A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel

Tie Liu, *Member, IEEE*, and Shlomo Shamai (Shitz), *Fellow, IEEE*

***Abstract*—The secrecy capacity of the multiple-antenna wiretap channel under the average total power constraint was recently characterized, independently, by Khisti and Wornell and Oggier and Hassibi using a Sato-like argument and matrix analysis tools. This paper presents an alternative characterization of the secrecy capacity of the multiple-antenna wiretap channel under a more general matrix constraint on the channel input using a channel-enhancement argument. This characterization is by nature information-theoretic and is directly built on the intuition regarding to the optimal transmission strategy in this communication scenario.**

***Index Terms*—Channel enhancement, multiple-antenna communications, wiretap channel.**

I. Introduction

CONSIDER a multiple-antenna wiretap channel with n_t transmit antennas and n_r and n_e receive antennas at the legitimate recipient and the eavesdropper

$$\begin{aligned} \boldsymbol{y}_r[m] &= \boldsymbol{H}_r\boldsymbol{x}[m] + \boldsymbol{z}_r[m] \\ \boldsymbol{y}_e[m] &= \boldsymbol{H}_e\boldsymbol{x}[m] + \boldsymbol{z}_e[m] \end{aligned} \tag{1}$$

where $\boldsymbol{H}_r$ and $\boldsymbol{H}_e$ are the real channel matrices associated with the legitimate recipient and the eavesdropper, respectively. The channel matrices $\boldsymbol{H}_r$ and $\boldsymbol{H}_e$ are assumed to be fixed during the entire transmission and are known to all terminals. The additive noise $\boldsymbol{z}_r[m]$ and $\boldsymbol{z}_e[m]$ are Gaussian vectors with zero mean and identity covariance matrices and are independent across the time index m. The channel input $\{\boldsymbol{x}[m]\}_m$ satisfies an average total power constraint

$$\frac{1}{n}\sum_{m=1}^{n} ||\boldsymbol{x}[m]||^2 \le P. \tag{2}$$

The *secrecy capacity* of a wiretap channel is defined as the maximum rate of communication such that the information can be decoded arbitrarily reliably at the legitimate recipient but cannot be inferred at any positive rate at the eavesdropper [1], [2]. An illustration of this communication scenario is shown in Fig. 1.

Manuscript received November 15, 2007; revised January 24, 2009. Current version published May 20, 2009. This work was supported by the European Commission in the framework of the FP7 Network of Excellence in Wireless Communications NEWCOM++. The material in this paper was presented in part at the Information Theory and Applications Workshop, University of California, San Diego, La Jolla, CA, January 2008.

T. Liu is with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA (e-mail: tieliu@tamu.edu).

S. Shamai (Shitz) is with the Department of Electrical Engineering, Technion–Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: sshlomo@ee.technion.ac.il).

Communicated by G. Kramer, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2009.2018322

For a general discrete memoryless wiretap channel with transition probability $p(y_r, y_e|x)$, a single-letter expression for the secrecy capacity was obtained by Csiszár and Körner [2]

$$C_s = \max_{p(u,x)} [I(U;Y_r) - I(U;Y_e)] \tag{3}$$

where U is an auxiliary variable satisfying the Markov relation

$$U \to X \to (Y_r, Y_e). \tag{4}$$

Moreover, the secrecy capacity expression (3) extends to continuous-alphabet problems with average cost constraints. Thus, the problem of characterizing the secrecy capacity of the multiple-antenna wiretap channel reduces to evaluating (3) for the specific channel model (1).

Note that evaluating (3) involves solving a functional (possibly) *nonconvex* optimization problem. Solving optimization problems of this type usually requires nontrivial techniques and strong inequalities. Indeed, for the single-antenna case ($n_t = n_r = n_e = 1$), the secrecy capacity expression (3) was successfully evaluated by Leung and Hellman [5] using a result of Wyner [1] on *degraded* wiretap channels and the celebrated entropy-power inequality [6, Ch. 16.7].[1] Unfortunately, the same approach does not extend to the multiple-antenna case, as the latter in its general form belongs to the class of *nondegraded* wiretap channels. The problem of characterizing the secrecy capacity of the multiple-antenna wiretap channel was open until the recent work of Khisti and Wornell [3] and Oggier and Hassibi [4]. The special cases when

1) $n_t = n_r = 2$, $n_e = 1$; and
2) $n_r = 1$, n_t and n_e arbitrary

were independently settled by Shafiee *et al.* [8] and Khisti *et al.* [9], respectively. In their respective work, Khisti and Wornell [3] and Oggier and Hassibi [4] followed an *indirect* approach to evaluate the secrecy capacity of the multiple-antenna wiretap channel (1). Key to their evaluations is the following genie-aided upper bound:

$$\begin{aligned} C_s &= \max_{p(u,x)} [I(U;Y_r) - I(U;Y_e)] \\ &\le \max_{p(u,x)} [I(U;Y_r,Y_e) - I(U;Y_e)] \\ &= \max_{p(u,x)} \Big\{ I(X;Y_r,Y_e) - I(X;Y_e) \\ &\qquad - [I(X;Y_r,Y_e|U) - I(X;Y_e|U)] \Big\} \qquad (5) \\ &\le \max_{p(x)} [I(X;Y_r,Y_e) - I(X;Y_e)] \\ &= \max_{p(x)} I(X;Y_r|Y_e) \qquad (6) \end{aligned}$$

[1] Alternatively, it can also be evaluated using Wyner's result [1] and a classical result from estimation theory via a relationship between mutual information and minimum mean-squared error estimate [7].

