On Ergodic Secrecy Capacity of Fast Fading MIMOME Wiretap Channel With Statistical CSIT

Shih-Chun Lin
Department of Electrical and Computer Engineering,
National Taiwan University of Science and Technology, Taipei, Taiwan 10607
sclin@mail.ntust.edu.tw

***Abstract*— In this paper, we consider the secure transmission in ergodic Rayleigh fast-faded multiple-input multiple-output multiple-antenna-eavesdropper (MIMOME) wiretap channels with only statistical channel state information at the transmitter (CSIT). When legitimate receiver has more (or equal) antennas than the eavesdropper, we prove the first MIMOME secrecy capacity result with partial CSIT by establishing a new secrecy capacity upper-bound. The key step is forming an MIMOME degraded channel by dividing the legitimate receiver's channel matrix into two submatrices, and setting one of which the same as the eavesdropper's channel matrix. Next, subject to the total power constraint overall transmit antennas, we solve the channel-input covariance matrix optimization problem to fully characterize the MIMOME secrecy capacity. Typically, the MIMOME optimization problems are non-concave. However, with aids of the proposed degraded channel, we show that the stochastic MIMOME optimization problem can be transformed to be a Schur-concave problem to find its optimal solution. Finally, we find that the MIMOME secrecy capacities scale with the signal-to-noise ratios with large enough numbers of antennas at legitimate receiver. However, as shown in previous works, such a scaling does not exist for wiretap channels with single antenna at legitimate receiver and eavesdropper each.**

I. Introduction

Key-based enciphering is a well-adopted technique to ensure the securities in current data transmission systems. However, for secure communications in wireless networks, the distributions and managements of secret keys may be challenging tasks [1]. The physical-layer security introduced in [2] [3] is appealing due to its keyless nature. The basic building block of physical-layer security is the so-called wiretap channel. In this channel, a source node wishes to transmit confidential messages securely to a legitimate receiver and to keep the eavesdropper as ignorant of the message as possible. Wyner [3] characterized the secrecy capacity of the discrete memoryless wiretap channel, in which the secret key was not used. The secrecy capacity is the largest rate communicated between the source and the destination nodes with the eavesdropper knowing no information of the messages. In order to meet the demand of high data rate transmission and improve the connectivity of the secure network [4], the multiple antenna systems with security concern are considered by several authors. In [5], the secrecy capacity of a Gaussian channel with two-input, two-output, single-antenna-eavesdropper was first characterized. Using various proof technique, the authors of [6], [7] proved the secrecy capacities of general Gaussian multiple-input multiple-output multiple-antenna-eavesdropper (MIMOME) channels. In wireless environments, the time-varying characteristic of fading channels can be further exploited to enhance the secrecy [8].

However, to attain the secrecy capacity results in [5]–[8], at least the perfect knowledge of the legitimate receiver's channel state information at the transmitter (CSIT) is required. For the fast fading channels, it may be hard to track the rapidly varying channel coefficients because of the limited feedback bandwidth and the delay caused by the channel estimation. Thus for fast-fading channels, it is more practical to consider the case with only partial CSIT of the legitimate channel. For this setting, the secrecy capacity is only rigorously characterized for multiple-input single-output single-antenna-eavesdropper (MISOSE) Rayleigh fast-faded channels [9]. A negative phenomenon was revealed in [9] that for the MISOSE channels with only statistical CSIT, the secrecy capacities do not scale with the signal-to-noise ratio (SNR). In the high SNR regime, using multiple transmitter antennas in the MISOSE system has limited help to increase the secrecy capacity compared to the system using single transmitter antenna.

In this paper, we wish to overcome the aforementioned drawbacks of the MISOSE channels and aim to obtain the SNR scaling of secrecy capacity. Here we consider the MIMOME fast Rayleigh-faded channels where the transmitter only have the statistical CSIT of the legitimate and eavesdropper channels. The MIMOME secrecy capacity is characterized when number of antennas of the legitimate receiver is more (or equal) than that of the eavesdropper. To the best of the author's knowledge, this is the first MIMOME secrecy capacity result with partial CSIT. Compared with our previous works [9], new proof techniques are developed for the MIMOME channels. First, we establish a new secrecy capacity upper-bound by dividing the channel matrix of legitimate receiver into two submatrices, one of which has dimensions equal to those of the eavesdropper's channel matrix, to form an MIMOME degraded channel. Second, instead of using completely monotone property as [9], which may only exists for the MISOSE problem, we solve the stochastic MIMOME optimization problem by transforming it to an equivalent Schur-concave problem. The

