note that when $\sigma_{\mathbf{g}} < \sigma_{\mathbf{h}}$, the RHS of (5) is positive. In contrast, when $\sigma_{\mathbf{g}} \geq \sigma_{\mathbf{h}}$, the upper bound in (9) is zero from [7] and the fact that $\mathbf{x} \to z \to y''$ given $\mathbf{g}$ according to (8). And it concludes the proof. ■

Remark 1: Note that if we directly consider the original setting in Definition 1, where $\mathbf{h}$ is revealed to the eavesdropper, then the equivocation constraint corresponding to (7) will become

$$R_e = h(w|z^N, (\mathbf{h}')^N, \mathbf{g}^N)/N \geq R - \varepsilon, \tag{11}$$

and [1, Lemma 2.1] may not be applied. To see this, from the proof of [1, Lemma 2.1], two channels have the same secrecy capacities if both the equivocation rates and error probabilities are the same given that both channels using the same codebooks and encoding schemes. Thus, one may need to show that R_e in (11) and (4) are the same. From the proof of [1, Lemma 2.1], $h(w|z^N, \mathbf{h}'^N, \mathbf{g}^N)$ in (11) depends on conditional probability $p(z^N, (\mathbf{h}')^N, \mathbf{g}^N|\mathbf{x}^N)$ while $h(w|z^N, \mathbf{h}^N, \mathbf{g}^N)$ in (4) depends on $p(z^N, \mathbf{h}^N, \mathbf{g}^N|\mathbf{x}^N)$. Since $\mathbf{g}$ and $\mathbf{h}' = (\sigma_h/\sigma_g)\mathbf{g}$ are correlated given $\mathbf{x}$, but $\mathbf{g}$ and $\mathbf{h}$ are independent,

$$p(z^N, (\mathbf{h}')^N, \mathbf{g}^N|\mathbf{x}^N) \neq p(z^N, \mathbf{h}^N, \mathbf{g}^N|\mathbf{x}^N).$$

Thus the equivocation rates R_e of the two channels in (11) and (4) may not be the same. We avoid this problem by hiding $\mathbf{h}$ from the eavesdropper. In this case, the equivocation constraints of the original channel (1) and that corresponding to (7) are the same as (6). Then [1, Lemma 2.1] can be used, and the following derivations based on (7) under secrecy constraint (6) can serve as the secrecy capacity upper bound for C_s.

Our proof of Lemma 1 also shows that for the considered MISOSE channel, revealing $\mathbf{h}$ or not to the eavesdropper in this channel does not change the secrecy capacity. Moreover, besides C_s, we also prove the secrecy capacity when $\mathbf{h}$ is not revealed to the eavesdropper. This by-product is also useful to study the more general two-user broadcast channel with confidential messages, where the wiretap channel can be treated as a special case of when only one user transmits in this broadcast channel.

Remark 2: We briefly compare our secrecy capacity results for fast fading channels with those for two different slow fading channels in [16] and [4], respectively. First, our secrecy capacity in Lemma 1 can be *non-zero*. On the contrary, in the setting of the Rayleigh slow fading channel with statistical CSIT in [16], the secrecy capacity *is zero*. This is because that in [16], the channel coefficients do not change within the code length N, and the secrecy capacity is limited by the worst case scenario [1, Section 3.3]. Note that the case that the eavesdropper channel is better than the legitimate channel always exists (i.e., eavesdropper channel can support higher rates than the legitimate channel). This worst case forces the secrecy capacity to be zero, since for any non-zero rate, the perfect secrecy constraint may be violated. And unlike our setting in Definition 1, it may be better to allow the secrecy outage event as in [16]. As for our fast fading setting, the perfect secrecy constraint is always satisfied for all $N > N_0$, and the non-zero secrecy capacity (5) can be achievable. Note that we prove that the additional channel prefixing in [2] is not necessary, i.e., $U \equiv \mathbf{x}$ in (9) of Lemma 1 is sufficient, and then the secrecy capacity in (5) can be treated as the difference of the supportable rates of the legitimate and eavesdropper channels. For the *ergodic* slow fading setting in [4], in contrast to [16], coding over many *different* slow fading blocks (each block has many symbols) must be allowed to obtain the non-zero secrecy capacity. However, in our setting, coding over multiple fast-fading channel states (symbols) is sufficient. The coding latency in [4] is much longer than ours, and may *not* be practical.

