CCIT Report #650 November 2007

A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel

Tie Liu and Shlomo Shamai (Shitz)

November 15, 2007

Abstract

The secrecy capacity of the multi-antenna wiretap channel was recently characterized independently by Khisti and Wornell [1] and Oggier and Hassibi [2] using a Sato-like argument and matrix analysis tools. This note presents an alternative characterization of the secrecy capacity of the multi-antenna wiretap channel using a channel enhancement argument. This characterization is by nature information rather than matrix theoretic, and is directly built on the physical intuition regarding to the optimal transmission strategy in this communication scenario. A secure V-BLAST transmission and receiver architecture is proposed to achieve the secrecy capacity of the multi-antenna wiretap channel.

1 Introduction

Consider a multi-antenna wiretap channel with n_t transmit antennas and n_r and n_e receive antennas at the legitimate recipient and the eavesdropper, respectively:

$$\begin{array}{rcl} \mathbf{y}_r[m] & = & \mathbf{H}_r\mathbf{x}[m] + \mathbf{w}_r[m] \\ \mathbf{y}_e[m] & = & \mathbf{H}_e\mathbf{x}[m] + \mathbf{w}_e[m] \end{array} \tag{1}$$

where $\mathbf{H}_r \in \mathbb{R}^{n_r \times n_t}$ and $\mathbf{H}_e \in \mathbb{R}^{n_e \times n_t}$ are the channel gain matrices associated with the legitimate recipient and the eavesdropper. The channel gain matrices $\mathbf{H}_r$ and $\mathbf{H}_e$ are assumed to be fixed during the entire transmission and are known to all three terminals. The additive noise $\mathbf{w}_r[m]$ and

$\mathbf{w}_e[m]$ are zero-mean i.i.d. Gaussian vectors with unit variance and are independent across the time index m. The channel input satisfies a total power constraint

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

The *secrecy capacity* 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 [3, 4].

For a discrete memoryless wiretap channel $P(Y_r, Y_e|X)$, a single-letter expression for the secrecy capacity was obtained by Csiszár and Körner [4] and can be written as

$$C_s = \max_{P(U,X)} \{I(U;Y_r) - I(U;Y_e)\} \tag{3}$$

where U is an auxiliary random variable over a certain alphabet that satisfies the Markov relation $U - X - (Y_r, Y_e)$. Moreover, (3) extends to continuous alphabet cases with power constraint, so the problem of characterizing the secrecy capacity of the multi-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 capacity expression (3) was successfully evaluated by Leung and Hellman [5] using a result of Wyner [3] on the degraded wiretap channel and the celebrated entropy-power inequality [6, Cha. 16.7]. (Alternatively, it can also be evaluated using Wyner's result [3] and a classical result from estimation theory via a relationship between mutual information and minimum mean-squared error estimation (MMSE) [7].) Unfortunately, the same approach does not extend to the multi-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 multi-antenna wiretap channel remained open until the recent work of Khisti and Wornell [1] and Oggier and Hassibi [2]. The special case of $n_t = n_r = 2$, $n_e = 1$ was independently settled by Shafiee et al. [8].

In their respective work, Khisti and Wornell [1] and Oggier and Hassibi [2] followed an indirect approach to evaluate the capacity expression (3) for the multi-antenna wiretap channel. Key to their evaluations is the following genie-aided upper bound:

$$\begin{aligned}
I(U;Y_r) - I(U;Y_e) &\le I(U;Y_r,Y_e) - I(U;Y_e) && (4)\\
&= I(X;Y_r,Y_e) - I(X;Y_e) - [I(X;Y_r,Y_e|U) - I(X;Y_e|U)] && (5)\\
&\le I(X;Y_r,Y_e) - I(X;Y_e) && (6)\\
&= I(X;Y_r|Y_e) && (7)
\end{aligned}$$

where (5) follows from the Markov chain $U - X - (Y_r, Y_e)$, and (6) follows from the trivial inequality $I(X; Y_r, Y_e|U) \geq I(X; Y_e|U)$. Khisti and Wornell [1] and Oggier and Hassibi [2] further 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 the marginals $P(Y_r|X)$ and $P(Y_e|X)$, whereas the upper bound $I(X; Y_r|Y_e)$ does depend on the *joint* conditional $P(Y_r, Y_e|X)$. A good upper bound on the secrecy capacity is thus contrived as:

$$C_s \leq \min_{P(Y_r', Y_e'|X) \in \mathcal{D}} \max_{P(X)} I(X; Y_r'|Y_e') \tag{8}$$

where $\mathcal{D}$ is a set of joint conditionals $P(Y_r', Y_e'|X)$ satisfying

$$P(Y_r'|X) = P(Y_r|X) \quad \text{and} \quad P(Y_e'|X) = P(Y_e|X). \tag{9}$$

The upper bound in (8) has a specific physical meaning: it is the secrecy capacity of the wiretap channel $P(Y_r', Y_e'|X)$ where the legitimate recipient has access to both Y_r' and Y_e', minimized over the worst cooperation between the legitimate recipient and the eavesdropper. In essence, this is very similar to the Sato upper bound on the sum capacity of a general broadcast channel [9]. For an additive Gaussian $P(Y_r', Y_e'|X)$, Khisti and Wornell [1] and Oggier and Hassibi [2] showed that the conditional mutual information $I(X; Y_r'|Y_e')$ is maximized when the channel input X is Gaussian. Hence, for the multi-antenna wiretap channel (1) the upper bound in (8) can be written as a matrix optimization problem. By comparing the value of the optimal *Gaussian* $U = X$ for the original optimization problem $\max_{P(U,X)}\{I(U; Y_r) - I(U; Y_e)\}$ with the upper bound in (8), Khisti and Wornell [1] and Oggier and Hassibi [2] showed that the results are *identical* and thus established the optimality of both matrix characterizations for the multi-antenna wiretap channel. Operationally, Khisti and Wornell [1] and Oggier and Hassibi [2] showed that the original multi-antenna wiretap channel has the same secrecy capacity as when the legitimate recipient has access to both received signals and optimized over the worst cooperation between the legitimate recipient and the eavesdropper. Considering the disparity between these two physical scenarios, this is a rather surprising result.

The approach of Khisti and Wornell [1] and Oggier and Hassibi [2] also reminded us of the degraded same marginals bound for the *capacity region* of the multi-antenna broadcast channel [10, 11]. 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. [12]. Motivated by the line of work on the multi-antenna broadcast channel, in this note we present a different approach to characterize the secrecy capacity of the multi-antenna wiretap channel. Compared with the approach of Khisti and Wornell [1] and Oggier and Hassibi [2], our approach is by nature information rather than matrix theoretic, and is directly built on the physical intuition regarding to the optimal transmission strategy in this communication scenario.

After formally characterizing the secrecy capacity of the multi-antenna wiretap channel in Section 2, a secure V-BLAST transmission and receiver architecture is proposed in Section 3, which we show to achieve the secrecy capacity of the multi-antenna wiretap channel.

2 Capacity Characterization via a Channel Enhancement Argument

2.1 Capacity characterization

We consider a canonical version of the channel (vector Gaussian wiretap channel)

$$\begin{aligned} \mathbf{y}_r[m] &= \mathbf{x}[m] + \mathbf{w}_r[m] \\ \mathbf{y}_e[m] &= \mathbf{x}[m] + \mathbf{w}_e[m], \end{aligned} \tag{10}$$

where $\mathbf{x}[m]$ is a real input vector of length t, and $\mathbf{w}_r[m]$ and $\mathbf{w}_e[m]$ are additive Gaussian noise vectors with zero mean and covariance matrix $\mathbf{K}_r$ and $\mathbf{K}_e$ respectively and are independent across the time index m. The noise covariance matrices $\mathbf{K}_r$ and $\mathbf{K}_e$ are assumed to be positive definite. The channel input satisfies a power-covariance constraint

$$\frac{1}{n}\sum_{m=1}^{n}\left(\mathbf{x}[m]\mathbf{x}^t[m]\right) \preceq \mathbf{S} \tag{11}$$

where $\mathbf{S}$ is a positive semidefinite matrix of size $t \times t$, and "$\preceq$" represents "less or equal to" in the positive semidefinite partial ordering between real symmetric matrices. Note that (11) is a rather general constraint that subsumes many other constraints including total and individual per antenna power constraints. Following [12], it can be shown that characterizing the secrecy capacity of the general multi-antenna wiretap channel (3) can be reduced to characterizing the canonical vector Gaussian wiretap channel (10). Without loss of generality, we shall focus on the vector Gaussian wiretap channel (10) with power-covariance constraint (11) for the rest of the note.