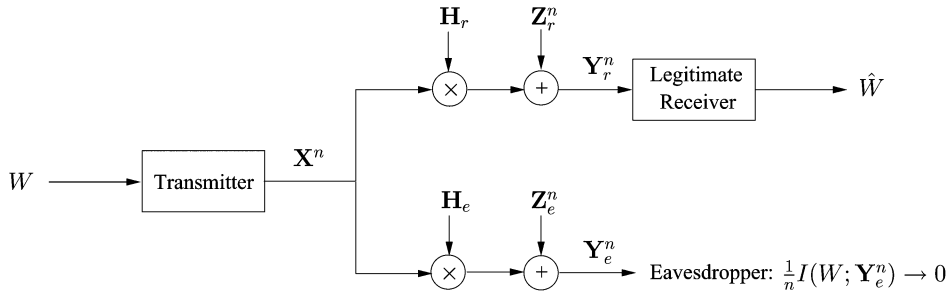

Fig. 1. Multiple-antenna wiretap channel.

where (5) follows from the Markov relation (4). Furthermore, Khisti and Wornell [3] and Oggier and Hassibi [4] noticed that the original objective of optimization $I(U;Y_r) - I(U;Y_e)$ depends on the channel transition probability $p(y_r, y_e|x)$ only through its marginals $p(y_r|x)$ and $p(y_e|x)$, whereas the objective function $I(X;Y_r|Y_e)$ in the upper bound (6) does depend on the *joint* conditional $p(y_r, y_e|x)$. Therefore, the upper bound (6) can be further improved as

$$C_s \le \max_{p(x)} I\left(X;Y_r'|Y_e'\right) \tag{7}$$

for any joint conditional $p\left(y_r', y_e'|x\right)$ such that $p\left(y_r'|x\right) = p(y_r|x)$ and $p\left(y_e'|x\right) = p(y_e|x)$.

Note that the upper bound on the right-hand side of (7) has a specific meaning: It is the secrecy capacity of the wiretap channel $p\left(y_r', y_e'|x\right)$ where the legitimate recipient has access to both Y_r' and Y_e', minimized over all possible correlations between Y_r' and Y_e'. In essence, this is very similar to the Sato upper bound [10] on the sum capacity of a general broadcast channel. For the multiple-antenna wiretap channel (1), Khisti and Wornell [3] and Oggier and Hassibi [4] showed that for a given jointly Gaussian $\left(\boldsymbol{Z}_r', \boldsymbol{Z}_e'\right)$, the conditional mutual information $I\left(\boldsymbol{X};\boldsymbol{X}+\boldsymbol{Z}_r'|\boldsymbol{X}+\boldsymbol{Z}_e'\right)$ is maximized when the channel input $\boldsymbol{X}$ is Gaussian. Therefore, the upper bound in the right-hand side of (6) can be written as a *matrix* optimization problem

$$\min_{\boldsymbol{K}_\phi \in \mathcal{K}_\phi} \max_{\boldsymbol{K}_x \in \mathcal{K}_x} I\left(\boldsymbol{X};\boldsymbol{X}+\boldsymbol{Z}_r'|\boldsymbol{X}+\boldsymbol{Z}_e'\right) \tag{8}$$

where $\boldsymbol{X}$ is Gaussian with zero mean and covariance matrix $\boldsymbol{K}_x$ with

$$\mathcal{K}_x = \{\boldsymbol{K}_x : \boldsymbol{K}_x \succeq 0, \mathrm{Tr}(\boldsymbol{K}_x) \le P\}$$

and $\left(\boldsymbol{Z}_r', \boldsymbol{Z}_e'\right)$ is Gaussian with zero mean and joint covariance matrix $\boldsymbol{K}_\phi$ with

$$\mathcal{K}_\phi = \left\{\boldsymbol{K}_\phi : \boldsymbol{K}_\phi = \begin{bmatrix} \boldsymbol{I}_{n_r} & \boldsymbol{\phi} \\ \boldsymbol{\phi}^t & \boldsymbol{I}_{n_e} \end{bmatrix}, \boldsymbol{K}_\phi \succeq 0\right\}.$$

Here, $\boldsymbol{I}_n$ denotes the identity matrix of size $n \times n$, and $\succeq$ denotes an order between two real symmetric matrices such that $\boldsymbol{A} \succeq \boldsymbol{B}$ means that $\boldsymbol{A} - \boldsymbol{B}$ is positive semidefinite.

On the other hand, by letting $U = \boldsymbol{X}$ be Gaussian with zero mean and covariance matrix $\boldsymbol{K}_x$ in (3), it is easy to see that the following secrecy rate is achievable:

$$\max_{\boldsymbol{K}_x \in \mathcal{K}_x} \left(\frac{1}{2}\log\left|\boldsymbol{H}_r\boldsymbol{K}_x\boldsymbol{H}_r^t + \boldsymbol{I}_{n_r}\right| - \frac{1}{2}\log\left|\boldsymbol{H}_e\boldsymbol{K}_x\boldsymbol{H}_e^t + \boldsymbol{I}_{n_e}\right|\right). \tag{9}$$

Khisti and Wornell [3] and Oggier and Hassibi [4] compared the value of the optimization problems (8) and (9) and showed that they are *identical*, thus establishing the optimality of both matrix characterizations. Operationally, Khisti and Wornell [3] and Oggier and Hassibi [4] showed that the original multiple-antenna wiretap channel (1) has the same secrecy capacity as when the legitimate recipient has access to both received signals, minimized over all possible correlations between them. Considering the disparity between these two physical scenarios, this is a rather surprising result.

The approach of Khisti and Wornell [3] and Oggier and Hassibi [4] also reminded us of the degraded–same–marginal bound [11], [12] for the *capacity region* of the multiple-antenna broadcast channel. There, the optimality of Gaussian codebooks is hard to come by and a precise characterization of the capacity region had to wait until the proposal of a very different approach by Weingarten *et al.* [13]. Motivated by [13], this paper presents a different approach to characterize the secrecy capacity of the multiple-antenna wiretap channel under a more general matrix constraint on the channel input. Compared with that of Khisti and Wornell [3] and Oggier and Hassibi [4], our approach is by nature information—rather than matrix—theoretic and is directly built on the intuition regarding the optimal transmission strategy in this communication scenario.