Remark 3: The secrecy capacity in [10] is wrong, since the secrecy capacity lower bound in [10] is not achievable for the MISOSE channel (1)(2). There are two reasons. First, the lower bound in [10] is based on the variable-rate coding in [4], where the full CSIT of the legitimate channel $\mathbf{h}$ must be used to vary the transmission rate in each slow fading channel state. This can not be done with only statistical CSIT of $\mathbf{h}$ as in our setting. Second, the variable-rate coding in [4] only works in the ergodic slow fading wiretap channel but not in the fast fading channel. On the contrary, our lower bound in (5) (equals to the secrecy capacity) is based on the results in [9] and is achievable in the fast fading MISOSE channel (1)(2).

For the secrecy capacity upper bound in [10], it is based on a channel where a correlation is introduced to n_y and n_z in (1) and (2). And the derivations of [10] follow directly from those in [4]. In contrast to [4] [10], our upper bound (9) is based on the channel (8) which can be treated by introducing a correlation between $\mathbf{h}$ and $\mathbf{g}$ in (1)(2). Our results show that when $\mathbf{h} = (\sigma_{\mathbf{h}}/\sigma_{\mathbf{g}})\mathbf{g}$,

the resulted upper bound in (9) matches the lower bound in (5), and thus is tighter than the upper bound in [10]. Although one may also introduce a correlation to n_y and n_z in (8), our results indicate that this will not further tighten the bound (9). As a final note, our upper-bounding technique can not be applied when the transmitter additionally knows the realizations of $\mathbf{h}$ as [4]. In such a setting, the legitimate channel (7) is not a same marginal channel for (1). With perfect CSIT of $\mathbf{h}$, the transmitted signal $\mathbf{x}$ is a function of $\mathbf{h}$. Given $\mathbf{x}$, $\mathbf{h}$ may not be Gaussian but $\mathbf{h}' = (\sigma_{\mathbf{h}}/\sigma_{\mathbf{g}})\mathbf{g}$ is, and thus $p(y', \mathbf{h}'|\mathbf{x})$ from (7) may not equal to $p(y, \mathbf{h}|\mathbf{x})$ from (1). Our CSIT assumption makes $\mathbf{x}$ independent of $\mathbf{h}$ and $\mathbf{g}$, and then the legitimate channel in (7) has the same marginal as that in (1). Therefore, we can get rids of the unrealistic ergodic *slow fading* assumption in [4], and be able to find the secrecy capacity of the *fast fading* channel.

For fast fading channels with multiple transmit antennas and perfect legitimate receiver's CSIT, the upper and lower bounds were presented in [8]. The upper bound in [8] follows from [4] as described above, while the lower bound uses the artificial-noise (AN) prefixing [17] which utilizes the legitimate channel's direction to transmit the additional AN to disrupt the eavesdropper's reception. In contrast to our secrecy capacity results, the upper and lower bounds for fast fading channels in [8] only coincide asymptotically when the number of transmit antenna N_T and the transmit signal-to-noise ratio (SNR) are both large. It is also interesting to consider a multi-antenna system with estimated CSIT which includes our results and those in [8] as special cases. Partial results were reported in [5]. In [5], the secrecy capacity is only found under the assumptions that the transmitter has single antenna ($N_T = 1$), $\sigma_{\mathbf{h}}^2 = \sigma_{\mathbf{g}}^2$, and the statistical CSIT is known. This setting in [5] is included in our more general MISOSE modal. Also as discussed in Remark 1, our proof for Lemma 1 includes a step which hides $\mathbf{h}$ from the eavesdropper. However, this proof step is neglected in [5].

Now we show that the optimal $\Sigma_{\mathbf{x}}$ of the stochastic optimization problem (5) is

$$\text{diag}\{P/N_T, \ldots, P/N_T\},$$

and fully characterize the secrecy capacity as follows. Note that such optimization problem does not exist for the single transmit antenna system considered in [5].