We first consider the secrecy capacity of a *degraded* vector Gaussian wiretap channel. The result is a natural extension of Leung and Hellman [5] for the scalar Gaussian wiretap channel.

Theorem 1: The secrecy capacity of a degraded vector Gaussian wiretap channel (10) with $\mathbf{K}_r \preceq \mathbf{K}_e$ and under the power covariance constraint (11) can be written as

$$C_s = \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{S}\mathbf{K}_r^{-1}\right) - \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{S}\mathbf{K}_e^{-1}\right). \tag{12}$$

Proof: For a degraded wiretap channel $P(Y_r, Y_e|X)$, Wyner [3] showed that the secrecy capacity is given by

$$\max_{P(X)}\left\{I(X;Y_r) - I(X;Y_e)\right\}. \tag{13}$$

It follows that the secrecy capacity of a degraded vector Gaussian wiretap channel (10) with $\mathbf{K}_r \preceq \mathbf{K}_e$ can be written as

$$\begin{aligned} C_s &= \max_{f(\mathbf{X}):\, E[\mathbf{X}\mathbf{X}^t] \preceq \mathbf{S}} \{I(\mathbf{X}; \mathbf{X}+\mathbf{W}_r) - I(\mathbf{X}; \mathbf{X}+\mathbf{W}_e)\} \\ &= \max_{f(\mathbf{X}):\, E[\mathbf{X}\mathbf{X}^t] \preceq \mathbf{S}} \{h(\mathbf{X}+\mathbf{W}_r) - h(\mathbf{X}+\mathbf{W}_e)\} - \left(\frac{1}{2}\log\det\mathbf{K}_r - \frac{1}{2}\log\det\mathbf{K}_e\right). \end{aligned} \tag{14}$$

For any random vector $\mathbf{X}$ with a covariance matrix $\mathbf{K}_x \preceq \mathbf{S}$, we have

$$\begin{aligned} h(\mathbf{X}+\mathbf{W}_r) - h(\mathbf{X}+\mathbf{W}_e) &= h(\mathbf{X}+\mathbf{W}_r) - h(\mathbf{X}+\mathbf{W}_r+\mathbf{W}) \\ &= -I(\mathbf{W}; \mathbf{X}+\mathbf{W}_r+\mathbf{W}) \\ &\leq -\frac{1}{2}\log\det\left(\mathbf{I} + (\mathbf{K}_e-\mathbf{K}_r)(\mathbf{K}_x+\mathbf{K}_r)^{-1}\right) \qquad (15) \\ &\leq -\frac{1}{2}\log\det\left(\mathbf{I} + (\mathbf{K}_e-\mathbf{K}_r)(\mathbf{S}+\mathbf{K}_r)^{-1}\right) \\ &= \frac{1}{2}\log\det(\mathbf{S}+\mathbf{K}_r) - \frac{1}{2}\log\det(\mathbf{S}+\mathbf{K}_e) \end{aligned}$$

where $\mathbf{W} \sim \mathcal{N}(0, \mathbf{K}_e - \mathbf{K}_r)$ is independent of $(\mathbf{X}, \mathbf{W}_r)$, and (15) follows from the worst additive noise result of Diggavi and Cover [13, Lemma II.2]. Thus, $\mathbf{X} \sim \mathcal{N}(0, \mathbf{S})$ is an optimal solution to the optimization problem in (14), and we have

$$\begin{aligned} C_s &= \left[\frac{1}{2}\log\det(\mathbf{S}+\mathbf{K}_r) - \frac{1}{2}\log\det(\mathbf{S}+\mathbf{K}_e)\right] - \left(\frac{1}{2}\log\det\mathbf{K}_r - \frac{1}{2}\log\det\mathbf{K}_e\right) \\ &= \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{S}\mathbf{K}_r^{-1}\right) - \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{S}\mathbf{K}_e^{-1}\right). \end{aligned}$$

This completes the proof of Theorem 1. ■

Next, we use a channel enhancement argument to lift the result of Theorem 1 to the general vector Gaussian wiretap channel. Channel enhancement argument was first introduced by Weingarten et al. [12] to characterize the capacity region of the multi-antenna broadcast channel. Adaptations are made here to fit our purposes. The difference between the channel enhancement argument here and that of Weingarten et al. [12] is highlighted in Section 2.2.

