where $\boldsymbol{z}_1^n$ is $-1$, and $\mathcal{S}_2$ is the corresponding set for $\boldsymbol{z}_2^n$, it must be that $\mathcal{S}_1 \neq \mathcal{S}_2$. Therefore, according to Definition 1 and the one-to-one property of the subset map $\psi_{l,i_l}$, the subset of indices $i \leq i_l$ where $\phi(\boldsymbol{z}_1^n)$ is $-1$ and the corresponding subset of indices for $\phi(\boldsymbol{z}_2^n)$ must differ. This completes the proof that $\phi$ is one to one.

It remains to prove Property 3 of $\phi$, that if $\sum_{i=1}^n a_i z_i > n - 2j$ then $\hat{\boldsymbol{z}}^n = \phi(\boldsymbol{z}^n)$ satisfies $\sum_{i=1}^n a_i \hat{z}_i \leq n - 2j$. To see this, define the subsets of indices

$$\mathcal{S}^{(1)} = \{i_1, \ldots, i_l\} \text{ and } \mathcal{S}^{(2)} = \{i : i_l + 1 \leq i \leq n\}$$

and

$$\mathcal{S} = \mathcal{S}^{(1)} \cup \psi_{l,i_l}(\mathcal{S}^{(1)}) \cup \mathcal{S}^{(2)}.$$

The cardinality of $\mathcal{S}$ is

$$\begin{aligned} |\mathcal{S}| &= n - i_l + 2l \\ &= n - (n - 2j + 2l) + 2l \\ &= 2j \end{aligned} \tag{27}$$

so that $|\mathcal{S}^c| = n - 2j$, where (27) uses (26). If

$$\begin{aligned} \sum_{i=1}^n a_i z_i &= \sum_{i \in \mathcal{S}} a_i z_i + \sum_{i \in \mathcal{S}^c} a_i z_i \\ &> n - 2j \end{aligned}$$

then

$$\begin{aligned} \sum_{i \in \mathcal{S}} a_i z_i &> n - 2j - \sum_{i \in \mathcal{S}^c} a_i z_i \\ &\geq n - 2j - |\mathcal{S}^c| \\ &= 0. \end{aligned} \tag{28}$$

From the definition of $\phi$ (Definition 1), however, $\hat{\boldsymbol{z}}^n = \phi(\boldsymbol{z}^n)$ satisfies

$$\hat{z}_i = -z_i, \qquad \text{for } i \in \mathcal{S} \quad \text{and} \quad \hat{z}_i = z_i, \qquad \text{for } i \in \mathcal{S}^c.$$

Therefore, (28) implies that $\sum_{i \in \mathcal{S}} a_i \hat{z}_i < 0$, and hence,

$$\begin{aligned} \sum_{i=1}^n a_i \hat{z}_i &= \sum_{i \in \mathcal{S}} a_i \hat{z}_i + \sum_{i \in \mathcal{S}^c} a_i \hat{z}_i \\ &< \sum_{i \in \mathcal{S}^c} a_i \hat{z}_i \\ &\leq |\mathcal{S}^c| \\ &= n - 2j. \end{aligned}$$

This completes the proof of Lemma 1. □.

## ACKNOWLEDGMENT

The author wishes to thank Shlomo Shamai for bringing this problem to his attention.

## REFERENCES

[1] N. L. Biggs, *Discrete Mathematics*. Oxford, U.K.: Oxford Univ. Press, 1985.

[2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[3] P. Harremöes, "Binomial and Poisson distributions as maximum entropy distributions," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 2039–2041, Jul. 2001.

[4] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and its Applications*. London, U.K.: Academic, 1979, vol. 143, Mathematics in Science and Engineering.

[5] S. Shamai (Shitz) and S. Verdú, "BSF Grant Application," Appendix, Nov. 1992.

[6] L. A. Shepp and I. Olkin, "Entropy of the Sum of Independent Bernoulli Random Variables and of the Multinomial Distribution," Stanford Univ., Dept. Statistics, Stanford, CA, Tech. Rep. 131, 1978.

# An Achievable Region for the Gaussian Wiretap Channel With Side Information

Chaichana Mitrpant, A. J. Han Vinck, *Fellow, IEEE*, and Yuan Luo

***Abstract*—In this correspondence, we extend the Gaussian wiretap channel model introduced by Leung–Yan–Cheong and Hellman to the Gaussian wiretap channel with side information by introducing additive white Gaussian interference in the main channel, which is available to the encoder in advance. This model is also an extension of the dirty-paper channel introduced by Costa since its main channel is the dirty-paper channel. A perfect-secrecy-achieving coding strategy for the model is proposed. It is used to derive achievable rates with asymptotic perfect secrecy and an achievable rate-equivocation region. The achievable rates with asymptotic perfect-secrecy are then compared to upper and lower bounds. The comparison indicates that the proposed coding strategy is optimal in some cases.**

***Index Terms*—Dirty-paper channel, Gaussian wiretap channel, Gaussian wiretap channel with side information, perfect secrecy.**

## I. INTRODUCTION

The wiretap channel, introduced in [1], provides a framework for the study of secret message transmission between a sender and a legitimate recipient over a main discrete memoryless channel (DMC) being wiretapped by an adversary via a wiretap DMC. The level of message secrecy is measured by using the concept of equivocation. It is of interest to design a communication system that allows reliable message transmission at high rates and high secrecy. A special case and a different variant of the wiretap channel model were investigated in [2] and [3] as the wiretap II channel and the Gaussian wiretap channel (GWC), respectively. It has been shown that positive information rates can be achieved with asymptotic perfect secrecy when the adversary's observation is a noisy version of the recipient's observation [1]–[3].

Motivated by a covert communication situation, we extend the GWC model by introducing an additive white Gaussian interference to the main channel as a covert communication channel. The interference is assumed to be completely known to the sender before the message transmission. The extended model is called Gaussian wiretap channel with side information (GWCSI). It can also be viewed as an extension of the dirty-paper channel (DPC) introduced in [4] since the main channel of the GWCSI is the DPC.

Manuscript received February 26, 2004; revised December 30, 2005. This work was supported by the German Science Foundation (DFG), the National Electronics and Computer Technology and the National Science Foundation of China under Grant 60402022.

C. Mitrpant is with the National Electronics and Computer Technology Center (NECTEC), Phathumthani 12120, Thailand.

A. J. Han Vinck is with the Institute for Experimental Mathematics, Universitaet Duisburg-Essen, Essen 45326, Germany.

Y. Luo is with the Computer Science and Engineering Department, Shanghai Jiao Tong University, Shanghai 200030, China.

Communicated by A. Lapidoth, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2006.872968

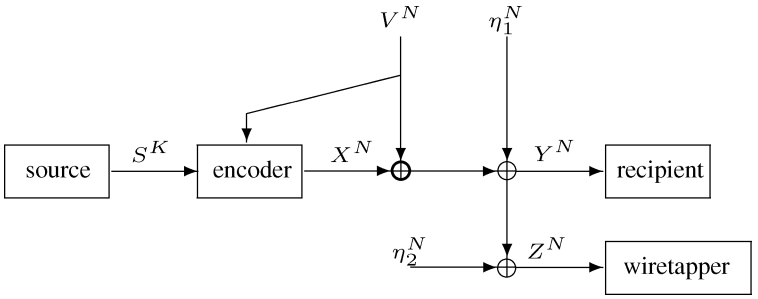


Fig. 1. The Gaussian wiretap channel with side information to the encoder.

We describe the GWCSI model in Section II. In Section III, the code-partitioning technique is considered for the GWCSI. A coding strategy, based on the code-partitioning technique, and a leakage function are proposed in Section IV for the GWCSI to achieve perfect secrecy. An achievable region for the GWCSI is derived based on the proposed coding strategy and the time-sharing lemma in Section V. In Section VI, the achievable rates with asymptotic perfect secrecy are compared to upper and lower bounds. Finally, concluding remarks are given in Section VII.

## II. Model Description

In the GWCSI model, there are three parties involved: a sender, a legitimate recipient and an adversary (wiretapper). The sender is interested in sending a message to the recipient via a dirty-paper channel (main channel) that is wiretapped by the adversary via an additive white Gaussian noise (AWGN) channel (wiretap channel). The sender would like to encode the message by using the side information about the interference available to him in advance so that the message can be reliably transmitted at a high rate with desired level of secrecy. The level of secrecy is measured using the concept of equivocation. The adversary is assumed to know the coding strategy and the associated codebook.