Theorem 1 *For the MISOSE fast Rayleigh fading wiretap channel* (1)(2) *with the statistical*

CSIT of $\mathbf{h}$ *and* $\mathbf{g}$*, under power constraint* P*, the non-zero secrecy capacity* C_s *is obtained only when* $\sigma_{\mathbf{h}} > \sigma_{\mathbf{g}}$*, which is*

$$C_s = \mathbb{E}_{\mathbf{h}}\left[\log\left(1+P\frac{||\mathbf{h}||^2}{N_T}\right)\right] - \mathbb{E}_{\mathbf{g}}\left[\log\left(1+P\frac{||\mathbf{g}||^2}{N_T}\right)\right], \tag{12}$$

where $\mathbf{h} \sim CN(0,\sigma_{\mathbf{h}}^2\mathbf{I})$*,* $\mathbf{g} \sim CN(0,\sigma_{\mathbf{g}}^2\mathbf{I})$*, and* N_T *is the number of transmit antennas.*

Proof: Subjecting to (3), after substituting $\mathbf{h} \sim CN(0,\sigma_{\mathbf{h}}^2\mathbf{I})$ and $\mathbf{g} \sim CN(0,\sigma_{\mathbf{g}}^2\mathbf{I})$ into the RHS of (5), the optimization problem becomes

$$\max_{\Sigma_{\mathbf{x}}}\left(\mathbb{E}_{\mathbf{g}}\left[\log\frac{\sigma_{\mathbf{g}}^2/\sigma_{\mathbf{h}}^2+\mathbf{g}^H\Sigma_{\mathbf{x}}\mathbf{g}}{\sigma_{\mathbf{g}}^2/\sigma_{\mathbf{h}}^2}\right] - \mathbb{E}_{\mathbf{g}}\left[\log(1+\mathbf{g}^H\Sigma_{\mathbf{x}}\mathbf{g})\right]\right). \tag{13}$$

By using the eigenvalue decomposition $\Sigma_{\mathbf{x}} = \mathbf{U}\mathbf{D}\mathbf{U}^H$, where $\mathbf{U}$ is unitary and $\mathbf{D}$ is diagonal, finding the optimal $\Sigma_{\mathbf{x}}$ of (13) is equivalent to solving

$$\begin{aligned}
&\max_{\mathbf{U},\mathbf{D}}\Big(\mathbb{E}_{\mathbf{g}}\left[\log\left(\sigma_{\mathbf{g}}^2/\sigma_{\mathbf{h}}^2+\mathbf{g}^H\mathbf{U}\mathbf{D}\mathbf{U}^H\mathbf{g}\right)\right] \\
&\qquad - \mathbb{E}_{\mathbf{g}}\left[\log(1+\mathbf{g}^H\mathbf{U}\mathbf{D}\mathbf{U}^H\mathbf{g})\right]\Big), \\
=&\max_{\mathbf{D}}\Big(\mathbb{E}_{\mathbf{g}}\left[\log\left(\sigma_{\mathbf{g}}^2/\sigma_{\mathbf{h}}^2+\mathbf{g}^H\mathbf{D}\mathbf{g}\right)\right] - \mathbb{E}_{\mathbf{g}}\left[\log(1+\mathbf{g}^H\mathbf{D}\mathbf{g})\right]\Big),
\end{aligned} \tag{14}$$

where the equality comes from the fact that the distribution of $\mathbf{g} \sim CN(0,\sigma_{\mathbf{g}}^2\mathbf{I})$ is unchanged by the rotation of unitary $\mathbf{U}$, and we can set $\Sigma_{\mathbf{x}} = \mathbf{D}$ ($\mathbf{U} = \mathbf{I}$) without loss of optimality.

In the following, we show that subjecting to $\mathrm{Tr}(\mathbf{D}) \le P$, the optimal $\mathbf{D}$ for (14) is

$$\mathbf{D}^* = \mathrm{diag}\{P/N_T, P/N_T, \cdots, P/N_T\}. \tag{15}$$

First of all, from [9, Section V], the optimal $\mathbf{D}$ for (14) satisfies $\mathrm{Tr}(\mathbf{D}) = P$. Then for any $\mathbf{D} = [d_1, d_2, \cdots, d_{N_T}]$ where $\sum_{i=1}^{N_T} d_i = P$ and $d_i \ge 0, \forall i$, we want to prove that for $\mathbf{D}^*$ defined in (15)