Theorem 2: The secrecy capacity of a general vector Gaussian wiretap channel (10) under the power covariance constraint (11) can be written as

$$C_s = \max_{0 \preceq \mathbf{K}_x \preceq \mathbf{S}} \left\{\frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{K}_x\mathbf{K}_r^{-1}\right) - \frac{1}{2}\log\det\left(\mathbf{I} + \mathbf{K}_x\mathbf{K}_e^{-1}\right)\right\}. \tag{16}$$

Proof: Following [12], it can be shown that without loss of generality, we may assume that S is (strictly) positive definite. In that case, let $\mathbf{K}_x^*$ be an optimal solution to the optimization problem

in (16). By the Karush-Kuhn-Tucker condition, $\mathbf{K}_x^*$ must satisfy

$$\begin{aligned} (\mathbf{K}_x^* + \mathbf{K}_r)^{-1} + \mathbf{M}_1 &= (\mathbf{K}_x^* + \mathbf{K}_e)^{-1} + \mathbf{M}_2 \\ \mathbf{K}_x^* \mathbf{M}_1 &= 0 \\ (\mathbf{S} - \mathbf{K}_x^*)\mathbf{M}_2 &= 0 \end{aligned} \tag{17}$$

for some positive semidefinite matrices $\mathbf{M}_1$ and $\mathbf{M}_2$. Recalling the single-letter capacity expression (3) and letting $U = \mathbf{X} \sim \mathcal{N}(0, \mathbf{K}_x^*)$, the secrecy capacity of a general vector Gaussian wiretap channel (10) can be bounded from below as

$$C_s \geq \frac{1}{2} \log\det(\mathbf{I} + \mathbf{K}_x^* \mathbf{K}_r^{-1}) - \frac{1}{2} \log\det(\mathbf{I} + \mathbf{K}_x^* \mathbf{K}_e^{-1}). \tag{18}$$

To prove the reverse inequality, let us define the real symmetric matrix $\tilde{\mathbf{K}}_r$ by

$$(\mathbf{K}_x^* + \tilde{\mathbf{K}}_r)^{-1} = (\mathbf{K}_x^* + \mathbf{K}_r)^{-1} + \mathbf{M}_1. \tag{19}$$

Following [12, Lemmas 10], we have

$$0 \prec \tilde{\mathbf{K}}_r = \left(\mathbf{K}_r^{-1} + \mathbf{M}_1\right)^{-1} \preceq \mathbf{K}_r. \tag{20}$$

Moreover, by (19) and the first equation in (17), we have

$$(\mathbf{K}_x^* + \tilde{\mathbf{K}}_r)^{-1} = (\mathbf{K}_x^* + \mathbf{K}_e)^{-1} + \mathbf{M}_2. \tag{21}$$

Clearly, $\tilde{\mathbf{K}}_r \preceq \mathbf{K}_e$. Note that $\tilde{\mathbf{K}}_r$ is positive definite. We may define a new wiretap channel with legitimate recipient and eavesdropper noise covariance matrices being $\tilde{\mathbf{K}}_r$ and $\mathbf{K}_e$, respectively. By virtue of $\tilde{\mathbf{K}}_r \preceq \mathbf{K}_e$, the new vector Gaussian wiretap channel is a degraded one. By Theorem 1, the secrecy capacity of this channel is equal to

$$\tilde{C}_s = \frac{1}{2} \log\det(\mathbf{I} + \mathbf{S}\tilde{\mathbf{K}}_r^{-1}) - \frac{1}{2} \log\det(\mathbf{I} + \mathbf{S}\mathbf{K}_e^{-1}). \tag{22}$$

Also note that

$$\begin{aligned} (\mathbf{S} + \tilde{\mathbf{K}}_r)(\mathbf{K}_x^* + \tilde{\mathbf{K}}_r)^{-1} &= (\mathbf{S} - \mathbf{K}_x^*)(\mathbf{K}_x^* + \tilde{\mathbf{K}}_r)^{-1} + \mathbf{I} \\ &= (\mathbf{S} - \mathbf{K}_x^*)\left((\mathbf{K}_x^* + \mathbf{K}_e)^{-1} + \mathbf{M}_2\right) + \mathbf{I} \qquad (23) \\ &= (\mathbf{S} - \mathbf{K}_x^*)(\mathbf{K}_x^* + \mathbf{K}_e)^{-1} + \mathbf{I} \qquad (24) \\ &= (\mathbf{S} + \mathbf{K}_e)(\mathbf{K}_x^* + \mathbf{K}_e)^{-1} \end{aligned}$$

where (23) follows (21), and (24) follows from and the third equation in (17). We thus have

$$\frac{1}{2} \log\det(\mathbf{S} + \tilde{\mathbf{K}}_r) - \frac{1}{2} \log\det(\mathbf{S} + \mathbf{K}_e) = \frac{1}{2} \log\det(\mathbf{K}_x^* + \tilde{\mathbf{K}}_r) - \frac{1}{2} \log\det(\mathbf{K}_x^* + \mathbf{K}_e). \tag{25}$$