II. Capacity Characterization Via a Channel-Enhancement Argument

To characterize the secrecy capacity of the multiple-antenna wiretap channel (1), we will first consider the special case where the channel matrices $\boldsymbol{H}_r$ and $\boldsymbol{H}_e$ are square $(n_t = n_r = n_e)$ and invertible. In this case, the channel model (1) can be equivalently written as

$$\begin{aligned} \boldsymbol{y}_r[m] &= \boldsymbol{x}[m] + \boldsymbol{z}_r[m] \\ \boldsymbol{y}_e[m] &= \boldsymbol{x}[m] + \boldsymbol{z}_e[m] \end{aligned} \tag{10}$$

where $\boldsymbol{z}_r[m]$ and $\boldsymbol{z}_e[m]$ are additive Gaussian noise vectors with zero means and covariance matrices

$$\boldsymbol{K}_r = \boldsymbol{H}_r^{-1}\boldsymbol{H}_r^{-t} \quad \text{and} \quad \boldsymbol{K}_e = \boldsymbol{H}_e^{-1}\boldsymbol{H}_e^{-t}$$

respectively and are independent across the time index m. Note that the noise covariance matrices $\boldsymbol{K}_r$ and $\boldsymbol{K}_e$ are (strictly) positive definite. In this paper, the channel model (10) is referred to as vector Gaussian wiretap channel. Rather than the average total power constraint (2), we will consider a matrix constraint on the channel input

$$\frac{1}{n}\sum_{m=1}^{n} \boldsymbol{x}[m]\boldsymbol{x}^t[m] \preceq \boldsymbol{S} \tag{11}$$

where $\boldsymbol{S}$ is a positive semidefinite matrix of size $n_t \times n_t$. As shown in [13, Lemma 1], the matrix constraint (11) is a more general constraint which subsumes the average total power constraint (2) as a special case.

Next, we will first focus on the vector Gaussian wiretap channel under the matrix constraint and provide a precise characterization of the secrecy capacity. We will then extend the result, through a limiting argument, to the more general multiple-antenna case under both matrix and average total power constraints.

A. Vector Gaussian Wiretap Channel

Let us first consider the case where the vector Gaussian wiretap channel is *degraded*. The following result is a natural extension of Leung and Hellman [5] on the scalar Gaussian wiretap channel.

Theorem 1 (Degraded Vector Gaussian Wiretap Channel): The secrecy capacity $C_s(\boldsymbol{S}, \boldsymbol{K}_r, \boldsymbol{K}_e)$ of the vector Gaussian wiretap channel (10) with degradedness order

$$\boldsymbol{K}_r \preceq \boldsymbol{K}_e \tag{12}$$

under the matrix constraint (11) is given by

$$C_s(\boldsymbol{S}, \boldsymbol{K}_r, \boldsymbol{K}_e) = \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{K}_r}{\boldsymbol{K}_r}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{K}_e}{\boldsymbol{K}_e}\right|. \tag{13}$$

Proof: Under the assumption (12), the vector Gaussian wiretap channel (10) is (stochastically) degraded. For degraded wiretap channels, Wyner [1] showed that $U = X$ is optimal in the single-letter secrecy capacity expression (3). Thus, the secrecy capacity $C_s(\boldsymbol{S}, \boldsymbol{K}_r, \boldsymbol{K}_e)$ of the vector Gaussian wiretap channel (10) is given by

$$\begin{aligned} &C_s(\boldsymbol{S}, \boldsymbol{K}_r, \boldsymbol{K}_e) \\ &\quad= \max_{E[\boldsymbol{X}X^t]\preceq\boldsymbol{S}} [I(\boldsymbol{X};\boldsymbol{Y}_r) - I(\boldsymbol{X};\boldsymbol{Y}_e)] \\ &\quad= \max_{E[\boldsymbol{X}X^t]\preceq\boldsymbol{S}} \{h(\boldsymbol{Y}_r) - h(\boldsymbol{Z}_r) - [h(\boldsymbol{Y}_e) - h(\boldsymbol{Z}_e)]\} \\ &\quad= \max_{E[\boldsymbol{X}X^t]\preceq\boldsymbol{S}} [h(\boldsymbol{Y}_r) - h(\boldsymbol{Y}_e)] - \frac{1}{2}\log\left|\frac{\boldsymbol{K}_r}{\boldsymbol{K}_e}\right|. \end{aligned} \tag{14}$$

Let $\boldsymbol{Z}$ be a Gaussian vector with zero mean and covariance matrix $\boldsymbol{K}_e - \boldsymbol{K}_r$. Assuming that $\boldsymbol{Z}$ is independent of $\boldsymbol{X}$ and $\boldsymbol{Z}_r$, we have

$$\begin{aligned} &\max_{E[\boldsymbol{X}X^t]\preceq\boldsymbol{S}} [h(\boldsymbol{Y}_r) - h(\boldsymbol{Y}_e)] \\ &\quad= \max_{E[\boldsymbol{X}X^t]\preceq\boldsymbol{S}} [h(\boldsymbol{X}+\boldsymbol{Z}_r) - h(\boldsymbol{X}+\boldsymbol{Z}_e)] \\ &\quad= \max_{E[\boldsymbol{X}X^t]\preceq\boldsymbol{S}} [h(\boldsymbol{X}+\boldsymbol{Z}_r) - h(\boldsymbol{X}+\boldsymbol{Z}_r+\boldsymbol{Z})] \\ &\quad= -\min_{E[\boldsymbol{X}X^t]\preceq\boldsymbol{S}} I(\boldsymbol{Z};\boldsymbol{X}+\boldsymbol{Z}_r+\boldsymbol{Z}) \\ &\quad= -\min_{0\preceq\boldsymbol{K}_x\preceq\boldsymbol{S}} \frac{1}{2}\log\left|\boldsymbol{I}_{n_t} + (\boldsymbol{K}_e-\boldsymbol{K}_r)(\boldsymbol{K}_x+\boldsymbol{K}_r)^{-1}\right| \qquad (15) \\ &\quad= -\frac{1}{2}\log\left|\boldsymbol{I}_{n_t} + (\boldsymbol{K}_e-\boldsymbol{K}_r)(\boldsymbol{S}+\boldsymbol{K}_r)^{-1}\right| \\ &\quad= \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{K}_r}{\boldsymbol{S}+\boldsymbol{K}_e}\right| \qquad (16) \end{aligned}$$

where (15) follows from the worst additive noise result of Diggavi and Cover [14, Lemma II.2]. Substituting (16) into (14) completes the proof of the theorem. □

Next, we use a *channel-enhancement* argument to lift the result of Theorem 1 to the general case. Channel-enhancement argument was first introduced by Weingarten *et al.* [13] to characterize the capacity region of the multiple-antenna broadcast channel with private messages. Proper modifications are made to fit our purposes here. The difference between the channel-enhancement argument here and that of Weingarten *et al.* [13] will be discussed in the next section. The main result is summarized in the following theorem.