Let $S^K$ represent a length-$K$ finite-alphabet message and $X^N$ be a length-$N$ codeword generated from $S^K$ by an encoding process with an average power constraint $P$

$$\frac{1}{N}\sum_{i=1}^{N} x_i^2 \le P.$$

Let $V^N \sim \mathcal{N}(0, Q)$ represent the normally distributed interference in the main channel known to the sender in advance. Let $Y^N = X^N + V^N + \eta_1^N$, and $Z^N = Y^N + \eta_2^N$ be the outputs of the main channel and the wiretap channel, where $\eta_1^N$ and $\eta_2^N$ are sequences of independent random variables identically distributed according to $\mathcal{N}(0, N_1)$ and $\mathcal{N}(0, N_2)$, respectively. The parameters $Q$, $N_1$ and $N_2$ are assumed to be greater than zero. The recipient decodes the output of the main channel $Y^N$ for a message estimate $\hat{S}^K$ at rate $H(S^K)/N$ with probability of error

$$P_e = \Pr\{S^K \neq \hat{S}^K\}$$

and normalized equivocation

$$\frac{H(S^K|Z^N)}{H(S^K)}.$$

We say that the rate-equivocation pair $(R, d)$ is achievable if, for any $\epsilon > 0$ and sufficiently large $N$, there exists an encoder-decoder pair such that

$$\frac{H(S^K)}{N} \ge R - \epsilon \tag{1}$$

$$\frac{H(S^K|Z^N)}{H(S^K)} \ge d - \epsilon \tag{2}$$

$$P_e \le \epsilon. \tag{3}$$

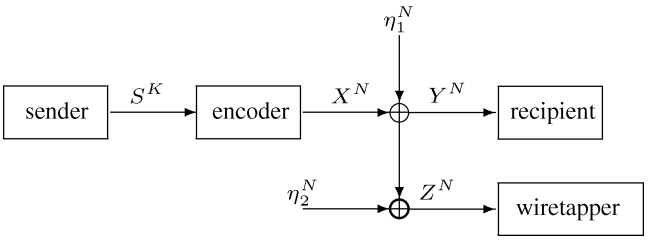


Fig. 2. The Gaussian wiretap channel (GWC).

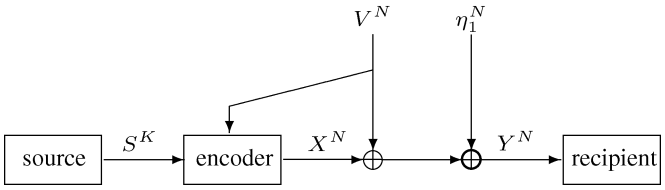


Fig. 3. The dirty-paper channel (DPC).

The perfect secrecy occurs when the message is independent of the adversary's observation $Z^N$; therefore, it is achieved when $d = 1$. Fig. 2 indicates that the GWCSI without the interference is the GWC. Fig. 3 shows that the main channel of the GWCSI is the DPC.

## III. Code-Partitioning Technique

The code-partitioning technique was used in the proof of the capacity region of the wiretap channel in [1] and in the proof of the capacity of channel with random parameters in [5]. It also allows communication at asymptotic perfect secrecy for the GWC and mitigates the effect of the interference in the DPC as shown in [3] and [4], respectively. In this section, we apply the code-partition technique to the GWCSI by partitioning a random code designed for an additive white Gaussian noise (AWGN) channel into bins so that high rates can be achieved with asymptotic perfect secrecy.

The main idea behind the coding technique is to partition the code designed for reliable communication via the main channel into bins so that each bin contains a code designed for reliable communication via the combined (main and wiretap) channel. The adversary's observation can then be decoded as possibly coming from any bin. Since each bin is associated with a message, high message equivocation can be achieved. In addition, the use of side information about the interference to mitigate its effect can be integrated in the coding strategy to improve transmission rate.

The coding technique makes use of the auxiliary random variable $U = X + \alpha V$, where $\alpha$ is a parameter to be specified. It consists of codebook generating, encoding and decoding processes. The codebook generating process is based on the code-partitioning technique while the encoding and decoding processes rely on the asymptotic equipartition properties (AEPs); hence, the wiretapper may use a typical decoder in an attempt to achieve the capacity of the combined channel.

The number of auxiliary codewords and the number of bins in the codebook are restricted by the power constraint via parameters $R_{\text{main}}$ and $R$, respectively. The sender's and the adversary's typicality parameter $\delta > 0$ is to be specified appropriately.

To describe the coding procedure (similar to that for the DPC), we define the following random variables:

$$U \sim \mathcal{N}(0, P' + \alpha^2 Q), \qquad Y \sim \mathcal{N}(0, P' + Q + N_1),$$
$$Z \sim \mathcal{N}(0, P' + Q + N_1 + N_2), \quad U = X + \alpha V,$$
$$V \sim \mathcal{N}(0, Q), \qquad X \sim \mathcal{N}(0, P')$$

$U_c$ represents the auxiliary codewords

where $P$ is the average power constraint and $P' = P(1 + 4\delta \ln(2))^{-1}$ (see Appendix A, Lemma A.1). The random variables have the following relations:

$$Y^N = X^N + V^N + \eta_1^N, \quad Z^N = X^N + V^N + \eta_1^N + \eta_2^N.$$

In addition, the definition of joint typicality [6] is used in the description of the proposed coding procedure as follows.

1) Generating the codebook. Generate $2^{NR_{\text{main}}}$ sequences $u^N$ according to the distribution $p(u^N) = \prod_{i=1}^N p(u_i)$, and $p(u_i) \sim \mathcal{N}(0, P' + \alpha^2 Q)$ for all $i \in \{1, 2, \ldots, N\}$. Place the sequences $u^N$ randomly into $2^{NR}$ bins. Index each bin by $j \in \{1, 2, \ldots, 2^{NR}\}$. The codebook is given to the sender and the recipient.
2) *Encoding*. To send a message $j$ through an interference $v^N$, the sender looks for a sequence $u_c$ in bin $j$ such that $v^N$ and $u_c$ are jointly typical, i.e., $(u_c, v^N) \in T_{U,V}^N(\delta)$, and transmit $x^N = u_c - \alpha v^N$. If there is more than one sequence $u_c$ that is jointly typical with $v^N$, randomly select one.
3) *Decoding*. To decode for the message, the recipient finds a sequence $u_c$ in the codebook that is jointly typical with the received sequence $y^N$, i.e., $(u_c, y^N) \in T_{U,Y}^N(\delta)$. Declare the index to the bin, in which the sequence is found as the message estimate.
4) *Wiretapper's decoding*. The wiretapper receives a sequence $z^N$ and finds a sequence $u_c$ in the codebook that is jointly typical with the received sequence, i.e., $(u_c, z^N) \in T_{U,Z}^N(\delta)$. Declare the index to the bin, in which the sequence is found as the wiretapper's message estimate.
5) Probability of error. An error occurs when a message $j$ is to be transmitted and one or more of the following events occurs:
   - $\mathcal{E}^V(j)$: in the encoding process, there is no sequence $u_c$ in bin $j$ that is jointly typical with the interference sequence;
   - $\mathcal{E}^X(j)|\mathcal{E}^V(j)^C$: in the encoding process, $x^N = u_c - \alpha v^N$ does not satisfy the power constraint provided that there is at least a sequence $u_c$ jointly typical with the interference $v^N$;
   - $\mathcal{E}^{Y1}(j)|\mathcal{E}^X(j)^C\mathcal{E}^V(j)^C$: in the decoding process, there is no sequence $u_c$ that is jointly typical with the received sequence provided that there is no error in the encoding process;
   - $\mathcal{E}^{Y2}(j)|\mathcal{E}^X(j)^C\mathcal{E}^V(j)^C$: in the decoding process, a sequence $u_c$ in bin $i \neq j$ is jointly typical with the received sequence provided that there is no error in the encoding process.

The average power constraint on the transmitted vector in the GWCSI imposes a limit on the transmission rate. The limited power available to the encoder will be used for two purposes: to confuse the adversary so that perfect secrecy can be achieved, and to mitigate the effect of the interference in the main channel so that the message can be transmitted at high rates. The power is regulated to attain the two purposes by selecting one of the two modes of the coding strategy given in the next section.

## IV. Coding Strategy for the GWCSI With Asymptotic Perfect Secrecy

In this section, we propose a coding strategy achieving high rates with asymptotic perfect secrecy for the GWCSI. There are two modes of operation designed for different levels of power constraint on $X^N$. The selection of the modes is based on the characteristics of a leakage function introduced for the GWCSI.

### A. Modes of Operation

The coding strategy is refined into two modes of operation. The two modes employ the same encoding and decoding processes with the error events described in Section III. The only differences are the sizes and the structures of the codebooks resulting in different rates of communication between the sender and the recipient. To describe the two modes of operation, we define the following random variables:

$$\tilde{U} \sim \mathcal{N}(0, P + \alpha^2 Q), \qquad \tilde{X} \sim \mathcal{N}(0, P)$$
$$\tilde{Y} \sim \mathcal{N}(0, P + Q + N_1), \quad \tilde{Z} \sim \mathcal{N}(0, P + Q + N_1 + N_2).$$

The random variables have the following relations:

$$\tilde{Y}^N = \tilde{X}^N + V^N + \eta_1^N, \quad \tilde{Z}^N = \tilde{X}^N + V^N + \eta_1^N + \eta_2^N$$

where $\tilde{X}$, $V$, $\eta_1$ and $\eta_2$ are independent among themselves. The two modes are specified as follows.