Substituting (25) into (29), we have

$$\begin{aligned}
\tilde{C}_s &= \left[\frac{1}{2}\log\det(\mathbf{S}+\tilde{\mathbf{K}}_r) - \frac{1}{2}\log\det(\mathbf{S}+\mathbf{K}_e)\right] - \left(\frac{1}{2}\log\det\tilde{\mathbf{K}}_r - \frac{1}{2}\log\det\mathbf{K}_e\right) \\
&= \left[\frac{1}{2}\log\det(\mathbf{K}_x^*+\tilde{\mathbf{K}}_r) - \frac{1}{2}\log\det(\mathbf{K}_x^*+\mathbf{K}_e)\right] - \left(\frac{1}{2}\log\det\tilde{\mathbf{K}}_r - \frac{1}{2}\log\det\mathbf{K}_e\right) \\
&= \frac{1}{2}\log\det(\mathbf{I}+\mathbf{K}_x^*\tilde{\mathbf{K}}_r^{-1}) - \frac{1}{2}\log\det(\mathbf{I}+\mathbf{K}_x^*\mathbf{K}_e^{-1}) \\
&= \frac{1}{2}\log\det(\mathbf{I}+\mathbf{K}_x^*(\mathbf{K}_r^{-1}+\mathbf{M}_1)) - \frac{1}{2}\log\det(\mathbf{I}+\mathbf{K}_x^*\mathbf{K}_e^{-1}) \qquad (26) \\
&= \frac{1}{2}\log\det(\mathbf{I}+\mathbf{K}_x^*\mathbf{K}_r^{-1}) - \frac{1}{2}\log\det(\mathbf{I}+\mathbf{K}_x^*\mathbf{K}_e^{-1}) \qquad (27)
\end{aligned}$$

where (26) follows from (20), and (27) follows from the second equation in (17). Note that $\tilde{\mathbf{K}}_r \preceq \mathbf{K}_r$, c.f. (20). Since reducing the noise covariance matrix for the legitimate recipient can only increase the secrecy capacity, we have

$$C_s \leq \tilde{C}_s = \frac{1}{2}\log\det(\mathbf{I}+\mathbf{K}_x^*\mathbf{K}_r^{-1}) - \frac{1}{2}\log\det(\mathbf{I}+\mathbf{K}_x^*\mathbf{K}_e^{-1}) \qquad (28)$$

which is the desired reverse inequality. Putting together (18) and (28) completes the proof of Theorem 2. ■

Finally, we extend the capacity result for the vector Gaussian wiretap channel to the general multi-antenna wiretap channel. The readers are referred to [12] for a proof of the following theorem.

Theorem 3: The secrecy capacity of the multi-antenna wiretap channel (1) under the power covariance constraint (11) can be written as

$$C_s = \max_{0\preceq\mathbf{K}_x\preceq\mathbf{S}} \left\{\frac{1}{2}\log\det\left(\mathbf{I}+\mathbf{H}_r\mathbf{K}_x\mathbf{H}_r^t\right) - \frac{1}{2}\log\det\left(\mathbf{I}+\mathbf{H}_e\mathbf{K}_x\mathbf{H}_e^t\right)\right\}. \qquad (29)$$

2.2 Physical intuition

Our approach of characterizing the secrecy capacity of the vector Gaussian wiretap channel hinges on the existence of an enhanced channel, which needs to satisfy:

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

In the foresight, it is not entirely clear whether such an enhanced channel would always exist, letting alone to actually construct one.