Theorem 2 (General Vector Gaussian Wiretap Channel): The secrecy capacity $C_s(\boldsymbol{S}, \boldsymbol{K}_r, \boldsymbol{K}_e)$ of the general vector Gaussian wiretap channel (10) under the matrix constraint (11) is given by

$$\begin{aligned} &C_s(\boldsymbol{S}, \boldsymbol{K}_r, \boldsymbol{K}_e) \\ &= \max_{0\preceq\boldsymbol{K}_x\preceq\boldsymbol{S}} \left(\frac{1}{2}\log\left|\frac{\boldsymbol{K}_x+\boldsymbol{K}_r}{\boldsymbol{K}_r}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{K}_x+\boldsymbol{K}_e}{\boldsymbol{K}_e}\right|\right). \end{aligned} \tag{17}$$

Proof: Let $\boldsymbol{K}_x^*$ be an optimal solution to the matrix optimization problem on the right-hand side of (17). Then, $\boldsymbol{K}_x^*$ must satisfy the following Karush–Kuhn–Tucker (KKT) conditions:[2]

$$(\boldsymbol{K}_x^* + \boldsymbol{K}_r)^{-1} + \boldsymbol{M}_1 = (\boldsymbol{K}_x^* + \boldsymbol{K}_e)^{-1} + \boldsymbol{M}_2 \tag{18}$$

$$\boldsymbol{K}_x^* \boldsymbol{M}_1 = 0 \tag{19}$$

$$(\boldsymbol{S} - \boldsymbol{K}_x^*)\boldsymbol{M}_2 = 0 \tag{20}$$

where $\boldsymbol{M}_1$ and $\boldsymbol{M}_2$ are positive semidefinite matrices. By choosing $U = \boldsymbol{X}$ to be Gaussian with zero mean and covariance matrix $\boldsymbol{K}_x^*$, we have from the single-letter secrecy capacity expression (3)

$$C_s(\boldsymbol{S}, \boldsymbol{K}_r, \boldsymbol{K}_e) \geq \frac{1}{2}\log\left|\frac{\boldsymbol{K}_x^*+\boldsymbol{K}_r}{\boldsymbol{K}_r}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{K}_x^*+\boldsymbol{K}_e}{\boldsymbol{K}_e}\right|.$$

To prove the reversed inequality, let $\tilde{\boldsymbol{K}}_r$ be a real symmetric matrix such that

$$\left(\boldsymbol{K}_x^* + \tilde{\boldsymbol{K}}_r\right)^{-1} = (\boldsymbol{K}_x^* + \boldsymbol{K}_r)^{-1} + \boldsymbol{M}_1. \tag{21}$$

By the KKT condition (19), $\tilde{\boldsymbol{K}}_r$ can be explicitly calculated as

$$\tilde{\boldsymbol{K}}_r = \left(\boldsymbol{K}_r^{-1} + \boldsymbol{M}_1\right)^{-1}. \tag{22}$$

Since $\boldsymbol{M}_1 \succeq 0$, we have

$$0 \prec \tilde{\boldsymbol{K}}_r \preceq \boldsymbol{K}_r. \tag{23}$$

Substituting (21) into the KKT condition (18), we may obtain

$$\left(\boldsymbol{K}_x^* + \tilde{\boldsymbol{K}}_r\right)^{-1} = (\boldsymbol{K}_x^* + \boldsymbol{K}_e)^{-1} + \boldsymbol{M}_2. \tag{24}$$

[2]As this optimization problem is not necessarily convex, a set of constraint qualifications (CQs) should be verified to make sure that the KKT conditions indeed hold. The CQs stated in [13, Appendix D] hold in a trivial manner for this optimization problem.

Since $\boldsymbol{M}_2 \succeq 0$, we have

$$\tilde{\boldsymbol{K}}_r \preceq \boldsymbol{K}_e. \tag{25}$$

Now consider the following enhanced vector Gaussian wiretap channel:

$$\begin{aligned} \tilde{\boldsymbol{y}}_r[m] &= \boldsymbol{x}[m] + \tilde{\boldsymbol{z}}_r[m] \\ \boldsymbol{y}_e[m] &= \boldsymbol{x}[m] + \boldsymbol{z}_e[m] \end{aligned} \tag{26}$$

where $\tilde{\boldsymbol{z}}_r[m]$ and $\boldsymbol{z}_e[m]$ are additive Gaussian noise vectors with zero means and covariance matrices $\tilde{\boldsymbol{K}}_r$ and $\boldsymbol{K}_e$, respectively, and are independent across the time index m. By (23), the noise covariance matrix of the legitimate recipient in the enhanced channel (26) is *reduced* from $\boldsymbol{K}_r$ to $\tilde{\boldsymbol{K}}_r$ as in the original channel (10). Since reducing the noise covariance of the legitimate recipient can only increase the secrecy capacity, we have

$$C_s(\boldsymbol{S}, \boldsymbol{K}_r, \boldsymbol{K}_e) \le C_s(\boldsymbol{S}, \tilde{\boldsymbol{K}}_r, \boldsymbol{K}_e) \tag{27}$$

where $C_s(\boldsymbol{S}, \tilde{\boldsymbol{K}}_r, \boldsymbol{K}_e)$ denotes the secrecy capacity of the enhanced channel (26) under the matrix constraint (11). Furthermore, by (25), the enhanced vector Gaussian wiretap channel (26) is degraded. Thus, by Theorem 1

$$C_s(\boldsymbol{S}, \tilde{\boldsymbol{K}}_r, \boldsymbol{K}_e) = \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\tilde{\boldsymbol{K}}_r}{\tilde{\boldsymbol{K}}_r}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{K}_e}{\boldsymbol{K}_e}\right|. \tag{28}$$