This work was supported by the National Science Council, Taiwan, R.O.C., under grant NSC 101-2221-E-027-085-MY3

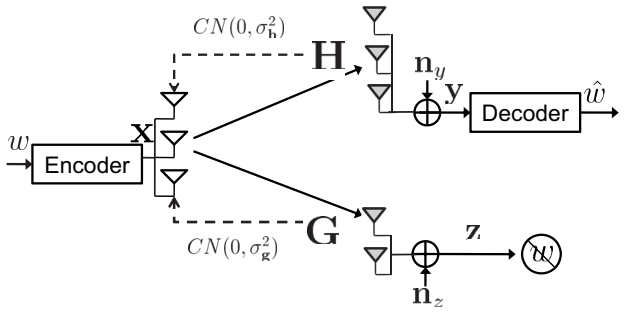

Fig. 1. Fast Rayleigh fading MIMOME wiretap channel with statistical CSIT.

key to this transformation is using the proposed equivalent MIMOME degraded channel. Based on our secrecy capacity results, on the contrary to [9], we show that the SNR scaling of secrecy capacity can be obtained in the MIMOME channels.

II. System Model

In the considered MIMOME 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 transmitter has n_t antennas, while the legitimate receiver and eavesdropper respectively have n_r and n_e antennas as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}_y, \tag{1}$$

$$\mathbf{z} = \mathbf{G}\mathbf{x} + \mathbf{n}_z, \tag{2}$$

where $\mathbf{x} \in \mathbb{C}^{n_t \times 1}$ represents the transmitted vector signal; the legitimate channel matrix is $\mathbf{H} \in \mathbb{C}^{n_r \times n_t}$ while the eavesdropper channel matrix is $\mathbf{G} \in \mathbb{C}^{n_e \times n_t}$; $\mathbf{n}_y$ and $\mathbf{n}_z$ are additive white Gaussian noise vectors at the legitimate receiver and eavesdropper, respectively, with each element independent and identically distributed (i.i.d.), circularly symmetric, and having zero mean and unit variance. The channels are assumed to be fast Rayleigh fading, that is, each element of $\mathbf{H}$ and $\mathbf{G}$ is i.i.d distributed as

$$CN(0,\sigma_{\mathbf{h}}^2) \text{ and } CN(0,\sigma_{\mathbf{g}}^2), \tag{3}$$

respectively, while the channel coefficients change in each symbol time. The $\mathbf{H}$, $\mathbf{G}$, $\mathbf{n}_y$ and $\mathbf{n}_z$ are independent. We 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.

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, where $\mathbf{z}^N$, $\mathbf{H}^N$, and $\mathbf{G}^N$ are the collections of $\mathbf{z}$, $\mathbf{H}$, and $\mathbf{G}$ over the code length N, respectively.

Definition 1 (Secrecy Capacity [1] [3] [8]): 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 $N > N_0$

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

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.*

Note that as [1] [3] [8], the equivocation under perfect secrecy requirement is measured by $I(w; \mathbf{z}^N, \mathbf{H}^N, \mathbf{G}^N)/N = R - R_e$, which is based on all the information $(\mathbf{z}^N, \mathbf{H}^N, \mathbf{G}^N)$ that the eavesdropper can obtain.

From Csiszár and Körner's seminal work [2], we know that the secrecy capacity of MIMOME channel (1) and (2) is

$$C_s = \max \; I(U; \mathbf{y}, \mathbf{H}) - I(U; \mathbf{z}, \mathbf{H}, \mathbf{G}), \tag{5}$$

where U is an auxiliary random variable satisfying the Markov relationship $U \rightarrow \mathbf{x} \rightarrow (\mathbf{y}, \mathbf{H}), (\mathbf{z}, \mathbf{H}, \mathbf{G})$. However, the optimal choice of U which maximizes C_s of considered fast fading MIMOME channel is *unknown*.

Notations: In this paper, lower and upper case bold alphabets denote vectors and matrices, respectively. The superscript $(.)^H$ denotes the transpose complex conjugate. $|\mathbf{A}|$ and $|a|$ represent the determinant of the square matrix $\mathbf{A}$ and the absolute value of the scalar variable a, respectively. The trace of $\mathbf{A}$ is denoted by $\mathrm{tr}(\mathbf{A})$, and $\mathbf{I}$ denotes the identity matrix. The mutual information between two random variables is denoted by $I(;)$.