*Mode I:* Given $\epsilon > 0$, let $\epsilon_{UV}$ and $\epsilon_{UZ}$ be positive constants, associated with the codebook generating process, to be specified appropriately. The codebook in this mode has $2^{N[R_{\text{main}} - \epsilon_{\text{main}}]}$ sequences $u_c$ and $2^{N[R-\epsilon]}$ bins, where $R_{\text{main}} = I(\tilde{U};\tilde{Y})$, $\epsilon_{\text{main}} = \epsilon - \epsilon_{UV}$ and $R = I(\tilde{U};\tilde{Y}) - I(\tilde{U};V)$. Moreover, each bin is further divided into subbins so that each subbin contains $2^{N[I(\tilde{U};\tilde{Z}) - \epsilon_{UZ}]}$ sequences $u_c$.

*Mode II:* Given $\epsilon > 0$, let $\epsilon_{UZ}$ be a positive constant, associated with the codebook generating process, to be specified appropriately. The codebook in this mode has $2^{N[R_{\text{main}} - \epsilon_{\text{main}}]}$ sequences $u_c$ and $2^{N[R-\epsilon]}$ bins, where $R_{\text{main}} = I(\tilde{U};\tilde{Y})$, $\epsilon_{\text{main}} = \epsilon + \epsilon_{UZ}$ and $R = I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z})$.

Depending on the number of bins in the codebook, the rate of communication between the sender and the recipient is $\log(2^{N[R-\epsilon]})/N = R - \epsilon$. In *Mode I*, rate $R = I(\tilde{U};\tilde{Y}) - I(\tilde{U};V) - \epsilon$ can be optimized over $\alpha$ since

$$\begin{aligned} &I(\tilde{U};\tilde{Y}) - I(\tilde{U};V) - \epsilon \\ &\quad = \frac{1}{2}\log\left[\frac{(P + \alpha^2 Q)(P + Q + N_1)}{(P + \alpha^2 Q)(P + Q + N_1) - (P + \alpha Q)^2}\right] \\ &\qquad - \frac{1}{2}\log\left[\frac{P + \alpha^2 Q}{P}\right] - \epsilon \\ &\quad = \frac{1}{2}\log\left[\frac{P(P + Q + N_1)}{(P + \alpha^2 Q)(P + Q + N_1) - (P + \alpha Q)^2}\right] - \epsilon. \end{aligned}$$

The maximum rate for *Mode I* is $C_M - \epsilon$ at $\alpha = \alpha_1$ where

$$C_M = \frac{1}{2}\log\left[\frac{P + N_1}{N_1}\right] \tag{4}$$

$$\alpha_1 = \frac{P}{P + N_1}. \tag{5}$$

Similarly, rate $R - \epsilon = I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z}) - \epsilon$ in *Mode II* can also be optimized over $\alpha$. The maximum rate for *Mode II* is $R_2 - \epsilon$ at $\alpha = \alpha_2$ where

$$R_2 = \frac{1}{2}\log\left[\frac{(P + Q + N_1)(N_1 + N_2)}{N_1(P + Q + N_1 + N_2)}\right]$$
$$\alpha_2 = 1. \tag{6}$$

In *Mode I*, the number of codewords in a bin is $2^{N[I(\tilde{U};V) + \epsilon_{UV}]}$, which is shown in the case of DPC to be sufficient for conveying partial information about the interference. In *Mode II*, the number of code-

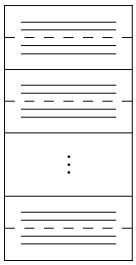


Fig. 4. The codebook for the coding strategy in *Mode I* for GWCSI.

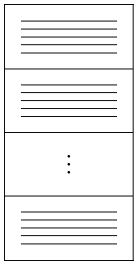


Fig. 5. The codebook for the coding strategy in *Mode II* for GWCSI.

words in a bin is $2^{N[I(\tilde{U};\tilde{Z})-\epsilon_{UZ}]}$, which is shown in the GWC to be sufficient for confusing the adversary. In order to select an appropriate mode of operation, we define the leakage function for the GWCSI in the next section.

### B. Leakage Function

In the GWC, there is no interference in the main channel, and the rate-equivocation pair $(I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z}), 1)$ can be achieved [3]. The average rate $I(\tilde{U};\tilde{Z})$ is used to confuse the adversary. In the DPC, there is no adversary wiretapping the main channel. The sender can communicate with the recipient at rate $I(\tilde{U};\tilde{Y}) - I(\tilde{U};V)$ [4]. The average rate $I(\tilde{U};V)$ is used to convey the partial information about the interference to mitigate its effect.

Because selecting an appropriate auxiliary codeword in a bin to convey the partial information about the interference has a beneficial side effect of confusing the adversary, the leakage function for the GWCSI is defined as $\Delta I(\alpha) = I(\tilde{U};\tilde{Z}) - I(\tilde{U};V)$. Consequently, when the power needed to confuse the wiretapper is more than what is used to convey the partial information about the interference to mitigate its effect, the leakage function is positive. On the other hand, the leakage function is negative when the power used to mitigate the effect of the interference is higher than what is needed to confuse the wiretapper.

The leakage function is of the form

$$\begin{aligned}
&\Delta I(\alpha)\\
&= I(\tilde{U};\tilde{Z}) - I(\tilde{U};V)\\
&= \frac{1}{2}\log\left[\frac{(P+\alpha^2 Q)(P+Q+N_1+N_2)}{(P+\alpha^2 Q)(P+Q+N_1+N_2)-(P+\alpha Q)^2}\right]\\
&\quad - \frac{1}{2}\log\left[\frac{P+\alpha^2 Q}{P}\right]\\
&= \frac{1}{2}\log\left[\frac{P(P+Q+N_1+N_2)}{(P+\alpha^2 Q)(P+Q+N_1+N_2)-(P+\alpha Q)^2}\right].
\end{aligned}$$

Hence

$$\Delta I(0) = \frac{1}{2}\log\left[\frac{P+Q+N_1+N_2}{Q+N_1+N_2}\right] > 0,$$
$$\Delta I(\alpha_0) = 0$$

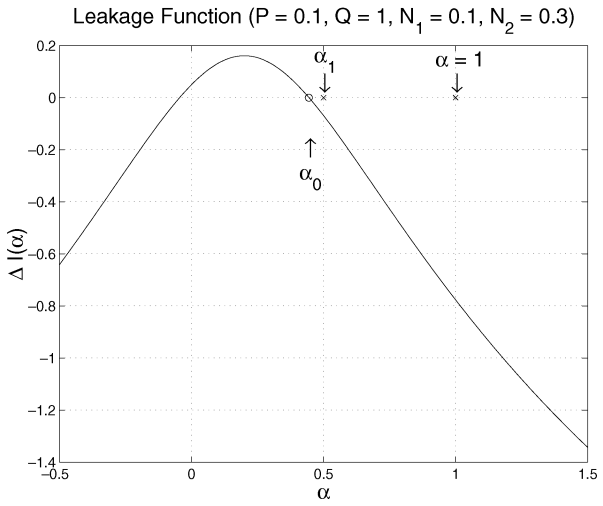


Fig. 6. Type I leakage function: $0 < \alpha_0 \le \alpha_1$.

where

$$\alpha_0 = \frac{P}{P+N_1+N_2}\left[1+\sqrt{\frac{P+Q+N_1+N_2}{Q}}\right]. \qquad (7)$$

It reaches its maximum value at

$$\alpha = \alpha_w = \frac{P}{P+N_1+N_2} < \alpha_0.$$

Hence, the leakage function has a positive value at $\alpha = 0$ and increases to its maximum value at $\alpha = \alpha_w$. It then decreases to 0 at $\alpha = \alpha_0$ and becomes negative as $\alpha$ increases. Note that when $\alpha = \alpha_w$, the capacity of the combined main-wiretap channel is reached and is equal to $C_{MW}$ while the secret message rate in the main channel is below the capacity of the main channel $C_M$, which is achieved when $\alpha = \alpha_1$ [4], where

$$C_{MW} = \frac{1}{2}\log\left[\frac{P+N_1+N_2}{N_1+N_2}\right].$$

There are three types of the leakage function characterized by the parameter $\alpha_0$ as illustrated in Figs. 6–8. *Type I* leakage function has $0 < \alpha_0 \le \alpha_1$. *Type II* leakage function has $\alpha_1 < \alpha_0 \le \alpha_2 = 1$. *Type III* leakage function has $\alpha_0 > \alpha_2 = 1$. The characteristics of the leakage function depend the system parameters $P$, $Q$, $N_1$, and $N_2$.

### C. Mode Selection

The mode of operation is selected based on the value of the leakage function. When $\Delta I(\alpha) \le 0$, the average rate used to convey partial information about the interference is greater than or equal to that used to confuse the adversary. *Mode I* can be employed so that the process of selecting an auxiliary codeword according to the interference achieves perfect secrecy automatically.