Our intuition regarding to the existence of the enhanced channel was mainly from the parallel Gaussian wiretap channel with a total power constraint, which is a special case of the vector Gaussian wiretap channel (10) with diagonal noise covariance matrices $\mathbf{K}_r$ and $\mathbf{K}_e$. In this case, it is shown in [14, 15] that the optimal transmission strategy is to transmit independently over the subchannels for which the received signal by the legitimate recipient is stronger than that by 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 variance levels of the eavesdropper. Clearly, the enhanced channel thus constructed is a degraded parallel Gaussian wiretap channel. Furthermore, the secrecy capacity of the enhanced channel is the same as the original channel, as the noise variances for the legitimate recipient did not change at all for any of the "active" subchannels while the "inactive" subchannels remained "inactive". Therefore, at least for the special case of the parallel Gaussian wiretap channel, the enhanced channel does always exist.

Carrying over to the general vector Gaussian wiretap channel, no information should be transmitted along any direction where the eavesdropper observes a stronger signal than the legitimate recipient. (This intuition was formally confirmed by Khisti and Wornell [1].) The effective channel for the eavesdropper is thus a degraded version of the effective channel for the legitimate recipient. Mathematically, however, since the optimal transmit directions are not always along the common eigendirections of $\mathbf{K}_e$ and $\mathbf{K}_r$ (which may not even exist), finding an enhanced channel (by reducing "just enough" the noise covariance matrix for the legitimate recipient) is much more involved than in the case of the parallel Gaussian wiretap channel. Our construction in Section 2.1 was based on the construction of the enhanced channel of Weingarten et al. [12] for the vector Gaussian broadcast channel (a canonical model for the multi-antenna broadcast channel). As suggested by Khisti and Wornell [16], a related enhanced channel can be constructed by degrading the noise covariance matrix of the eavesdropper:

$$(\mathbf{K}_x^* + \tilde{\mathbf{K}}_e)^{-1} = (\mathbf{K}_x^* + \mathbf{K}_e)^{-1} - \mathbf{M}_1$$

thus giving [12, Lemmas 10]:

$$\tilde{\mathbf{K}}_e = \left(\mathbf{K}_e^{-1} - \mathbf{M}_1\right)^{-1} \succeq \mathbf{K}_e,$$

as compared with reducing the noise covariance matrix of the legitimate recipient in (20). The fact that the vector Gaussian wiretap channel with legitimate and eavesdropper noise covariance matrices $\mathbf{K}_r$ and $\tilde{\mathbf{K}}_e$ respectively has the same secrecy capacity as the original vector Gaussian wiretap channel can be verified following the same footsteps as in the proof of Theorem 2.

Finally, recall that in their characterization of the capacity region of the vector Gaussian broadcast channel, Weingarten et al. [12] enhanced each and every channel (by reducing the corresponding noise covariance matrices) from the transmitter to the receivers. In our argument, however, we only

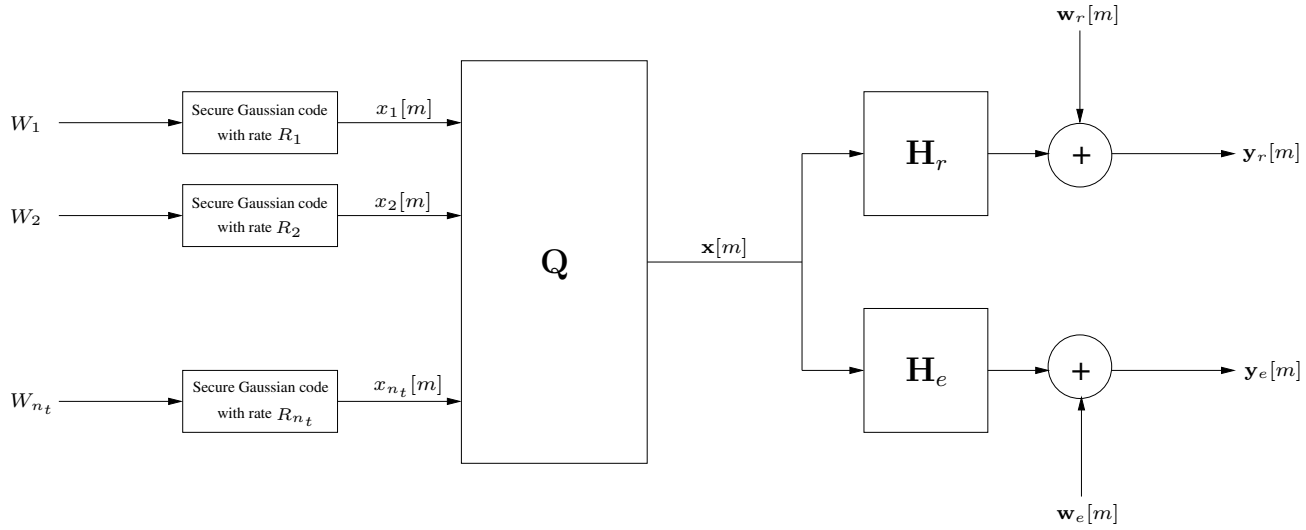

Figure 1: Transmission architecture for secure V-BLAST.