$$\begin{aligned}
&\mathbb{E}_{\mathbf{g}}\left[\log\left(a+\mathbf{g}^H\mathbf{D}\mathbf{g}\right)\right] - \mathbb{E}_{\mathbf{g}}\left[\log\left(1+\mathbf{g}^H\mathbf{D}\mathbf{g}\right)\right] \\
\le&\mathbb{E}_{\mathbf{g}}\left[\log\left(a+\mathbf{g}^H\mathbf{D}^*\mathbf{g}\right)\right] - \mathbb{E}_{\mathbf{g}}\left[\log\left(1+\mathbf{g}^H\mathbf{D}^*\mathbf{g}\right)\right],
\end{aligned} \tag{16}$$

where we denote $\sigma_{\mathbf{g}}^2/\sigma_{\mathbf{h}}^2$ by a, which belongs to $[0,1)$ since we only need to consider the case where $\sigma_{\mathbf{h}} > \sigma_{\mathbf{g}}$. Here we introduce some results from the stochastic ordering theory [11] to

proceed.

Definition 2 *[11, p.234] A function $\psi(x):[0,\infty)\to\mathbb{R}$ is completely monotone if for all $x>0$ and $n=0,1,2,\cdots$, its derivative $\psi^{(n)}$ exists and $(-1)^n\psi^{(n)}(x)\geq 0$.*

Definition 3 *[11, (5.A.1)] Let B_1 and B_2 be two nonnegative random variables such that $\mathbb{E}[e^{-sB_1}]\geq\mathbb{E}[e^{-sB_2}]$, for all $s>0$. Then B_1 is said to be smaller than B_2 in the Laplace transform order, denoted as $B_1\leq_{LT}B_2$.*

Lemma 2 *[11, Th. 5.A.4] Let B_1 and B_2 be two nonnegative random variables. If $B_1\leq_{LT}B_2$ then $\mathbb{E}[f(B_1)]\leq\mathbb{E}[f(B_2)]$, where the first derivative of a differentiable function f on $[0,\infty)$ is completely monotone, provided that the expectations exist.*

To prove (16), we let $B_1=\mathbf{g}^H\mathbf{D}\mathbf{g}$, $B_2=\mathbf{g}^H\mathbf{D}^*\mathbf{g}$, and $f(x)=\log(a+x)-\log(1+x)$ to invoke Lemma 2. It can be easily verified that ψ(x), the first derivative of $f(x)$, satisfies Definition 2. More specifically, the nth derivative of ψ meets

$$\psi^{(n)}(x)=\begin{cases}\frac{n!}{(a+x)^{n+1}}-\frac{n!}{(1+x)^{n+1}}>0, & \text{if } n \text{ is even},\\ \frac{-n!}{(a+x)^{n+1}}+\frac{n!}{(1+x)^{n+1}}<0, & \text{if } n \text{ is odd},\end{cases}\tag{17}$$

when $x>0$, since $a\in[0,1)$. Now from Lemma 2 and Definition 3, we know that to prove (16) is equivalent to proving $\mathbb{E}[e^{-sB_1}]\geq\mathbb{E}[e^{-sB_2}]$ or

$$\log(\mathbb{E}[e^{-sB_1}]/\mathbb{E}[e^{-sB_2}])\geq 0,\forall s>0.$$

From [18, p.40], we know that

$$\log\left(\frac{\mathbb{E}[e^{-sB_1}]}{\mathbb{E}[e^{-sB_2}]}\right)=\sum_{k=1}^{N_T}\log(1+\sigma_{\mathbf{g}}^2d_k^*s)-\sum_{k=1}^{N_T}\log(1+\sigma_{\mathbf{g}}^2d_ks).\tag{18}$$