However, when $\Delta I(\alpha) > 0$, the average rate used to confuse the adversary is greater than that used to mitigate the interference. Therefore, to achieve perfect secrecy, the bin in the codebook has to contain more auxiliary codewords than what is needed to convey the partial information about the interference, and *Mode II* can be used for this situation.

If the leakage function is of *Type I*, $\Delta I(\alpha_1) \le 0$, *Mode I* can be used with $\alpha_1$ at the optimal rate $C_M - \epsilon$ for a given $\epsilon > 0$. On the other hand, if the leakage function is of *Type III*, *Mode II* can be used with $\alpha_2 = 1$ at the optimal rate $R_2 - \epsilon$ for a given $\epsilon > 0$. Now, if the leakage function is of *Type II*, neither *Mode I* nor *Mode II* can be used at their optimal rates since $\Delta I(\alpha_1) > 0$ and $\Delta I(1) \le 0$. In this

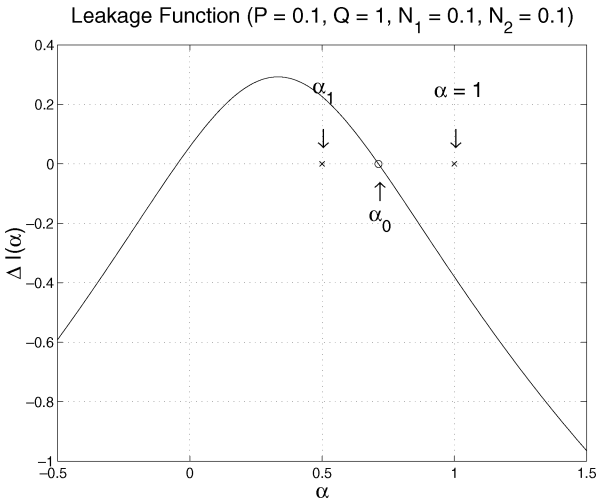


Fig. 7. Type II leakage function: $\alpha_1 < \alpha_0 \leq \alpha_2 = 1$.

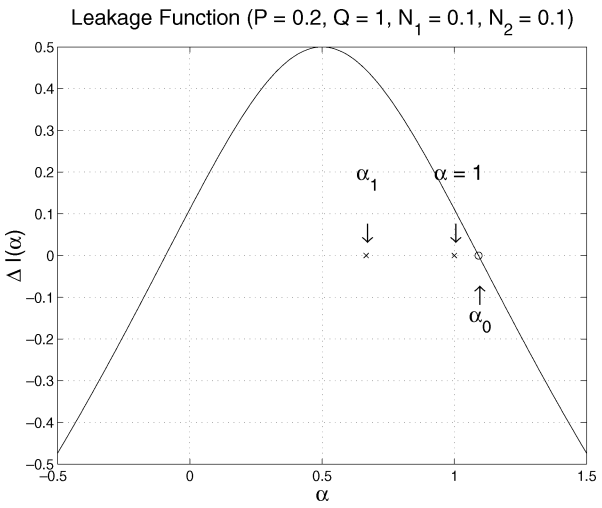


Fig. 8. Type III leakage function: $\alpha_0 > \alpha_2 = 1$.

situation, we select *Mode I* with $\alpha = \alpha_0$ so that the leakage function is zero, and the rate is $R_1 - \epsilon$ for a given $\epsilon > 0$, where

$$R_1 = \frac{1}{2}\log\left[\frac{P(P+Q+N_1)}{(P+\alpha_0^2 Q)(P+Q+N_1)-(P+\alpha_0 Q)^2}\right]. \quad (8)$$

The conditions on the leakage function can be translated into the conditions on the power constraint. The condition of using *Mode I* at the optimum rate is $\Delta I(\alpha_1) \leq 0$, which is satisfied when

$$0 \leq P \leq P_1 = -N_1 - \frac{Q}{2} + \frac{\sqrt{Q^2+4QN_2}}{2}. \quad (9)$$

Similarly, the condition for using *Mode II* at the optimum rate is $\Delta I(1) > 0$, which is satisfied when

$$P > P_2 = -\frac{Q}{2} + \frac{\sqrt{Q^2+4Q(N_1+N_2)}}{2}. \quad (10)$$

Note that when $P_1 < 0$, *Mode I* with $\alpha_1$ cannot be used, but $P_2$ is always greater than zero since $N_1$ and $N_2$ are assumed to be greater than zero. Furthermore, at $P = P_1$, $\alpha_0 = \alpha_1$ and $C_M = R_1$ since $\Delta I(\alpha_1) = 0$ at $P_1$. At $P = P_2$, $\alpha_0 = 1$ and $R_1 = R_2$ since $\Delta I(1) = 0$ at $P = P_2$. Consequently, the mode selection methodology results in a continuous rate curve when plotted as a function of the power constraint $P$.

Based on the coding strategy and the mode selection methodology, an achievable rate-equivocation region for the GWCSI is derived in the next section.

## V. An Achievable Region for the GWCSI

An achievable region for the GWCSI is obtained in three steps. In the first step,we prove achievable rates with asymptotic perfect secrecy using the proposed coding strategy. In the second step, we prove a rate-equivocation pair using thse coding strategy for the DPC. In the final step, we use the time-sharing lemma [3] to join the points in the first and second steps to obtain the whole achievable region.

### A. Achievable Rates With Asymptotic Perfect Secrecy

*Theorem 1:* For the Gaussian wiretap channel with side information with parameters $P, Q, N_1$ and $N_2$, *Modes I* and *II* can be used to achieve the following rate-equivocation pairs:

$(C_M, 1)$ for $P_1 > 0$ and $0 < P \leq P_1$;
$(R_1, 1)$ for $\max\{0, P_1\} < P \leq P_2$;
$(R_2, 1)$ for $P > P_2$;

where $C_M$, $R_1$, $R_2$, and are given by (4), (8) and (6), respectively.

*Proof:* Given $\epsilon > 0$ and the system parameters $P, Q, N_1$ and $N_2$, calculate $P_1$ and $P_2$ according to (9) and (10), respectively. The proof will be carried out in three cases corresponding to the three intervals of $P$. Each case consists of three parts for proving the rate, the probability of error and the equivocation. If $P_1 < 0$, *Case I* does not need to be considered.

*Case I:* $0 < P \leq P_1$

*Rate.* Using *Mode I* of the coding strategy with $\alpha = \alpha_1$ specified in (5), condition (1) is satisfied with rate $C_M - \epsilon$.

Probability of Error. Using the AEPs [6], it can be shown that the probability that at least one of the error events occurs can be bounded by $\epsilon$ for sufficiently small $\delta$, $\epsilon_{UV}$ and sufficiently large $N$. Hence, the condition (3) is satisfied.

*Equivocation.* In proving that the perfect secrecy can be achieved, we define random variable $W$ to represent the subbin index $w$ so that $w \in \{1, 2, \ldots, 2^{N[I(\tilde{U};V)-I(\tilde{U};\tilde{Z})+\epsilon_{UV}+\epsilon_{UZ}]}\}$, and proceed in three steps as follows (see Appendix B):

1) show that

$$H(S^K|Z^N) \geq N[I(U;Y) - I(U;Z) - I(\tilde{U};V) + I(\tilde{U};\tilde{Z}) - \epsilon_{UV} - \epsilon_{UZ}] - H(U_c|S^K, W, Z^N);$$

2) show that

$$I(U;Y) - I(U;Z) - I(\tilde{U};V) + I(\tilde{U};\tilde{Z}) - \epsilon_{UV} - \epsilon_{UZ} \geq (R-\epsilon)(1-\epsilon/2)$$

for sufficiently small $\delta$, $\epsilon_{UV}$ and $\epsilon_{UZ}$;

3) show that $H(U_c|S^K, W, Z^N)/(R-\epsilon)N \leq \epsilon/2$ for sufficiently small $\delta$ and sufficiently large $N$.

Combining the three steps:

$$\begin{aligned} H(S^K|Z^N) &\geq N[I(U;Y) - I(U;Z) - I(\tilde{U};V) + I(\tilde{U};\tilde{Z}) \\ &\quad - \epsilon_{UV} - \epsilon_{UZ}] - H(U_c|S^K, W, Z^N) \\ &\geq N(R-\epsilon)(1-\epsilon/2) - H(U_c|S^K, W, Z^N) \\ &\geq N(R-\epsilon)(1-\epsilon/2) - N(R-\epsilon)\epsilon/2 \\ \frac{H(S^K|Z^N)}{H(S^K)} &\geq (1-\epsilon/2) - \epsilon/2 = 1-\epsilon. \end{aligned}$$

Hence, for $\epsilon > 0$, pick sufficiently small $\delta > 0$, $\epsilon_{UV} > 0$, $\epsilon_{UZ} > 0$ and sufficiently large $N$, and the rate-equivocation pair $(C_M, 1)$ can be achieved by using *Mode I* with $\alpha_1$.