Note that

$$\begin{aligned} &(\boldsymbol{S}+\tilde{\boldsymbol{K}}_r)\left(\boldsymbol{K}_x^*+\tilde{\boldsymbol{K}}_r\right)^{-1} \\ &= \left[\boldsymbol{S}-\boldsymbol{K}_x^*+\left(\boldsymbol{K}_x^*+\tilde{\boldsymbol{K}}_r\right)\right]\left(\boldsymbol{K}_x^*+\tilde{\boldsymbol{K}}_r\right)^{-1} \\ &= (\boldsymbol{S}-\boldsymbol{K}_x^*)\left(\boldsymbol{K}_x^*+\tilde{\boldsymbol{K}}_r\right)^{-1} + \boldsymbol{I}_{n_t} \\ &= (\boldsymbol{S}-\boldsymbol{K}_x^*)\left[(\boldsymbol{K}_x^*+\boldsymbol{K}_e)^{-1}+\boldsymbol{M}_2\right] + \boldsymbol{I}_{n_t} \qquad (29) \\ &= (\boldsymbol{S}-\boldsymbol{K}_x^*)(\boldsymbol{K}_x^*+\boldsymbol{K}_e)^{-1} + \boldsymbol{I}_{n_t} \qquad (30) \\ &= [\boldsymbol{S}-\boldsymbol{K}_x^*+(\boldsymbol{K}_x^*+\boldsymbol{K}_e)](\boldsymbol{K}_x^*+\boldsymbol{K}_e)^{-1} \\ &= (\boldsymbol{S}+\boldsymbol{K}_e)(\boldsymbol{K}_x^*+\boldsymbol{K}_e)^{-1} \end{aligned}$$

where (29) follows from (24), and (30) follows from the KKT condition (20). Thus

$$\left|\frac{\boldsymbol{S}+\tilde{\boldsymbol{K}}_r}{\boldsymbol{S}+\boldsymbol{K}_e}\right| = \left|\frac{\boldsymbol{K}_x^*+\tilde{\boldsymbol{K}}_r}{\boldsymbol{K}_x^*+\boldsymbol{K}_e}\right|. \tag{31}$$

Similarly

$$\begin{aligned} \left(\boldsymbol{K}_x^*+\tilde{\boldsymbol{K}}_r\right)\tilde{\boldsymbol{K}}_r^{-1} &= \boldsymbol{K}_x^*\tilde{\boldsymbol{K}}_r^{-1} + \boldsymbol{I}_{n_t} \\ &= \boldsymbol{K}_x^*\left(\boldsymbol{K}_r^{-1}+\boldsymbol{M}_1\right) + \boldsymbol{I}_{n_t} \qquad (32) \\ &= \boldsymbol{K}_x^*\boldsymbol{K}_r^{-1} + \boldsymbol{I}_{n_t} \qquad (33) \\ &= (\boldsymbol{K}_x^*+\boldsymbol{K}_r)\boldsymbol{K}_r^{-1} \end{aligned}$$

where (32) follows from (22), and (33) follows from the KKT condition (19). Therefore

$$\left|\frac{\boldsymbol{K}_x^*+\tilde{\boldsymbol{K}}_r}{\tilde{\boldsymbol{K}}_r}\right| = \left|\frac{\boldsymbol{K}_x^*+\boldsymbol{K}_r}{\boldsymbol{K}_r}\right|. \tag{34}$$

Substituting (31) and (34) into (28), we may obtain

$$\begin{aligned} C_s(\boldsymbol{S}, \tilde{\boldsymbol{K}}_r, \boldsymbol{K}_e) &= \frac{1}{2}\log\left(\left|\frac{\boldsymbol{S}+\tilde{\boldsymbol{K}}_r}{\boldsymbol{S}+\boldsymbol{K}_e}\right|\left|\frac{\boldsymbol{K}_e}{\tilde{\boldsymbol{K}}_r}\right|\right) \\ &= \frac{1}{2}\log\left(\left|\frac{\boldsymbol{K}_x^*+\tilde{\boldsymbol{K}}_r}{\boldsymbol{K}_x^*+\boldsymbol{K}_e}\right|\left|\frac{\boldsymbol{K}_e}{\tilde{\boldsymbol{K}}_r}\right|\right) \\ &= \frac{1}{2}\log\left(\left|\frac{\boldsymbol{K}_x^*+\tilde{\boldsymbol{K}}_r}{\tilde{\boldsymbol{K}}_r}\right|\left|\frac{\boldsymbol{K}_e}{\boldsymbol{K}_x^*+\boldsymbol{K}_e}\right|\right) \\ &= \frac{1}{2}\log\left(\left|\frac{\boldsymbol{K}_x^*+\boldsymbol{K}_r}{\boldsymbol{K}_r}\right|\left|\frac{\boldsymbol{K}_e}{\boldsymbol{K}_x^*+\boldsymbol{K}_e}\right|\right) \\ &= \frac{1}{2}\log\left|\frac{\boldsymbol{K}_x^*+\boldsymbol{K}_r}{\boldsymbol{K}_r}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{K}_x^*+\boldsymbol{K}_e}{\boldsymbol{K}_e}\right|. \end{aligned} \tag{35}$$

Putting together (27) and (35), we obtain the desired reverse inequality

$$C_s(\boldsymbol{S}, \boldsymbol{K}_r, \boldsymbol{K}_e) \le \frac{1}{2}\log\left|\frac{\boldsymbol{K}_x^*+\boldsymbol{K}_r}{\boldsymbol{K}_r}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{K}_x^*+\boldsymbol{K}_e}{\boldsymbol{K}_e}\right|.$$

This completes the proof of the theorem. □

B. Multiple-Antenna Wiretap Channel

Finally, We extend the secrecy capacity result of Theorem 2 for the general vector Gaussian wiretap channel to the multiple-antenna wiretap channel. The main ideas of the proof are borrowed from [13, Sec.V-B] with proper adaptations.

Theorem 3 (Multiple-Antenna Wiretap Channel): The secrecy capacity $C_s(\boldsymbol{S}, \boldsymbol{H}_r, \boldsymbol{H}_e)$ of the multiple-antenna wiretap channel (1) under the matrix constraint (11) is given by

$$\begin{aligned} C_s(\boldsymbol{S}, \boldsymbol{H}_r, \boldsymbol{H}_e) = \max_{0\preceq\boldsymbol{K}_x\preceq\boldsymbol{S}} \Bigg(&\frac{1}{2}\log\left|\boldsymbol{H}_r\boldsymbol{K}_x\boldsymbol{H}_r^t + \boldsymbol{I}_{n_r}\right| \\ &-\frac{1}{2}\log\left|\boldsymbol{H}_e\boldsymbol{K}_x\boldsymbol{H}_e^t + \boldsymbol{I}_{n_e}\right|\Bigg). \end{aligned} \tag{36}$$

Proof: By choosing $U = \boldsymbol{X}$ to be Gaussian in (3), it is clear that the secrecy rate

$$\frac{1}{2}\log\left|\boldsymbol{H}_r\boldsymbol{K}_x\boldsymbol{H}_r^t + \boldsymbol{I}_{n_r}\right| - \frac{1}{2}\log\left|\boldsymbol{H}_e\boldsymbol{K}_x\boldsymbol{H}_e^t + \boldsymbol{I}_{n_e}\right|$$

is achievable for any $0 \preceq \boldsymbol{K}_x \preceq \boldsymbol{S}$. We therefore concentrate on proving the converse result. As mentioned previously, the case when both channel matrices $\boldsymbol{H}_r$ and $\boldsymbol{H}_e$ are square and invertible can be easily transformed into a vector Gaussian wiretap channel and thus Theorem 2 completes the proof. Our goal next is to *approximate* a multiple-antenna wiretap channel with general channel matrices by one with invertible channel matrices.