To show that the above is nonnegative, we resort to the majorization theory. Note that $\sum_{k=1}^{N_T}\log(1+\sigma_{\mathbf{g}}^2\check{d}_ks)$ is a Schur-concave function [12] in $(\check{d}_1,\ldots,\check{d}_{N_T})$, $\forall s>0$, and by definition of majorization [12],

$$\begin{aligned}(d_1^*,\cdots,d_{N_T}^*)&=(P/N_T,P/N_T,\cdots,P/N_T)\\&\prec(d_1,d_2,\cdots d_{N_T}),\end{aligned}\tag{19}$$

where $\mathbf{b} \prec \mathbf{a}$ means that $\mathbf{b}$ is majorized by $\mathbf{a}$. Thus from [12], we know that the RHS of (18) is nonnegative, $\forall s > 0$. Then (16) is valid, and $\mathbf{D}^*$ is optimal for (14). Note that $\mathbf{D}^*$ is also the optimal $\Sigma_{\mathbf{x}}$ of (5) since $\mathbf{U}$ in (14) is selected as $\mathbf{I}$. Substituting $\mathbf{D}^*$ in (15) as the optimal $\Sigma_{\mathbf{x}}$ into the target function of (5), we have (12). ■

Remark 4: In [9, Sec. VII], the channel input covariance matrix $\Sigma_{\mathbf{x}}$ for (5) is solved by an iterative algorithm *numerically*. Although the MISO legitimate channel in [9] can be correlated, even in our i.i.d. fading cases, the algorithm in [9] cannot guarantee the optimality. In contrast, the contribution of our Theorem 1 is that we *analytically* solve the optimal $\Sigma_{\mathbf{x}}$, which equals to the diagonal $\mathbf{D}^*$ in (15). Finally, as discussed in Remark 2, the secrecy capacity lower bound in [10] is *not* achievable. Thus the conclusion in [10], which claims that the uniform power allocation among transmit antennas is not secrecy capacity achieving, is *wrong*.

Remark 5: One can immediately generalize our results in Lemma 1 to the case where the legitimate receiver and eavesdropper with multiple antennas. Specifically, if the legitimate user and eavesdropper have the same number of antenna and the two channels $\mathbf{H}$ and $\mathbf{G}$ (corresponding to $\mathbf{h}$ and $\mathbf{g}$ in (1), respectively) are i.i.d. Rayleigh fading, then the fast fading secrecy capacity with only statistical CSIT is

$$\begin{aligned} C_s &= \max_{p_{\mathbf{x}}} I(\mathbf{x},\mathbf{y}|\mathbf{H}) - I(\mathbf{x},\mathbf{y}|\mathbf{G}) \\ &= \max_{\Sigma_{\mathbf{x}}} \left(\mathbb{E}_{\mathbf{H}} \left[\log \left| \mathbf{I} + \mathbf{H}^H \Sigma_{\mathbf{x}} \mathbf{H} \right| \right] - \mathbb{E}_{\mathbf{G}} \left[\log \left| \mathbf{I} + \mathbf{G}^H \Sigma_{\mathbf{x}} \mathbf{G} \right| \right] \right), \end{aligned}$$

where the second equality corresponds to (5). However, extending our proof of Theorem 1 to this case is not trivial. Thus whether the optimal covariance matrix for the above optimization problem is still a scaled identity matrix or not is still unknown.

Based on our secrecy capacity results in Theorem 1, we have the following asymptotic results. Unfortunately, with only statistical CSIT, the secrecy capacity scales with neither the transmitter power constraint P nor the number of antennas N_T for the considered MISOSE channel (1) (2).

Corollary 1 *With only statistical CSIT of* $\mathbf{h}$ *and* $\mathbf{g}$, *when* $P \to \infty$, *the secrecy capacity* C_s *in* (12) *converges to* $2\log(\sigma_{\mathbf{h}}/\sigma_{\mathbf{g}})$ *when* $\sigma_{\mathbf{h}} > \sigma_{\mathbf{g}} > 0$.

Proof: Note that we only consider the scenario $\sigma_{\mathbf{h}} > \sigma_{\mathbf{g}}$, since from our results the secrecy capacity is zero when $\sigma_{\mathbf{h}} \leq \sigma_{\mathbf{g}}$. When $\sigma_{\mathbf{h}} > \sigma_{\mathbf{g}}$,