*Case II:* $\max\{0, P_1\} < P \leq P_2$

In this case, *Mode I* of the coding strategy is used with $\alpha = \alpha_0$, and the rate $R_1 - \epsilon$ can be reached. The probability of error and the equivocation in this case can also be bounded in similar ways as in *Case I* for sufficiently small $\delta$, $\epsilon_{UV}$, $\epsilon_{UZ}$ and sufficiently large $N$ since the proofs in *Case I* do not depend on the value of $\alpha$.

Hence, for $\epsilon > 0$, pick sufficiently small $\delta > 0$, $\epsilon_{UV} > 0$, $\epsilon_{UZ} > 0$ and sufficiently large $N$, and the rate-equivocation pair $(R_1, 1)$ can be achieved by using *Mode I* with $\alpha_0$.

*Case III:* $P > P_2$

*Rate.* Using *Mode II* of the coding strategy with $\alpha = \alpha_2 = 1$ for $\epsilon > 0$, condition (1) is satisfied, with rate $R_2 - \epsilon$.

Probability of Error. Using the AEPs [6], it can be shown that the probability that at least one of the error events occurs can be bounded by $\epsilon$ for sufficiently small $\delta$, $\epsilon_{UZ}$ and sufficiently large $N$. Hence, condition (3) is satisfied.

*Equivocation.* Using *Mode II*, we proceed with the proof of equivocation in three steps as follows (see Appendix C):

1) show that $H(S^K|Z^N) \geq N[I(U;Y) - I(U;Z)] - H(U_c|S^K, Z^N)$;

2) show that $I(U;Y) - I(U;Z) \geq (R-\epsilon)(1-\epsilon/2)$ for sufficiently small $\delta$;

3) show that $H(U_c|S^K, Z^N)/(R-\epsilon)N \leq \epsilon/2$ for sufficiently small $\delta$ and sufficiently large $N$.

Combining the above three steps as follows:

$$\begin{aligned} H(S^K|Z^N) &\geq N[I(U;Y) - I(U;Z)] - H(U_c|S^K, Z^N) \\ &\geq N(R-\epsilon)(1-\epsilon/2) - H(U_c|S^K, Z^N) \\ &\geq N(R-\epsilon)(1-\epsilon/2) - N(R-\epsilon)\epsilon/2 \\ \frac{H(S^K|Z^N)}{H(S^K)} &\geq (1-\epsilon) - \epsilon/2 = 1-\epsilon. \end{aligned}$$

Hence, for $\epsilon > 0$, pick sufficiently small $\delta > 0$, $\epsilon_{UV} > 0$ and sufficiently large $N$, and the rate-equivocation pair $(R_2, 1)$ can be achieved by using *Mode II* with $\alpha_2$. □

### B. High Rates With Low Equivocation

From the previous section, the rates arbitrarily close to the capacity of the main channel can be achieved with asymptotic perfect secrecy in *Case I*. In *Cases II* and *III*, however, the secrecy of the message has to be sacrificed if rates close to the capacity of the main channel are desired. In this section, we prove that the rate-equivocation pair $(C_M, d_C)$ is achievable by using *Mode I* with $\alpha_1$, where

$$\begin{aligned} d_C &= 1 - \frac{I(\tilde{U};\tilde{Z})}{C_M} \qquad (11) \\ &= 1 - \frac{1}{2C_M} \\ &\quad \log\left[\frac{(P+\alpha_1^2 Q)(P+Q+N_1+N_2)}{(P+\alpha_1^2 Q)(P+Q+N_1+N_2)-(P+\alpha_1 Q)^2}\right]. \qquad (12) \end{aligned}$$

*Theorem 2:* For the Gaussian wiretap channel with side information with parameters $P$, $Q$, $N_1$ and $N_2$, *Mode I* with $\alpha_1$ can be used to achieve the rate-equivocation pair $(C_M, d_C)$.

*Proof:* When *Mode I* with $\alpha_1$ is used, the rate is $C_M - \epsilon$ for $\epsilon > 0$. Furthermore, the probability of error can also be bounded by $\epsilon$ provided sufficiently small $\delta$, $\epsilon_{UV}$, $\epsilon_{UZ}$ and sufficiently large $N$.

Now, the equivocation can be calculated as follows:

$$\begin{aligned} H(S^K|Z^N) &= H(S^K, Z^N) - H(Z^N) \\ &= H(S^K, U_c, Z^N) - H(U_c|S^K, Z^N) - H(Z^N) \\ &= H(S^K|U_c, Z^N) + H(U_c|Z^N) \\ &\quad - H(U_c|S^K, Z^N) \\ &\overset{(1)}{\geq} H(U_c|Z^N) - H(U_c|S^K, Z^N) \\ &\overset{(2)}{\geq} H(U_c|Z^N) - N[I(\tilde{U};V) + \epsilon_{UV}] \\ &\overset{(3)}{\geq} H(U_c|Z^N) - H(U_c|Y^N) - N[I(\tilde{U};V) \\ &\quad + \epsilon_{UV}] \\ &= [H(U_c, Z^N) - H(Z^N)] - [H(U_c, Y^N) \\ &\quad - H(Y^N)] - N[I(\tilde{U};V) + \epsilon_{UV}] \\ &= [H(U_c) + H(Z^N|U_c) - H(Z^N)] \\ &\quad - [H(U_c) + H(Y^N|U_c) - H(Y^N)] \\ &\quad - N[I(\tilde{U};V) + \epsilon_{UV}] \\ &\overset{(4)}{=} [H(Z^N|U_c) - H(Z^N|U^N) - H(U^N) \\ &\quad + H(U^N|Z^N)] - [H(Y^N|U_c) - H(Y^N|U^N) \\ &\quad - H(U^N) + H(U^N|Y^N)] - N[I(\tilde{U};V) \\ &\quad + \epsilon_{UV}] \\ &\overset{(5)}{=} H(U^N|Z^N) - H(U^N|Y^N) - N[I(\tilde{U};V) \\ &\quad + \epsilon_{UV}] \\ &= I(U^N;Y^N) - I(U^N;Z^N) - N[I(\tilde{U};V) \\ &\quad + \epsilon_{UV}] \\ &= N[I(U;Y) - I(\tilde{U};V) - I(U;Z) - \epsilon_{UV}]. \end{aligned}$$

(1) follows from the fact that $H(S^K|U_c, Z^N) \geq 0$; (2) follows from the fact that there are $2^{N[I(\tilde{U};V)+\epsilon_{UV}]}$ auxiliary codewords in a bin; (3) follows from the fact that $H(U_c|Y^N) \geq 0$; (4) follows from the fact that $H(Z^N) = H(U^N) + H(Z^N|U^N) - H(U^N|Z^N)$ and $H(Y^N) = H(U^N) + H(Y^N|U^N) - H(U^N|Y^N)$; (5) follows from the fact that $H(Y^N|U_c) = H(Y^N|U^N)$ and $H(Z^N|U_c) = H(Z^N|U^N)$.

Now, we know that

$$\begin{aligned} I(U;Y) - I(\tilde{U};V) - I(U;Z) + I(\tilde{U};\tilde{Z}) - \epsilon_{UV} \\ = I(\tilde{U};\tilde{Y}) - I(\tilde{U};V) - \epsilon_{UV} = C_M - \epsilon_{UV} \end{aligned}$$

when $\delta = 0$ since $\alpha = \alpha_1$. By imposing the condition $\epsilon_{UV} < \epsilon C_M$, $C_M - \epsilon_{UV} > C_M(1-\epsilon)$. Therefore, for $\delta = 0$, $I(U;Y) - I(\tilde{U};V) - I(U;Z) + I(\tilde{U};\tilde{Z}) - \epsilon_{UV} > C_M(1-\epsilon)$. Since $I(U;Y) - I(\tilde{U};V) - I(U;Z) + I(\tilde{U};\tilde{Z}) - \epsilon_{UV}$ is continuous, and $C_M(1-\epsilon)$ is constant with respect to $\delta$, for sufficiently small $\delta > 0$

$$\begin{aligned} I(U;Y) - I(\tilde{U};V) - I(U;Z) + I(\tilde{U};\tilde{Z}) - \epsilon_{UV} &> C_M(1-\epsilon) \\ I(U;Y) - I(\tilde{U};V) - I(U;Z) - \epsilon_{UV} &> C_M(1-\epsilon) \\ &\quad - I(\tilde{U};\tilde{Z}). \end{aligned}$$

Hence

$$\begin{aligned} H(S^K|Z^N) &> N[C_M(1-\epsilon) - I(\tilde{U};\tilde{Z})] \\ &= NC_M\left[1 - \frac{I(\tilde{U};\tilde{Z})}{C_M} - \epsilon\right] \\ &> N(C_M - \epsilon)\left[1 - \frac{I(\tilde{U};\tilde{Z})}{C_M} - \epsilon\right] \\ \frac{H(S^K|Z^N)}{N(C_M-\epsilon)} &> \left[1 - \frac{I(\tilde{U};\tilde{Z})}{C_M} - \epsilon\right] \\ &> d_C - \epsilon. \end{aligned}$$

The theorem follows by setting appropriate constants $\delta > 0, \epsilon_{UV} > 0, \epsilon_{UZ} > 0$ and $N$. □

### C. Time-Sharing Lemma

The time-sharing lemma was used in [3] to prove the achievable region for the GWC. We will also use it in our derivation of an achievable region for the GWCSI.