III. Secrecy capacity for the fast fading MIMOME wiretap channel

In this section, we explicitly find the optimal U in (5) for wiretap channel (1)(2), and fully characterize the MIMOME secrecy capacity with statistical CSIT in the upcoming Theorem 1. When there is full CSIT [6] [7], one can find the optimal auxiliary random variable U by constructing an equivalent degraded MIMOME channel to upper-bound the secrecy capacity. With only statistical CSIT, (5) becomes

$$C_s = \max_{U \rightarrow \mathbf{x} \rightarrow (\mathbf{y},\mathbf{H}),(\mathbf{z},\mathbf{H},\mathbf{G})} I(U; \mathbf{y}|\mathbf{H}) - I(U; \mathbf{z}|\mathbf{H}, \mathbf{G}), \tag{6}$$

which results from the fact that the transmitter does not have the knowledge of the realizations of $\mathbf{H}$ and $\mathbf{G}$. However, with only the statistical CSIT, in general it is very hard to find the optimal U maximizing (6). It is because that if one naively applies the degraded channel construction methods in [6] [7], the resulting secrecy capacity upper-bound will depend on the realizations of $\mathbf{H}$ and $\mathbf{G}$. However, in the following Lemma, by using the properties of Rayleigh fading channels in (3), we show that one may still construct a degraded channel and

find the optimal U maximizing (6) . The key for building this equivalent degraded MIMOME channel for (1)(2) is replacing the legitimate channel $\mathbf{H}$ in (7) with equivalent $\mathbf{H}'$ in upcoming (8). Due to the limited space, in this paper, we only provide the sketches of proofs for all results while all the details are given in [10].

Lemma 1: For the MIMOME fast Rayleigh fading wiretap channel (1)(2) with the statistical CSIT of $\mathbf{H}$ and $\mathbf{G}$, using Gaussian $\mathbf{x}$ without prefixing $U \equiv \mathbf{x}$ is the optimal transmission strategy for (6) when $n_r \geq n_e$ and $\sigma_h \geq \sigma_g$, where n_r and n_e are the number of antennas at the legitimate receiver and eavesdropper, respectively, while σ_h and σ_g are defined in (3).

Sketch of Proof: We first form the degraded MIMOME channel with respect to (1)(2). Since $n_r \geq n_e$, one can separate legitimate channel matrix $\mathbf{H}$ as two submatrices

$$\mathbf{H} = [\mathbf{H}_{(n_r-n_e)}^T \ \mathbf{H}_{n_e}^T]^T, \tag{7}$$

where $\mathbf{H}_{(n_r-n_e)} \in \mathbb{C}^{(n_r-n_e)\times n_t}$ and $\mathbf{H}_{n_e} \in \mathbb{C}^{n_e \times n_t}$, with each element of $\mathbf{H}_{(n_r-n_e)}$ and $\mathbf{H}_{n_e}$ distributed as i.i.d. $CN(0,\sigma_h^2)$. From the properties of complex Gaussian distributions, the distribution of $\mathbf{H}$ is the same as that of

$$\mathbf{H}' = [\mathbf{H}_{(n_r-n_e)}^T \ \left(\frac{\sigma_\mathbf{h}}{\sigma_\mathbf{g}}\right)\mathbf{G}^T]^T, \tag{8}$$

since each element of eavesdropper channel matrix $\mathbf{G}$ is distributed as $CN(0,\sigma_g^2)$ as (3). And we can form an equivalent received signal

$$\mathbf{y}' = \mathbf{H}'\mathbf{x} + \mathbf{n}_y, \tag{9}$$

which has the same marginal distribution as the legitimate received signal $\mathbf{y}$ in (1). Then we have the Markov relationship

$$\mathbf{x} \rightarrow \frac{\sigma_\mathbf{g}}{\sigma_\mathbf{h}}\mathbf{y}' \rightarrow \mathbf{z}. \tag{10}$$

The degraded MIMOME wiretap channel $(\mathbf{x}, (\sigma_\mathbf{g}/\sigma_\mathbf{h})\mathbf{y}', \mathbf{z})$ is then formed.