Without loss of generality, we may assume that the channel matrices $\boldsymbol{H}_r$ and $\boldsymbol{H}_e$ are square (but not necessarily invertible). If that is not the case, we can use singular value decomposition (SVD) to show that there is an equivalent channel which does have $n_t \times n_t$ square channel matrices. That is, we may find a new channel with square channel matrices which are derived from the original ones via matrix multiplications. The new channel is equivalent to the original one in preserving the secrecy capacity under the same input constraint. Consider using SVD to write the channel matrices as follows:

$$\boldsymbol{H}_r = \boldsymbol{U}_r \boldsymbol{\Lambda}_r \boldsymbol{V}_r^t \quad \text{and} \quad \boldsymbol{H}_e = \boldsymbol{U}_e \boldsymbol{\Lambda}_e \boldsymbol{V}_e^t$$

where $\boldsymbol{U}_r, \boldsymbol{V}_r, \boldsymbol{U}_e$, and $\boldsymbol{V}_e$ are $n_t \times n_t$ orthogonal matrices, and $\boldsymbol{\Lambda}_r$ and $\boldsymbol{\Lambda}_e$ are diagonal. We now define a new multiple-antenna wiretap channel which has invertible channel matrices

$$\begin{aligned} \overline{\boldsymbol{y}}_r[m] &= \overline{\boldsymbol{H}}_r \boldsymbol{x}[m] + \boldsymbol{z}_r[m] \\ \overline{\boldsymbol{y}}_e[m] &= \overline{\boldsymbol{H}}_e \boldsymbol{x}[m] + \boldsymbol{z}_e[m] \end{aligned} \tag{37}$$

where

$$\overline{\boldsymbol{H}}_r = \boldsymbol{U}_r(\boldsymbol{\Lambda}_r + \alpha \boldsymbol{I}_{n_t})\boldsymbol{V}_r^t \quad \text{and} \quad \overline{\boldsymbol{H}}_e = \boldsymbol{U}_e(\boldsymbol{\Lambda}_e + \alpha \boldsymbol{I}_{n_t})\boldsymbol{V}_e^t$$

for some $\alpha > 0$. Note that the multiple-antenna wiretap channel (37) does have invertible channel matrices. Therefore, the secrecy capacity, $C_s(\boldsymbol{S}, \overline{\boldsymbol{H}}_r, \overline{\boldsymbol{H}}_e)$, under the matrix constraint (11) is given by

$$C_s(\boldsymbol{S}, \overline{\boldsymbol{H}}_r, \overline{\boldsymbol{H}}_e) = \max_{0 \preceq \boldsymbol{K}_x \preceq \boldsymbol{S}} \left(\frac{1}{2} \log \left| \overline{\boldsymbol{H}}_r \boldsymbol{K}_x \overline{\boldsymbol{H}}_r^t + \boldsymbol{I}_{n_t} \right| - \frac{1}{2} \log \left| \overline{\boldsymbol{H}}_e \boldsymbol{K}_x \overline{\boldsymbol{H}}_e^t + \boldsymbol{I}_{n_t} \right| \right).$$

Further note that we can write $\boldsymbol{H}_r = \boldsymbol{D}_r \overline{\boldsymbol{H}}_r$ where

$$\boldsymbol{D}_r = \boldsymbol{U}_r \boldsymbol{\Lambda}_r (\boldsymbol{\Lambda}_r + \alpha \boldsymbol{I}_{n_t})^{-1} \boldsymbol{U}_r^t.$$

Since $\boldsymbol{D}_r \boldsymbol{D}_r^t \prec \boldsymbol{I}_{n_t}$, we have

$$\boldsymbol{X} \to \overline{\boldsymbol{Y}}_r \to \boldsymbol{Y}_r \tag{38}$$

forms a Markov chain. Similarly, it can be shown that

$$\boldsymbol{X} \to \overline{\boldsymbol{Y}}_e \to \boldsymbol{Y}_e \tag{39}$$

also forms a Markov chain. Therefore, both the legitimate recipient and the eavesdropper receive a better signal in the new channel (37) than in the original channel (1). Unlike the private message problem considered in [13], here the enhancement of both channels does not necessarily lead to an increase in secrecy capacity. However, we can bound the difference between the secrecy capacity $C_s(\boldsymbol{S}, \boldsymbol{H}_r, \boldsymbol{H}_e)$ of the original multiple-antenna wiretap channel (1) and $C_s(\boldsymbol{S}, \overline{\boldsymbol{H}}_r, \overline{\boldsymbol{H}}_e)$ of the new multiple-antenna wiretap channel (37) under the same matrix constraint (11) as follows:

$$\begin{aligned} &C_s(\boldsymbol{S}, \boldsymbol{H}_r, \boldsymbol{H}_e) - C_s(\boldsymbol{S}, \overline{\boldsymbol{H}}_r, \overline{\boldsymbol{H}}_e) \\ &\quad = \max_{p(U,\boldsymbol{X})} [I(U;\boldsymbol{Y}_r) - I(U;\boldsymbol{Y}_e)] \\ &\qquad - \max_{p(U,\boldsymbol{X})} [I(U;\overline{\boldsymbol{Y}}_r) - I(U;\overline{\boldsymbol{Y}}_e)] \end{aligned} \tag{40}$$