$$\begin{aligned} C_s =& \mathbb{E}_{\mathbf{h}}\left[\log\left(1+P\frac{||\mathbf{h}||^2}{N_T}\right)\right] - \mathbb{E}_{\mathbf{g}}\left[\log\left(1+P\frac{||\mathbf{g}||^2}{N_T}\right)\right] \\ \overset{(a)}{=}& \mathbb{E}_{\mathbf{g}}\left[\log\left(1+\frac{\sigma_{\mathbf{h}}^2}{\sigma_{\mathbf{g}}^2}\frac{P||\mathbf{g}||^2}{N_T}\right)\right] - \mathbb{E}_{\mathbf{g}}\left[\log\left(1+\frac{P||\mathbf{g}||^2}{N_T}\right)\right] \\ =& \mathbb{E}_{\mathbf{g}}\left[\log\left(\frac{\frac{1}{P}+\frac{\sigma_{\mathbf{h}}^2}{\sigma_{\mathbf{g}}^2}\frac{||\mathbf{g}||^2}{N_T}}{\frac{1}{P}+\frac{||\mathbf{g}||^2}{N_T}}\right)\right] \\ =& \int \log\left(\frac{\frac{1}{P}+\frac{\sigma_{\mathbf{h}}^2}{\sigma_{\mathbf{g}}^2}\frac{||\mathbf{g}||^2}{N_T}}{\frac{1}{P}+\frac{||\mathbf{g}||^2}{N_T}}\right) f_{\mathbf{g}} d\mathbf{g}, \end{aligned} \tag{20}$$

where (a) uses the fact that $\mathbf{h}$ and $(\sigma_{\mathbf{h}}/\sigma_{\mathbf{g}})\mathbf{g}$ has the same distributions, and $f_{\mathbf{g}}$ in (20) is the p.d.f. of $\mathbf{g}$. Then we have the following two facts, $\forall\, P$, when $\sigma_{\mathbf{h}} > \sigma_{\mathbf{g}} > 0$,

$$\left|\log\left(\frac{\frac{1}{P}+\frac{\sigma_{\mathbf{h}}^2}{\sigma_{\mathbf{g}}^2}\frac{||\mathbf{g}||^2}{N_T}}{\frac{1}{P}+\frac{||\mathbf{g}||^2}{N_T}}\right)\right| \leq \log\left(\frac{\frac{\sigma_{\mathbf{h}}^2}{\sigma_{\mathbf{g}}^2}\frac{||\mathbf{g}||^2}{N_T}}{\frac{||\mathbf{g}||^2}{N_T}}\right),$$

and

$$\begin{aligned} \int \log\left(\frac{\frac{\sigma_{\mathbf{h}}^2}{\sigma_{\mathbf{g}}^2}\frac{||\mathbf{g}||^2}{N_T}}{\frac{||\mathbf{g}||^2}{N_T}}\right) f_{\mathbf{g}} d\mathbf{g} &= \int \log\left(\frac{\sigma_{\mathbf{h}}^2}{\sigma_{\mathbf{g}}^2}\right) f_{\mathbf{g}} d\mathbf{g} \\ &= 2\log\left(\frac{\sigma_{\mathbf{h}}}{\sigma_{\mathbf{g}}}\right) < \infty. \end{aligned}$$

Note that we exclude the case $\sigma_{\mathbf{g}} = 0$ since it is a trivial case corresponding to the communication without secrecy. From the above two facts, we can invoke the dominated convergence theorem [19, Th. 16.4] to exchange the order of the limit operation and the integral to compute $\lim_{P\to\infty} C_s$

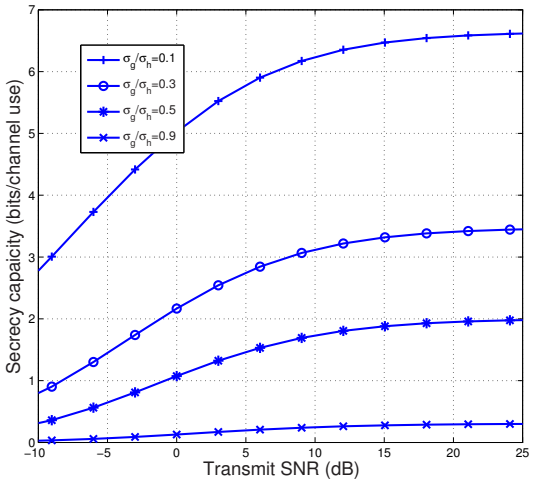

Fig. 2. Comparison of the secrecy capacities of fast Rayleigh fading MISOSE wiretap channels under different eavesdropper-to-legitimate-channel qualities $\sigma_{\mathbf{g}}/\sigma_{\mathbf{h}}$.