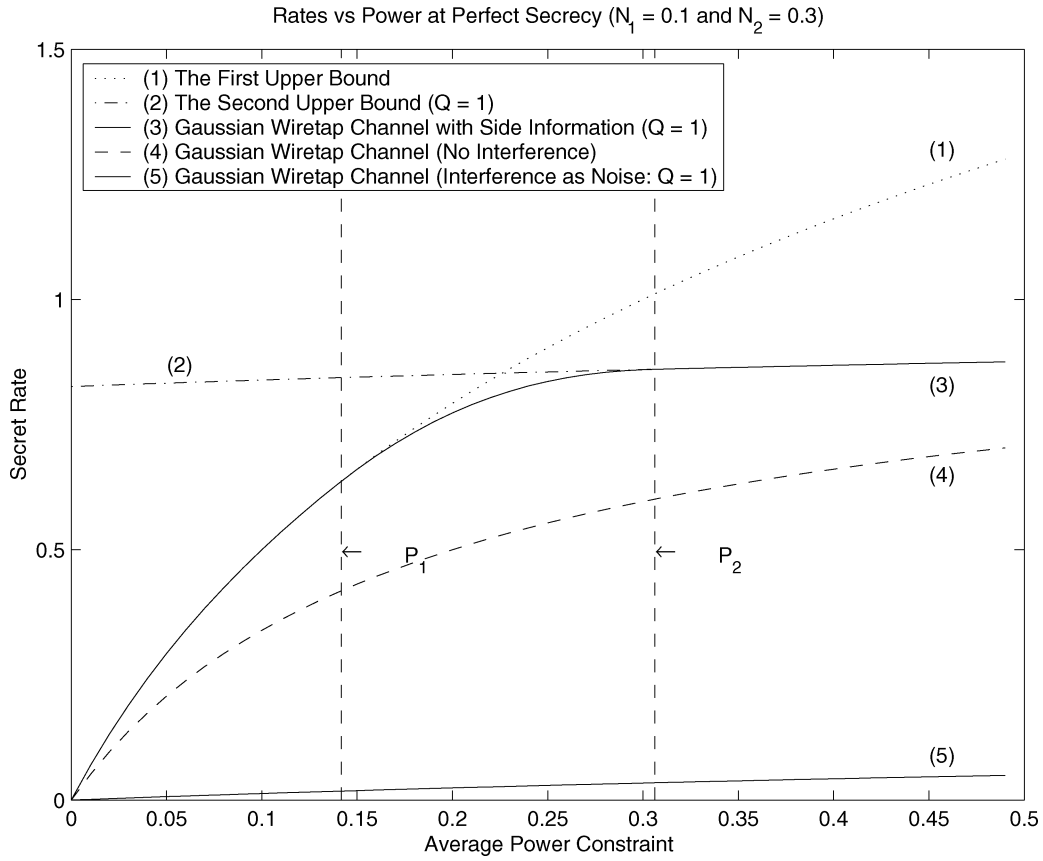


Fig. 9. Performance Comparison: $P_1 > 0$.

*Lemma 1:* [3] Let $R_1 d_1 = R_2 d_2 = c$, a constant. Assume $R_1 > R_2$ and hence $d_1 < d_2$. If the points $(R_1, d_1)$ and $(R_2, d_2)$ are achievable, then by time-sharing any point $(R, d)$ with $R_2 \leq R \leq R_1$, $d_1 \leq d \leq d_2$, and $Rd = c$ is achievable.

*Theorem 3:* For the Gaussian wiretap channel with side information, a rate-equivocation pair $(R, d)$ is achievable if

$$\begin{aligned} R &\leq C_M \\ d &\leq 1 \\ Rd &\leq \begin{cases} C_M & 0 < P \leq P_1 \\ \min\{C_M d_C, R_1\} & P_1 < P \leq P_2. \\ \min\{C_M d_C, R_2\} & P > P_2 \end{cases} \end{aligned}$$

*Proof:* For $0 < P \leq P_1$, *Mode I* with $\alpha_1$ can be used to achieve the pair $(C_M, 1)$. Using codes that perform worse than that in *Mode I* with $\alpha_1$ achieves the pairs dominated by $(C_M, 1)$.

For $P_1 < P \leq P_2$, if $R_1 \leq C_M d_C$, time-share the code in *Mode I* with $\alpha_0$ with the code achieving the pair $(C_M, R_1/C_M)$. Otherwise, time-share the codes achieving the pairs $(C_M d_C, 1)$ and $(C_M, d_C)$.

For $P > P_2$, if $R_2 \leq C_M d_C$, time-share the code in *Mode II* with $\alpha_2$ with the code achieving the pair $(C_M, R_2/C_M)$. Otherwise, time-share the codes achieving the pairs $(C_M d_C, 1)$ and $(C_M, d_C)$. □

## VI. Bounds on the Rates With Asymptotic Perfect Secrecy

In this section, we look at the optimality of the rates with asymptotic perfect secrecy by considering upper and lower bounds. We then compare the performance of the proposed coding strategy with the bounds.

### A. Upper and Lower Bounds

A lower bound can be obtained by considering the interference as an additional noise in the main channel unknown to the sender. Accordingly, this is the case of the GWC with main channel noise variance $Q + N_1$ as opposed to $N_1$. The rate with asymptotic perfect secrecy of transmission is (plotted as curve (5) for $\mathrm{Q} = 1$ in Figs. 9 and 10)

$$I(\tilde{X};\tilde{Y}) - I(\tilde{X};\tilde{Z}) = \frac{1}{2}\log\left[\frac{(P+Q+N_1)(Q+N_1+N_2)}{(Q+N_1)(P+Q+N_1+N_2)}\right].$$

The first upper bound on the rate of transmission is the capacity of the main channel $C_M$, which is plotted as curve (1) in Figs. 9 and 10. The second upper bound can be derived by considering the interference as part of the codeword generated by the encoder implying that the encoder has a power limit of $P + Q$ without interference in the main channel. Under this consideration, the channel becomes the GWC with power constraint $P + Q$. The capacity of this channel dominates all the achievable rates associated with the GWCSI since the encoder in this case has an additional power $Q$ for transmission at its disposal. The second upper bound, therefore, is

$$I(\tilde{X};\tilde{Y}) - I(\tilde{X};\tilde{Z}) = \frac{1}{2}\log\left[\frac{(P+Q+N_1)(N_1+N_2)}{(N_1)(P+Q+N_1+N_2)}\right].$$

This upper bound is plotted as curve (2) for $Q = 1$ in Figs. 9 and 10.

### B. Performance Comparison

For performance comparison, we plot the rates with perfect secrecy achieved by the proposed coding strategy for the GWCSI with $Q = 1$ as curve (3) in Figs. 9 and 10. We can see that the rates coincide with the upper bound (1) for $0 < P \leq P_1$ and upper bound (2) for $P \geq P_2$. They however are below the upper bounds for $\max\{0, P_1\} < P < P_2$, and the optimality of the coding scheme in this region is still unknown.

As a reference, we plot the capacity of the GWC with the same $P$, $N_1$ and $N_2$ as in the case of GWCSI as curve (4) in Figs. 9 and 10. We