enhanced the channel for the legitimate recipient (while the channel for the eavesdropper did not change at all). This is due to the fact that in both arguments, the enhancement *a priori* must increase 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 capacity of the vector Gaussian broadcast channel, reducing the noise covariance matrix 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. [12] for the vector Gaussian broadcast channel.

3 The Secure V-BLAST Architecture

The result of Theorem 3 motivates the secure V-BLAST architecture as shown in Figure 1 (transmission) and Figure 2 (receiver), which is a natural extension of the well-known V-BLAST architecture [17, Cha. 8.1] for the multi-antenna channel without the secrecy constraint. The performance of this architecture can be analyzed as follows.

Let the optimal covariance matrix in (29)

$$\mathbf{K}_x^* = \mathbf{Q}\,\mathrm{diag}\{P_1, \ldots, P_{n_t}\}\,\mathbf{Q}^t$$

where $\mathbf{Q}$ is an orthogonal matrix, and let $X_k \sim \mathcal{N}(0, P_k)$, $k = 1, \ldots, n_t$, be n_t independent Gaussian

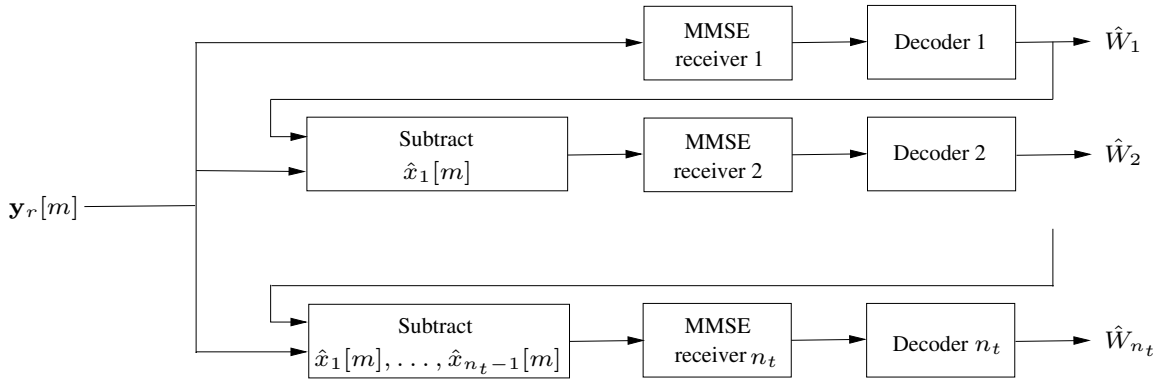

Figure 2: Receiver architecture for secure V-BLAST.

variables. The covariance matrix of the random vector

$$\mathbf{X} = \mathbf{Q}\,[X_1, \ldots, X_{n_t}]^t.$$

is equal to $\mathbf{K}_x^*$. The k-th message W_k is encoded using a secure Gaussian code [5] with power P_k and rate

$$\begin{aligned} R_k &= I(X_k; \mathbf{Y}_r, X_1, \ldots, X_{k-1}) - I(X_k; \mathbf{Y}_e, X_1, \ldots, X_{k-1}) \\ &= I(X_k; \mathbf{Y}_r | X_1, \ldots, X_{k-1}) - I(X_k; \mathbf{Y}_e | X_1, \ldots, X_{k-1}) \end{aligned}$$

where the second equality follows from the mutual independence of X_k. Note that such codes are secure with respect to the wiretap channel with $(\mathbf{Y}_r, X_1, \ldots, X_{k-1})$ at the legitimate recipient and $(\mathbf{Y}_e, X_1, \ldots, X_{k-1})$ at the eavesdropper. We thus have

$$I(W_k; \mathbf{Y}_e^n, X_1^n, \ldots, X_{k-1}^n) \leq n\epsilon_k$$

for large enough n, where $\mathbf{Y}_e^n$ denotes $(\mathbf{Y}_e[1], \ldots, \mathbf{Y}_e[n])$ and so on. By the chain rule of mutual information, the sum rate of this scheme is equal to