from (20) as

$$\begin{aligned}\lim_{P\to\infty} C_s &= \lim_{P\to\infty} \int \log\left(\frac{\frac{1}{P}+\frac{\sigma_{\mathbf{h}}^2}{\sigma_{\mathbf{g}}^2}\frac{||\mathbf{g}||^2}{N_T}}{\frac{1}{P}+\frac{||\mathbf{g}||^2}{N_T}}\right) f_{\mathbf{g}} d\mathbf{g} \\ &= \int \lim_{P\to\infty} \log\left(\frac{\frac{1}{P}+\frac{\sigma_{\mathbf{h}}^2}{\sigma_{\mathbf{g}}^2}\frac{||\mathbf{g}||^2}{N_T}}{\frac{1}{P}+\frac{||\mathbf{g}||^2}{N_T}}\right) f_{\mathbf{g}} d\mathbf{g} \\ &= 2\log\frac{\sigma_{\mathbf{h}}}{\sigma_{\mathbf{g}}}.\end{aligned}$$

■

Corollary 2 *With only statistical CSIT of* $\mathbf{h}$ *and* $\mathbf{g}$*, the secrecy capacity* C_s *in* (12) *converges to*

$$\log\left(1+P\sigma_{\mathbf{h}}^2\right)-\log\left(1+P\sigma_{\mathbf{g}}^2\right),$$

when $N_T \to \infty$.

Proof: By law of large numbers, as $N_T \to \infty$, $||\mathbf{h}||^2/N_T \to \sigma_{\mathbf{h}}^2$ and $||\mathbf{g}||^2/N_T \to \sigma_{\mathbf{g}}^2$, respectively. Applying these facts to (12), our corollary is proved. ■

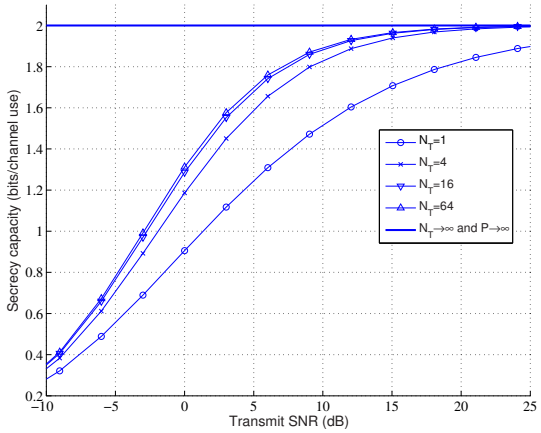

Fig. 3. Comparison of the secrecy capacities of fast Rayleigh fading MISOSE wiretap channels under different numbers of transmit antennas N_T.

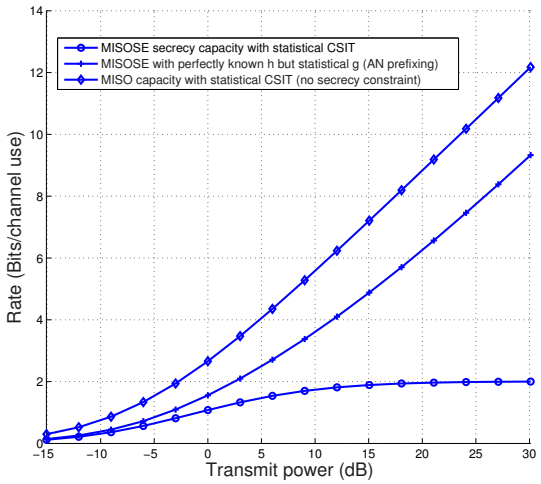

Fig. 4. Comparison of rates/capacities in different fast fading channel settings: MISOSE channel with statistical CSIT of $\mathbf{h}$ and $\mathbf{g}$, MISOSE channel with perfect CSIT of legitimate channel $\mathbf{h}$ and statistical CSIT of the eavesdropper channel $\mathbf{g}$, and MISO channel with statistical CSIT but without secrecy constraint.