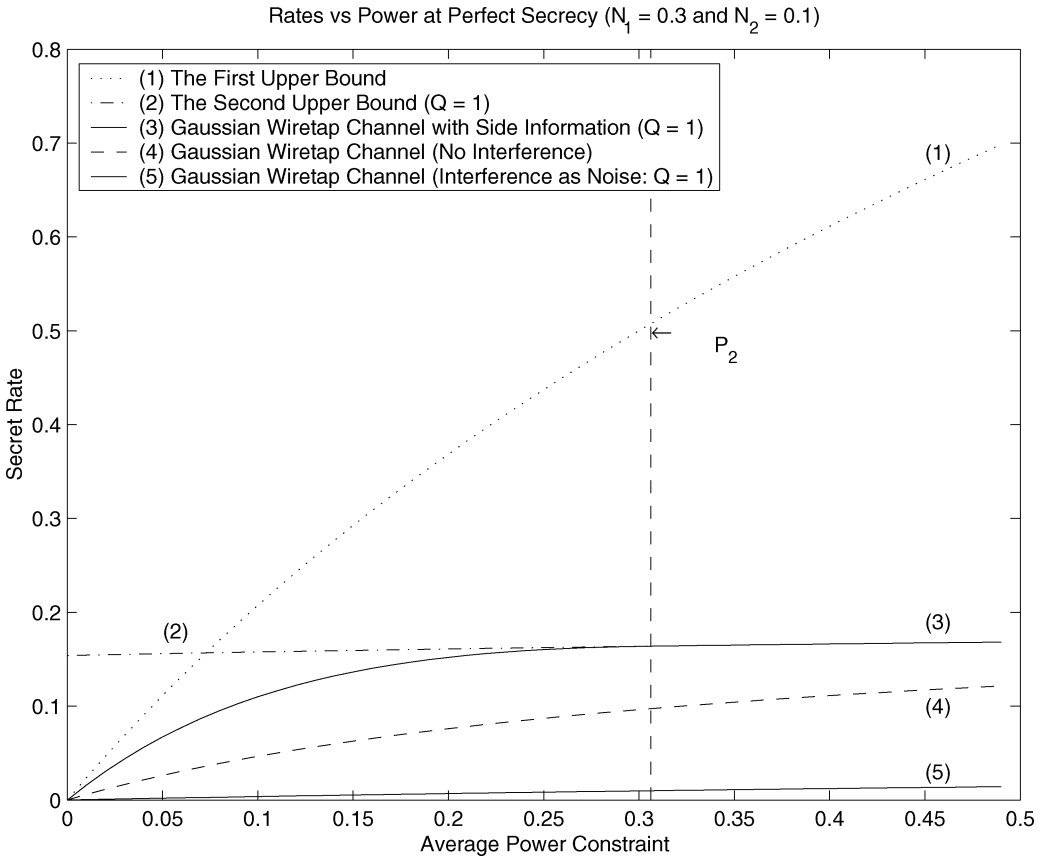


Fig. 10. Performance Comparison: $P_1 \leq 0$.

can see that the achievable rates for the GWCSI (curves (3)) dominate the rates for the GWC (curve (4)) in this particular case.

## VII. Conclusion

We introduce the GWCSI model as an extension of the GWC and the DPC. A Coding strategy consisting of two operating modes is proposed for the GWCSI. A leakage function for the GWCSI is introduced and used as a criteria for mode selection. *Mode I* with $\alpha_1$ and *Mode II* with $\alpha_2$ are shown to be optimal for the GWCSI. In *Mode I* with $\alpha_1$, the capacity of the main channel can be achieved with perfect secrecy. In *Mode II* with $\alpha_2$, the power of the interference $Q$, in addition to the transmission power $P$, is used to confuse the wiretapper even though the interference cannot be controlled by the encoder. The rates in this mode therefore reach the upper bound, given by the GWC with transmission power $P+Q$, with perfect secrecy. The optimality of the proposed coding strategy for the region $\max\{0, P_1\} < P < P_2$ is still unknown. An achievable region is derived based on the proposed coding strategy and the time-sharing lemma.

## Appendix A
## The Condition on the Average Power Constraint

We apply the following Lemma to the condition on the average power constraint by letting $P' = P(1+4\delta\ln(2))^{-1}$.

*Lemma A.1:* Let $X^N$ and $V^N$ be two independent sequences of i.i.d. random variables $X \sim \mathcal{N}(0,\sigma_X^2)$ and $V \sim \mathcal{N}(0,\sigma_V^2)$, respectively. Let $U^N = X^N + \alpha V^N$ for a constant real number $\alpha$. If $(u^N, v^N) \in T^N_{U,V}(\delta)$, for any $\delta > 0$, and $\sigma_X^2 \leq P(1+4\delta\ln(2))^{-1}$, then $[\sum_{i=1}^N x_i^2]/N \leq P$.

*Proof:* Since $X^N$ and $V^N$ are two independent sequences of i.i.d. Gaussian random variables, $U^N$ is a sequence of i.i.d. Gaussian random variables drawn according to $\mathcal{N}(0, \sigma_X^2 + \alpha^2\sigma_V^2)$. Furthermore, $(u^N, v^N) \in T^N_{U,V}(\delta)$ implies that

$$
\begin{aligned}
\delta &> \left| -\frac{1}{N}\log p(u^N, v^N) - H(U,V) \right| \\
&= \left| -\frac{1}{N}\log p(u^N, v^N) - H(V) - H(U|V) \right| \\
&= \left| -\frac{1}{N}\log p(u^N, v^N) - H(V) - H(X) \right| \\
2\delta &> \left| -\frac{1}{N}\log p(u^N, v^N) + \frac{1}{N}\log p(v^N) - H(X) \right| \\
&= \left| -\frac{1}{N}\log p(u^N|v^N) - H(X) \right| \\
&= \left| -\frac{1}{N}\log p(x^N) - H(X) \right| \\
&= \left| -\frac{1}{N}\sum_{i=1}^N \log p(x_i) - \frac{1}{2}\log(2\pi e\sigma_x^2) \right| \\
&= \frac{1}{\ln(2)}\left| \frac{1}{N}\sum_{i=1}^N \left[ \frac{x_i^2}{2\sigma_x^2} + \frac{1}{2}\ln(2\pi\sigma_x^2) \right] - \frac{1}{2}\ln(2\pi e\sigma_x^2) \right| \\
&= \frac{1}{\ln(2)}\left| \frac{1}{N}\sum_{i=1}^N \frac{x_i^2}{2\sigma_x^2} - \frac{1}{2} \right| \\
&= \frac{1}{\ln(2)}\left| \frac{\langle x^N, x^N\rangle}{2N\sigma_x^2} - \frac{1}{2} \right|
\end{aligned}
$$

$$4\delta\ln(2) > \left|\frac{\langle x^N, x^N\rangle}{N\sigma_x^2} - 1\right|$$

$$\frac{\langle x^N, x^N\rangle}{N} < \sigma_X^2[1+4\delta\ln(2)] \le \frac{P}{1+4\delta\ln(2)}[1+4\delta\ln(2)]$$

$$\frac{1}{N}\sum_{i=1}^{N} x_i^2 \le P. \qquad \square$$

## Appendix B
## Proof of the Equivocation in *Case I*

We proceed to the three steps as follows:

$$\begin{aligned}
H(S^K|Z^N) &\overset{(1)}{=} H(S^K, W|U_c, Z^N) + H(U_c|Z^N) \\
&\quad - H(U_c|S^K, W, Z^N) - H(W|S^K, Z^N) \\
&\overset{(2)}{\ge} H(U_c|Z^N) - H(U_c|S^K, W, Z^N) \\
&\quad - H(W|S^K, Z^N) \\
&\overset{(3)}{\ge} H(U_c|Z^N) - H(U_c|Y^N) \\
&\quad - H(W|S^K, Z^N) - H(U_c|S^K, W, Z^N) \\
&= [H(U_c, Z^N) - H(Z^N)] - [H(U_c, Y^N) \\
&\quad - H(Y^N)] - H(W|S^K, Z^N) \\
&\quad - H(U_c|S^K, W, Z^N) \\
&= [H(U_c) + H(Z^N|U_c) - H(Z^N)] \\
&\quad - [H(U_c) + H(Y^N|U_c) - H(Y^N)] \\
&\quad - H(W|S^K, Z^N) - H(U_c|S^K, W, Z^N) \\
&\overset{(4)}{=} [H(Z^N|U_c) - H(Z^N|U^N) \\
&\quad - H(U^N) + H(U^N|Z^N)] \\
&\quad - [H(Y^N|U_c) - H(Y^N|U^N) \\
&\quad - H(U^N) + H(U^N|Y^N)] \\
&\quad - H(W|S^K, Z^N) - H(U_c|S^K, W, Z^N) \\
&\overset{(5)}{=} H(U^N|Z^N) - H(U^N|Y^N) \\
&\quad - H(W|S^K, Z^N) - H(U_c|S^K, W, Z^N) \\
&= I(U^N; Y^N) - I(U^N; Z^N) \\
&\quad - H(W|S^K, Z^N) - H(U_c|S^K, W, Z^N) \\
&\overset{(6)}{\ge} I(U^N; Y^N) - I(U^N; Z^N) \\
&\quad - N[I(\tilde{U};V) - I(\tilde{U};\tilde{Z}) + \epsilon_{UV} + \epsilon_{UZ}] \\
&\quad - H(U_c|S^K, W, Z^N) \\
&\overset{(7)}{=} N[I(U;Y) - I(U;Z) - I(\tilde{U};V) + I(\tilde{U};\tilde{Z}) \\
&\quad - \epsilon_{UV} - \epsilon_{UZ}] - H(U_c|S^K, W, Z^N).
\end{aligned}$$

(1) follows from $H(A|B) = H(A,B) - H(B)$ and $H(A,B) = H(A,B,C) - H(C|A,B)$; (2) follows from $H(S^K, W|U_c, Z^N) \ge 0$; (3) follows from $H(U_c|Y^N) \ge 0$; (4) follows from the fact that $H(Z^N) = H(U^N) + H(Z^N|U^N) - H(U^N|Z^N)$ and $H(Y^N) = H(U^N) + H(Y^N|U^N) - H(U^N|Y^N)$; (5) follows from the fact that $H(Y^N|U_c) = H(Y^N|U^N)$ and $H(Z^N|U_c) = H(Z^N|U^N)$. (6) follows from the number of subbins in a bin. (7) follows from the i.i.d. properties of $U^N$, $Y^N$ and $Z^N$.