$$\begin{aligned} R &= \sum_{k=1}^{n_t} [I(X_k; \mathbf{Y}_r | X_1, \ldots, X_{k-1}) - I(X_k; \mathbf{Y}_e | X_1, \ldots, X_{k-1})] \\ &= I(X_1, \ldots, X_{n_t}; \mathbf{Y}_r) - I(X_1, \ldots, X_{n_t}; \mathbf{Y}_e) \\ &= I(\mathbf{X}; \mathbf{Y}_r) - I(\mathbf{X}; \mathbf{Y}_e) \qquad (30) \\ &= \frac{1}{2} \log\det\left(\mathbf{I} + \mathbf{H}_r \mathbf{K}_x^* \mathbf{H}_r^t\right) - \frac{1}{2} \log\det\left(\mathbf{I} + \mathbf{H}_e \mathbf{K}_x^* \mathbf{H}_e^t\right) \qquad (31) \end{aligned}$$

where (30) follows from the fact that $\mathbf{Q}$ is nonsingular, and (31) follows from the fact that the covariance matrix of $\mathbf{X}$ is equal to $\mathbf{K}_x^*$ by construction. The security of the scheme can be verified

as follows:

$$\begin{aligned} I(W_1,\ldots,W_{n_t};\mathbf{Y}_e^n) &= \sum_{k=1}^{n_t} I(W_k;\mathbf{Y}_e^n|W_1,\ldots,W_{k-1}) \\ &\leq \sum_{k=1}^{n_t} I(W_k;\mathbf{Y}_e^n,X_1^n,\ldots,X_{k-1}^n|W_1,\ldots,W_{k-1}) \\ &= \sum_{k=1}^{n_t} I(W_k;\mathbf{Y}_e^n|W_1,\ldots,W_{k-1},X_1^n,\ldots,X_{k-1}^n) \qquad (32) \\ &= \sum_{k=1}^{n_t} I(W_k;\mathbf{Y}_e^n|X_1^n,\ldots,X_{k-1}^n) \qquad (33) \\ &\leq n\sum_{k=1}^{n_t}\epsilon_k \end{aligned}$$

where (32) follows from the conditional independence of W_k and $(X_1^n,\ldots,X_{k-1}^n)$ given $(W_1,\ldots,W_{k-1})$, and (33) follows from the Markov chains $(W_1,\ldots,W_{k-1})-(X_1^n,\ldots,X_{k-1}^n)-\mathbf{Y}_e^n$. The optimality of the MMSE filters at the legitimate recipient follows from the standard sufficient statistic argument. Thus, the secure V-BLAST architecture achieves the secrecy capacity of the multi-antenna wiretap channel.

Acknowledgment

The authors would like to thank Ashish Khisti and Gregory Wornell from MIT and Babak Hassibi from Caltech for insightful comments on an earlier version of this note.

References

[1] A. Khisti and G. Wornell, "The MIMOME channel," in *Proc. 45th Annual Allerton Conf. Comm., Contr., and Computing*, Monticello, Illinois, Sept. 2007. Available at `http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.1325v1.pdf`

[2] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," preprint. Available at `http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.1920v1.pdf`

[3] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

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

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Info. 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. Info. Theory*, submitted for publication. Available at `http://arxiv.org/PS_cache/arxiv/pdf/0709/0709.3541v1.pdf`

[9] H. Sato, "An outer bound to the capacity region of broadcast channels," *IEEE Trans. Info. Theory*, vol. IT-24, no. 3, pp. 374-377, May 1978.

[10] 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.

[11] 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.

[12] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "The capacity region of the Gaussian multiple-input-multiple-output broadcast channel," *IEEE Trans. Info. Theory*, vol. 52, no. 9, pp. 3936-3964, Sept. 2006.

[13] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Trans. Info. Theory*, vol. 47,. no. 7, pp. 3072-3081, Nov. 2001.

[14] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. 44th Annual Allerton Conf. Comm., Contr., and Computing*, Monticello, Illinois, Sept. 2006. Available at `http://www.winlab.rutgers.edu/~zang/Papers/ZangAllerton06.pdf`

[15] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Info. Theory*, submitted for publication. Available at `http://arxiv.org/PS_cache/arxiv/pdf/0708/0708.2733v1.pdf`

[16] A. Khisti and G. W. Wornell, Private communication.

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