$$\begin{aligned} &\le \max_{p(U,\boldsymbol{X})} \{I(U;\boldsymbol{Y}_r) - I(U;\boldsymbol{Y}_e) \\ &\qquad - [I(U;\overline{\boldsymbol{Y}}_r) - I(U;\overline{\boldsymbol{Y}}_e)]\} \\ &= \max_{p(U,\boldsymbol{X})} \{I(U;\overline{\boldsymbol{Y}}_e) - I(U;\boldsymbol{Y}_e) \\ &\qquad - [I(U;\overline{\boldsymbol{Y}}_r) - I(U;\boldsymbol{Y}_r)]\} \\ &\le \max_{p(U,\boldsymbol{X})} [I(U;\overline{\boldsymbol{Y}}_e) - I(U;\boldsymbol{Y}_e)] \end{aligned} \tag{41}$$

$$= \max_{p(\boldsymbol{X})} [I(\boldsymbol{X};\overline{\boldsymbol{Y}}_e) - I(\boldsymbol{X};\boldsymbol{Y}_e)] \tag{42}$$

$$= \max_{p(\boldsymbol{X})} I(\boldsymbol{X};\overline{\boldsymbol{Y}}_e|\boldsymbol{Y}_e) \tag{43}$$

$$\le \frac{1}{2} \log \left| \overline{\boldsymbol{H}}_e \boldsymbol{S} \overline{\boldsymbol{H}}_e^t + \boldsymbol{I}_{n_t} \right| - \frac{1}{2} \log \left| \boldsymbol{H}_e \boldsymbol{S} \boldsymbol{H}_e^t + \boldsymbol{I}_{n_t} \right| \tag{44}$$

where (40) follows from the single-letter secrecy capacity expression (3); (41) follows from the Markov relation (38) so $I(U;\overline{\boldsymbol{Y}}_r) - I(U;\boldsymbol{Y}_r) \ge 0$; (42) follows from the Markov relation (39) so $U = \boldsymbol{X}$ is optimal; (43) follows, again, from the Markov relation (39); and finally, (44) follows from an inequality due to Thomas [17, Lemma 1]. Thus, for any $\alpha > 0$ we have

$$\begin{aligned} &C_s(\boldsymbol{S}, \boldsymbol{H}_r, \boldsymbol{H}_e) \le C_s(\boldsymbol{S}, \overline{\boldsymbol{H}}_r, \overline{\boldsymbol{H}}_e) \\ &\quad + \left(\frac{1}{2} \log \left| \overline{\boldsymbol{H}}_e \boldsymbol{S} \overline{\boldsymbol{H}}_e^t + \boldsymbol{I}_{n_t} \right| - \frac{1}{2} \log \left| \boldsymbol{H}_e \boldsymbol{S} \boldsymbol{H}_e^t + \boldsymbol{I}_{n_t} \right| \right). \end{aligned} \tag{45}$$

As $\alpha \downarrow 0$, we have $\overline{\boldsymbol{H}}_r \to \boldsymbol{H}_r$ and $\overline{\boldsymbol{H}}_e \to \boldsymbol{H}_e$ and hence

$$\frac{1}{2} \log \left| \overline{\boldsymbol{H}}_e \boldsymbol{S} \overline{\boldsymbol{H}}_e^t + \boldsymbol{I}_{n_t} \right| - \frac{1}{2} \log \left| \boldsymbol{H}_e \boldsymbol{S} \boldsymbol{H}_e^t + \boldsymbol{I}_{n_t} \right| \to 0 \tag{46}$$

and

$$C_s(\boldsymbol{S}, \overline{\boldsymbol{H}}_r, \overline{\boldsymbol{H}}_e) \to \max_{0 \preceq \boldsymbol{K}_x \preceq \boldsymbol{S}} \left(\frac{1}{2} \log \left| \boldsymbol{H}_r \boldsymbol{K}_x \boldsymbol{H}_r^t + \boldsymbol{I}_{n_t} \right| - \frac{1}{2} \log \left| \boldsymbol{H}_e \boldsymbol{K}_x \boldsymbol{H}_e^t + \boldsymbol{I}_{n_t} \right| \right). \tag{47}$$

Letting $\alpha \downarrow 0$, we conclude from (45), (46), and (47) that

$$C_s(\boldsymbol{S}, \boldsymbol{H}_r, \boldsymbol{H}_e) \le \max_{0 \preceq \boldsymbol{K}_x \preceq \boldsymbol{S}} \left(\frac{1}{2} \log \left| \boldsymbol{H}_r \boldsymbol{K}_x \boldsymbol{H}_r^t + \boldsymbol{I}_{n_t} \right| - \frac{1}{2} \log \left| \boldsymbol{H}_e \boldsymbol{K}_x \boldsymbol{H}_e^t + \boldsymbol{I}_{n_t} \right| \right).$$

This is the desired converse result, which completes the proof of the theorem. □

The following corollary, which characterizes the secrecy capacity of the multiple-antenna wiretap channel under the average total power constraint, is an immediate consequence of Theorem 3 and [13, Lemma 1].

Corollary 1 ([3], [4]): The secrecy capacity $C_s(P, \boldsymbol{H}_r, \boldsymbol{H}_e)$ of the multiple-antenna wiretap channel (1) under the average total power constraint (2) is given by

$$C_s(P, \boldsymbol{H}_r, \boldsymbol{H}_e) = \max_{\boldsymbol{K}_x \succeq 0, \mathrm{Tr}(\boldsymbol{K}_x) \le P} \left(\frac{1}{2} \log \left| \boldsymbol{H}_r \boldsymbol{K}_x \boldsymbol{H}_r^t + \boldsymbol{I}_{n_r} \right| - \frac{1}{2} \log \left| \boldsymbol{H}_e \boldsymbol{K}_x \boldsymbol{H}_e^t + \boldsymbol{I}_{n_e} \right| \right). \tag{48}$$

III. Intuitions on the Enhanced Channel

In this paper, our approach of characterizing the secrecy capacity of the vector Gaussian wiretap channel hinges on the existence of the enhanced channel which needs to satisfy the following conditions:

1) it is degraded, so the secrecy capacity can be readily characterized as in Theorem 1; and
2) it has the same secrecy capacity as the original wiretap channel.

A priori, it is not clear whether such an enhanced channel would always exist, letting alone actually construct one.