IV. Numerical Results

In this section we compare the secrecy capacities under different channel conditions, and without loss of generality we set $\sigma_{\mathbf{g}} = 1$ in all figures. The transmit SNR is defined as P in dB scale since both n_y and n_z have unit variances. In Fig. 2 we compare the secrecy capacities with $N_T = 2$ under different $\sigma_{\mathbf{g}}/\sigma_{\mathbf{h}}$, and find that the secrecy capacity increases while $\sigma_{\mathbf{g}}/\sigma_{\mathbf{h}}$

decreases. Also the secrecy capacity converges to $2\log(\sigma_{\mathbf{h}}/\sigma_{\mathbf{g}})$ when the SNR is high, which is consistent with Corollary 1. In Fig. 3, with $\sigma_{\mathbf{h}}^2 = 4$, we compare the secrecy capacities under different numbers of transmit antennas N_T. We can also find that the secrecy capacity converges when N_T is large enough, which is consistent with Corollary 2. Moreover, when the SNR P increases, the secrecy capacity under large N_T will approach 2 bit/channel use, which is from $\lim_{P\to\infty} \log\left(1+P\sigma_{\mathbf{h}}^2\right) - \log\left(1+P\sigma_{\mathbf{g}}^2\right) = \log\left(\sigma_{\mathbf{h}}^2/\sigma_{\mathbf{g}}^2\right)$ with $\sigma_{\mathbf{h}}^2 = 4$ and $\sigma_{\mathbf{g}}^2 = 1$. Finally, we compare our results with achievable secrecy rates/capacities of other channel settings in Fig. 4, where we set $N_T = 2$ and $\sigma_{\mathbf{g}}/\sigma_{\mathbf{h}} = 0.5$. The fast fading MISOSE channel in [8] [15] [17] is used in comparison, where the transmitter has perfect CSIT of the legitimate channel $\mathbf{h}$ but only statistical CSIT of $\mathbf{g}$. In contrast to the results in Lemma 1, the secrecy capacity of such a channel is unknown and the AN prefixing [8] [15] [17] is useful to increase the secrecy rate. Moreover, unlike results in Corollary 1, with additional perfect CSIT of $\mathbf{h}$, the achievable secrecy rates using AN prefixing scale with P. The capacity of the MISO channel with statistical CSIT but without secrecy constraint is also compared in Fig. 4. As expected, the capacity of such a channel [20], which scales with P, is much larger than the secrecy capacity in Theorem 1.

V. Conclusion

In this paper, we derived the secrecy capacity of the MISOSE ergodic fast Rayleigh fading wiretap channel, where only the statistical CSIT of the legitimate and eavesdropper channels is known. By introducing a new secrecy capacity upper bound, we first showed that the Gaussian input without prefixing is secrecy capacity achieving. Then we analytically found the optimal channel input covariance matrix, and fully characterized the secrecy capacity.

References

[1] Y. Liang, H. V. Poor, and S. S. Shamai, "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, Apr. 2009.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

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

[5] Z. Rezki, A. Khisti, and M. Alouini, "On the ergodic secrecy capacity of the wiretap channel under imperfect main channel estimation," in *Proc. 2011 45th Asilomar Conference on Signals, Systems and Computers (Asilomar2011)*, Nov. 2011, pp. 952–957.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inform. Theory*, vol. 57, no. 8, Aug. 2011.

[7] T. Liu and S. Shamai, "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Trans. Inform. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[8] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[9] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, April 2011.

[10] Z. Rezki, F. Gagnon, and V. Bhargava, "The ergodic capacity of the MIMO wire-tap channel," *http://arxiv.org/abs/0902.0189*, 2009.

[11] M. Shaked and J. G. Shanthikumar, *Stochastic Orders*. Springer, 2007.

[12] A. W. Marshall and I. Olkin, *Inequalities: theory of majorization and its application*. Academic Press, 1980.

[13] T. M. Cover and J. A. Thomas, *Elements of information theory*, 2nd ed. Wiley-Interscience, 2006.

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

[15] Z. Li, R. Yates, and W. Trappe, "Achieving secret communication for fast Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 9, pp. 2792 – 2799, Sep. 2010.

[16] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 762–771, March 2011.

[17] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[18] A. M. Mathai and S. B. Provost, *Quadratic forms in random variables*. Marcel Dekker, New York, 1992.

[19] P. Billingsley, *Probability and Measure*, 3rd ed. John Wiley and Sons, 1995.

[20] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.