Now based on the proposed degraded channel $(\mathbf{x}, (\sigma_\mathbf{g}/\sigma_\mathbf{h})\mathbf{y}', \mathbf{z})$, we know that

$$\begin{aligned} C_s &\leq \max_\mathbf{x} I(\mathbf{x}; \frac{\sigma_\mathbf{g}}{\sigma_\mathbf{h}}\mathbf{y}'|\mathbf{H}') - I(\mathbf{x};\mathbf{z}|\mathbf{G}), \\ &= \max_\mathbf{x} I(\mathbf{x};\mathbf{y}|\mathbf{H}) - I(\mathbf{x};\mathbf{z}|\mathbf{G}). \end{aligned} \tag{11}$$

From [2], we also know the RHS of (11) is achievable. Thus the RHS of (11) is the secrecy capacity C_s. Furthermore, from [7], we know that Gaussian $\mathbf{x}$ is optimal for the secrecy capacity in (11). Then our claim is valid. *Q.E.D.*

Note that on the contrary to [6] [7], our secrecy capacity upper-bound (11) is independent of the realizations of $\mathbf{H}$ and $\mathbf{G}$ and tight. Compared to the proof for the MISOSE secrecy capacity [9], the key for deriving the tight MIMOME upper-bound is separating the legitimate channel matrix $\mathbf{H}$ by two submatrices $\mathbf{H}_{(n_r-n_e)}$ and $\mathbf{H}_{n_e}$ as (7), and only introducing correlations between $\mathbf{H}_{n_e}$ and $\mathbf{G}$ as (8). One can treat that the sub channel-matrix $\mathbf{H}_{(n_r-n_e)}$ is a "safe" one without being eavesdropped, and provides SNR scaling for secrecy capacity. In MISOSE channel, such a $\mathbf{H}_{(n_r-n_e)}$ does not exist since $n_r = n_e = 1$, and there is no SNR scaling. This intuition is verified rigorously from the upcoming Theorem 1 and Corollary 1.

Now we fully characterize the MIMOME secrecy capacity based on Lemma 1. Typically, the MIMOME secrecy capacity optimization problems like the upcoming (13) are non-concave. This is due to that the MIMOME secrecy capacity, such as (13), is a difference of two concave functions. However, with aids of the degraded MIMOME channels formed by (8), the stochastic MIMOME optimization problem (13) can be transformed to be a Schur-concave problem. It helps a lot to find the optimal solution (14). Note that the completely monotone property for MISOSE optimization problem [9] may not exist for the MIMOME one, thus the method in [9] is hard to be extended to the MIMOME case.

Theorem 1: Subject to the total power constraint

$$\mathrm{Tr}\left(\Sigma_\mathbf{x}\right) \leq P \tag{12}$$

the MIMOME secrecy capacity under $n_r \geq n_e$ and $\sigma_h \geq \sigma_g$ is

$$C_s = \max_{\Sigma_\mathbf{x}} \left(\mathbb{E}_\mathbf{H}\left[\log\left|\mathbf{I} + \mathbf{H}\Sigma_\mathbf{x}\mathbf{H}^\dagger\right|\right] - \mathbb{E}_\mathbf{G}\left[\log\left|\mathbf{I} + \mathbf{G}\Sigma_\mathbf{x}\mathbf{G}^\dagger\right|\right)\right), \tag{13}$$

and the optimal channel input covariance matrix subject to (12) is

$$\Sigma_\mathbf{x}^* = \frac{P}{n_t}\mathbf{I}. \tag{14}$$

Sketch of Proof: First, we show that under our setting, the stochastic MIMOME optimization problem is indeed concave as follows. The key is cleverly using the same marginal channel formed by (8). Note that by setting where $\mathbf{x} \sim CN(0,\Sigma_\mathbf{x})$, the target function in (13) can be rewriten as

$$\begin{aligned} &I(\mathbf{x};\mathbf{y}|\mathbf{H}) - I(\mathbf{x};\mathbf{z}|\mathbf{G}) \\ =&I(\mathbf{x};\frac{\sigma_\mathbf{g}}{\sigma_\mathbf{h}}\mathbf{y}'|\mathbf{z},\mathbf{H}'). \end{aligned} \tag{15}$$

From [6], we know that the RHS of (15) is concave in $\Sigma_\mathbf{x}$ and thus (13) is concave.

After showing that (13) is concave, we can further transform (13) to a Schur-concave problem. Then the optimal $\Sigma_\mathbf{x} = \alpha\mathbf{I}$ where $0 \leq \alpha \leq P/n_t$. Finally, we can show show that using all the available power, that is, $\Sigma_x = P/n_t$ is optimal for (13) under (12). It then concludes our proof. *Q.E.D.*

Now we have the following high SNR result for the secrecy capacity in Theorem 1 when $P \rightarrow \infty$

Corollary 1: Subject to total power constraint (12), as $P \rightarrow \infty$, the MIMOME secrecy capacity C_s has

$$\lim_{P\rightarrow\infty}\frac{C_s}{\log P} = \begin{cases} n_r - n_e, & n_t \geq n_r > n_e \\ n_t - n_e, & n_r \geq n_t > n_e \\ 0, & n_r \geq n_e \geq n_t \end{cases}$$

for fixed $\sigma_h \geq \sigma_g > 0$, where n_t, n_r, and n_e are the number of antennas at the transmitter, legitimate receiver and eavesdropper, respectively.