Our intuition regarding the existence of the enhanced channel was mainly from the parallel Gaussian wiretap channel model, which can be seen as a special case of the vector Gaussian wiretap channel with *diagonal* noise covariance matrices. For the parallel Gaussian wiretap channel, it was shown in [15], [16] that the optimal transmission strategy is to transmit independently over the subchannels for which the legitimate recipient receives a better signal than the eavesdropper. Therefore, an enhanced channel can be constructed by reducing the noise variances for the legitimate recipient in each of the subchannels to the noise level of the eavesdropper. Clearly, the enhanced channel so constructed is degraded: the signal received by the legitimate recipient is at least as good as that received by the eavesdropper in each of the subchannels. Furthermore, the secrecy capacity of the enhanced channel is the same as the original channel, as the noise variance for the legitimate recipient does not change at all for any of the "active" subchannels and at the same time the "inactive" subchannels remains "inactive." Therefore, at least for the special case of parallel Gaussian wiretap channel the enhanced channel always exists.

Carrying over to the vector Gaussian wiretap channel, no information should be transmitted along any directions where the eavesdropper observes a stronger signal than the legitimate recipient. (This intuition was separately confirmed by Khisti and Wornell [3] and Oggier and Hassibi [4].) Thus, the effective channel for the eavesdropper must be degraded with respect to the effective channel for the legitimate recipient. However, in a vector Gaussian wiretap channel, the noise covariance matrices for the legitimate recipient and the eavesdropper may not always have the same eigendirections. Therefore, finding the enhanced channel (by reducing "just" enough the noise covariance for the legitimate recipient) is much more involved than in the parallel case. Our construction in this paper was motivated by the construction of the enhanced channel of Weingarten *et al.* [13] for the vector Gaussian broadcast channel problem with private messages.

Finally, recall that in their constructions Weingarten *et al.* [13] enhanced every transmitter–receiver channels (by reducing the corresponding noise covariance). In our construction, however, we only enhanced the channel to the legitimate recipient. (The transmitter–eavesdropper channel remained unchanged, cf. the channel model (26).) This is due to the fact that in both arguments, the enhancement must increase, *a priori*, the capacity (secrecy or regular) of the channel. (Otherwise, both arguments would break down.) Whereas reducing the noise covariances will benefit all the receivers and hence improve the private message capacity of the vector Gaussian broadcast channel, reducing the noise covariance of the eavesdropper may compromise the security of the transmission scheme and hence lower the secrecy capacity of the vector Gaussian wiretap channel. This is a key difference between the channel enhancement argument here and that of Weingarten *et al.* [13] for the vector Gaussian broadcast channel problem with private messages.

Acknowledgment

The authors wish to thank Ashish Khisti and Greg Wornell from MIT, Babak Hassibi from Caltech, and the Associate Editor for their comments on an earlier version of this paper.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MIMOME channel," *IEEE Trans. Inf. Theory*, to be published.
[4] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, ON, Canada, Jul. 2008, pp. 524–528.
[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.
[6] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiely, 1991.
[7] D. Guo, S. Shamai (Shitz), and S. Verdú, "Properties of the MMSE in Gaussian channels with applications," in preparation.
[8] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel," *IEEE Trans. Inf. Theory*, to be published.
[9] A. Khisti, G. W. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, Jun. 2007, pp. 2471–2475.
[10] H. Sato, "An outer bound to the capacity region of broadcast channels," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 374–377, May 1978.
[11] S. Vishwanath, G. Kramer, S. Shamai (Shitz), S. Jafar, and A. Goldsmith, "Capacity bounds for Gaussian vector broadcast channels," in *Multiantenna Channels: Capacity, Coding and Signal Processing*, G. J. Foschini and S. Verdú, Eds. Providence, RI: DIMACS, 2003, pp. 107–122.
[12] D. N. C. Tse and P. Viswanath, "On the capacity of the multiple antenna broadcast channel," in *Multiantenna Channels: Capacity, Coding and Signal Processing*, G. J. Foschini and S. Verdú, Eds. Providence, RI: DIMACS, 2003, pp. 87–105.
[13] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "The capacity region of the Gaussian multiple-input-multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.
[14] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3072–3081, Nov. 2001.
[15] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. 44th Annu. Allerton Conf. Communications, Control, and Computing*, Monticello, IL, Sep. 2006, pp. 841–848.
[16] 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, Jun. 2008.
[17] J. A. Thomas, "Feedback can at most double Gaussian multiple access channel capacity," *IEEE Trans. Inf. Theory*, vol. IT-33, no. 5, pp. 711–716, Sep. 1987.

Tie Liu (S'99–M'06) received the B.S. (1998) and M.S. (2000) degrees, both in electrical engineering, from the Tsinghua University, Beijing, China, and the M.S. degree in mathematics (2004) and Ph.D. degree in electrical and computer engineering (2006) from the University of Illinois at Urbana-Champaign.

Since August 2006, he has been with the Texas A&M University, College Station, where he is currently an Assistant Professor in Electrical and Computer Engineering. His research interests are in the field of information theory, wireless communication, and signal processing.

Prof. Liu is a recipient of the M. E. Van Valkenburg Graduate Research Award (2006) from the University of Illinois at Urbana-Champaign and the Best Paper Award (2008) from the Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications.

Shlomo Shamai (Shitz) (S'82–M'85–SM'88–F'94) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Technion–Israel Institute of Technology, Haifa, Israel, in 1975, 1981, and 1986, respectively.

During 1975–1985, he was with the Communications Research Labs in the capacity of a Senior Research Engineer. Since 1986 he has been with the Department of Electrical Engineering, Technion–Israel Institute of Technology, where he is now the William Fondiller Professor of Telecommunications. His research interests encompasses a wide spectrum of topics in information theory and statistical communications.

Dr. Shamai (Shitz) is a member of the Union Radio Scientifique Internationale (URSI). He is the recipient of the 1999 van der Pol Gold Medal of URSI, and a corecipient of the 2000 IEEE Donald G. Fink Prize Paper Award, the 2003 and the 2004 joint IT/COM societies paper awards, and the 2007 IEEE Information Theory Society Paper Award. He is also the recipient of 1985 Alon Grant for distinguished young scientists and the 2000 Technion Henry Taub Prize for Excellence in Research. He has served as Associate Editor for the Shannon Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY, and also has been on the Board of Governors of the Information Theory Society.