In [9], it was shown that when $n_r = n_e = 1$, the secrecy capacity does not scale with P. Our Corollary 1 further shows that as long as $n_r = n_e$, even the legitimate receiver has multiple antennas, the secrecy capacity does not scale with P. Moreover, such a scaling does not exist even when $n_r > n_e$, if the number of transmit antenna is not large enough as $n_e \geq n_t$. To make secrecy capacity scale with P, we must let $n_t > n_e$. Adding enough number of transmit antennas n_t (also enough number of legitimate-receiver antennas n_r) is very important for increasing the secrecy capacity.

It will be interesting to see when the secrecy capacity is zero. We have the following result, where the proof is similar to that of Lemma 1.

Corollary 2: For the MIMOME fast Rayleigh fading wire-tap channel (1)(2) with the statistical CSIT of $\mathbf{H}$ and $\mathbf{G}$, the secrecy capacity is zero when $n_r \leq n_e$ and $\sigma_h \leq \sigma_g$.

IV. Numerical results

In this section, we provide numerical results for our secrecy capacity in Theorem 1. Each noise at the legitimate receiver and eavesdropper has unit variance. We compare the the SNR scaling of MIMOME secrecy capacities subject to total power constraints P as (12) in Fig. 2. And the SNR equals to $10\log_{10} P$. Three different number of antennas combinations (n_t, n_r, n_e) are considered, where n_t, n_r and n_e respectively are the number of antennas at the transmitter, legitimate receiver, and eavesdropper. Consistent with [9], when $n_r = n_e = 1$, the secrecy capacities do not scale with SNR and converges at high SNR. Thus it may be a waste of resources by increasing the SNR in this setting. To overcome this drawback, with fixed number of transmit antennas $n_t > n_e$, one can increase the number of antennas at legitimate receiver n_r to make $n_r > n_e$. And adding more antennas at legitimate receiver, such as increasing $n_r = 3$ to $n_r = 4$, is very helpful to increase the secrecy capacities at the high SNR regime. These observations meet our results in Corollary 1.

V. Conclusion

In this paper, the secure transmission in ergodic Rayleigh MIMOME wiretap channels with only the statistics of CSIT was considered. When the number of antennas of legitimate receiver was more (or equal) than that of the eavesdropper, we proved the first MIMOME secrecy capacity result with partial CSIT. We found that the MIMOME secrecy capacities scale with the signal-to-noise ratios with large enough numbers of antennas at legitimate receiver. This overcome the shortcoming of MISOSE channel, where it was shown that SNR scaling for the secrecy capacity did not exist.

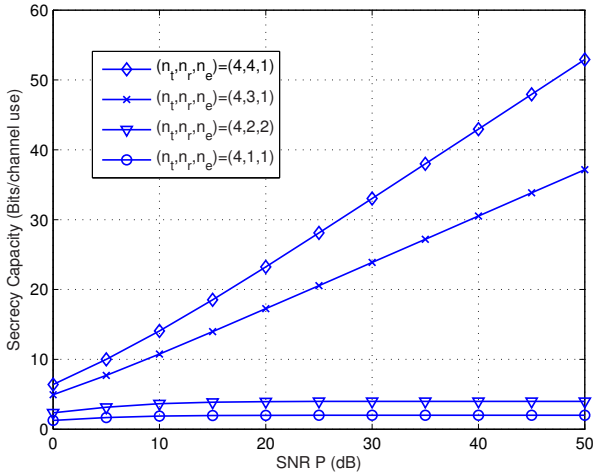

Fig. 2. Subject to total power constraints, the secrecy capacities versus SNRs with different number of antennas and $\sigma_h^2/\sigma_g^2 = 4$.

References

[1] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "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. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

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

[4] X. Zhou, R. K. Ganti, and J. G. Andews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[5] S. Shafiee and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: the 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sept. 2009.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov 2010.

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

[8] P. 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, Oct. 2008.

[9] S.-C. Lin and P.-H. Lin, "On secrecy capacity of fast fading multiple input wiretap channels with statistical CSIT," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 2, pp. 414–419, Feb. 2013.

[10] S. C. Lin and C. L. Lin, "On secrecy capacity of fast fading MIMOME wiretap channels with statistical CSIT," *submitted to IEEE Transactions on Wireless Communications*. [Online]. Available: http://arxiv.org/abs/1309.1516