In Step 2), we note that $R - \epsilon = I(\tilde{U};\tilde{Y}) - I(\tilde{U};V) - \epsilon$ and therefore $(R-\epsilon)(1-\epsilon/2)$ is parabolic in $\epsilon$, with the minimum at $\epsilon = 1 + [I(\tilde{U};\tilde{Y}) - I(\tilde{U};V)]/2$. Furthermore, $(R-\epsilon)(1-\epsilon/2) = I(\tilde{U};\tilde{Y}) - I(\tilde{U};V)$ when $\epsilon = 0$ or $2 + I(\tilde{U};\tilde{Y}) - I(\tilde{U};V)$. Hence, $(R-\epsilon)(1-\epsilon/2) < I(\tilde{U};\tilde{Y}) - I(\tilde{U};V)$ when $\epsilon \in (0, 2 + I(\tilde{U};\tilde{Y}) - I(\tilde{U};V))$. The condition $\epsilon_{UV} + \epsilon_{UZ} < [I(\tilde{U};\tilde{Y}) - I(\tilde{U};V)] - R(1-\epsilon/2)$ can then be imposed on $\epsilon_{UV}$ and $\epsilon_{UZ}$ in the interval. It implies that

$$\begin{aligned}
(R-\epsilon)(1-\epsilon/2) + \epsilon_{UV} + \epsilon_{UZ} - I(\tilde{U};\tilde{Z}) + I(\tilde{U};V) \\
< I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z}).
\end{aligned} \tag{13}$$

On the other hand, for $\delta > 0$

$$I(U;Y) - I(U;Z) < I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z}). \tag{14}$$

Since $I(U;Y) - I(U;Z)$ is continuous in $\delta$ with the value of $I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z})$ at $\delta = 0$, and $(R-\epsilon)(1-\epsilon/2) + \epsilon_{UV} + \epsilon_{UZ} - I(\tilde{U};\tilde{Z}) + I(\tilde{U};V)$ is continuous and constant in $\delta$ with the value less than $I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z})$. If the two curves do not intersect, then there is no constraint on $\delta$. However, if the two curves intersect, then $0 < \delta < \delta^*$, where $\delta^*$ is the smallest value such that the two curves intersect. Then the condition on $\delta$ becomes $0 < \delta < \delta_0$, where $\delta_0 = \min\{\delta^*, \infty\}$. Thus

$$\begin{aligned}
I(U;Y) - I(U;Z) - I(\tilde{U};V) + I(\tilde{U};\tilde{Z}) - \epsilon_{UV} - \epsilon_{UZ} \\
\ge (R-\epsilon)(1-\epsilon/2)
\end{aligned}$$

when

$$\begin{aligned}
\epsilon &\in (0, 2 + I(\tilde{U};\tilde{Y}) - I(\tilde{U};V)), \\
\epsilon_{UV} + \epsilon_{UZ} &< [I(\tilde{U};\tilde{Y}) - I(\tilde{U};V)] - R(1-\epsilon/2), \\
\delta &< \delta_0.
\end{aligned}$$

Note that for $\epsilon \ge 2 + I(\tilde{U};\tilde{Y}) - I(\tilde{U};V)$, $I(\tilde{U};\tilde{Y}) - I(\tilde{U};V) - \epsilon < 0$, $1 - \epsilon < 0$, $\epsilon > 1$, and there is nothing to prove.

In Step 3), the wiretapper's decoding process is considered. The term $H(U_c|S^K, W, Z^N)$ is the entropy of the auxiliary codeword given the wiretapper's observation, the bin and the subbin in which the auxiliary codeword is. It can be bounded by using Fano's inequality as follows:

$$H(U_c|S^K, W, Z^N) \le h(P_{SB}) + P_{SB} N I(\tilde{U};\tilde{Z}),$$

where $h(\cdot)$ is the binary entropy function, and $P_{SB}$ is the probability of error in decoding $Z^N$ for $U_c$ given $S^K$ and $W$ (subbin decoding), and therefore

$$\frac{H(U_c|S^K, W, Z^N)}{H(S^K)} \le \frac{h(P_{SB}) + P_{SB} N I(\tilde{U};\tilde{Z})}{(R-\epsilon)N}. \tag{15}$$

The conditional entropy can be bounded by via bounding the wiretapper's probability of error in the subbin decoding. $P_{SB}$ can be made arbitrarily small given sufficiently small $\delta$ and sufficiently large $N$ via the AEPs since there are $2^{N[I(\tilde{U};\tilde{Z}) - \epsilon_{UZ}]}$ sequences in a subbin which is exponentially smaller than $2^{N I(\tilde{U};\tilde{Z})}$.

## Appendix C
## Proof of the Equivocation in *Case III*

We proceed to the three steps as follows:

$$\begin{aligned}
H(S^K|Z^N) &\overset{(1)}{=} H(U_c, Z^N) + H(S^K|U_c, Z^N) \\
&\quad - H(U_c|S^K, Z^N) - H(Z^N) \\
&\overset{(2)}{\ge} H(U_c|Z^N) - H(U_c|S^K, Z^N) \\
&\overset{(3)}{\ge} H(U_c|Z^N) - H(U_c|Y^N) - H(U_c|S^K, Z^N) \\
&\overset{(4)}{=} H(U^N|Z^N) - H(U^N|Y^N) \\
&\quad - H(U_c|S^K, Z^N) \\
&= I(U^N; Y^N) - I(U^N; Z^N) - H(U_c|S^K, Z^N) \\
&\overset{(5)}{=} N[I(U;Y) - I(U;Z)] - H(U_c|S^K, Z^N).
\end{aligned}$$

(1) follows from $H(A|B) = H(A,B) - H(B)$ and $H(A,B) = H(A,B,C) - H(C|A,B)$; (2) follows from $H(S^K|U_c, Z^N) \ge 0$; (3) follows from $H(U_c|Y^N) \ge 0$; (4) follows from the fact that

$H(Y^N|U_c) = H(Y^N|U^N)$ and $H(Z^N|U_c) = H(Z^N|U^N)$; (5) follows from the i.i.d. properties of $U^N$, $Y^N$ and $Z^N$.

In Step 2), we note that $R - \epsilon = I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z}) - \epsilon$ and therefore $(R-\epsilon)(1-\epsilon/2)$ is parabolic in $\epsilon$, with the minimum at $\epsilon = 1 + [I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z})]/2$. Furthermore, $(R-\epsilon)(1-\epsilon/2) = I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z})$ when $\epsilon = 0$ or $2 + I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z})$. Hence, $(R-\epsilon)(1-\epsilon/2) < I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z})$ when $\epsilon \in (0, 2 + I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z}))$.

On the other hand, for $\delta > 0$

$$I(U;Y) - I(U;Z) < I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z}). \tag{16}$$

Since $I(U;Y) - I(U;Z)$ is continuous in $\delta$ with the value of $I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z})$ at $\delta = 0$, and $(R-\epsilon)(1-\epsilon/2)$ is continuous and constant in $\delta$ with the value less than $I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z})$. If the two curves do not intersect, then there is no constraint on $\delta$. However, if the two curves intersect, then $0 < \delta < \delta^*$, where $\delta^*$ is the smallest value such that the two curves intersect. Then the condition on $\delta$ becomes $0 < \delta < \delta_0$, where $\delta_0 = \min\{\delta^*, \infty\}$. Thus

$$I(U;Y) - I(U;Z) \geq (R-\epsilon)(1-\epsilon/2)$$

when

$$\epsilon \in (0, 2 + I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z}))$$
$$\delta < \delta_0.$$

Note that for $\epsilon \geq 2 + I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z}), I(\tilde{U};\tilde{Y}) - I(\tilde{U};\tilde{Z}) - \epsilon < 0$, $1 - \epsilon < 0$, $\epsilon > 1$, and there is nothing to prove.

In step 3, the wiretapper's decoding process is considered. The term $H(U_c|S^K, Z^N)$ is the entropy of the auxiliary codeword given the wiretapper's observation and the bin in which the auxiliary codeword is. It can be bounded by using Fano's inequality as follows:

$$H(U_c|S^K, Z^N) \leq h(P_B) + P_B N I(\tilde{U};\tilde{Z}),$$

where $h(\cdot)$ is the binary entropy function, and $P_B$ is the probability of error in decoding $Z^N$ for $U_c$ given $S^K$, and therefore

$$\frac{H(U_c|S^K, Z^N)}{H(S^K)} \leq \frac{h(P_B) + P_B N I(\tilde{U};\tilde{Z})}{(R-\epsilon)N}. \tag{17}$$

The conditional entropy can be bounded by via bounding the wiretapper's probability of error in the bin decoding. $P_B$ can be made arbitrarily small given sufficiently small $\delta$ and sufficiently large $N$ via the AEPs since there are $2^{N[I(\tilde{U};\tilde{Z})-\epsilon_{UZ}]}$ sequences in a subbin which is exponentially smaller than $2^{NI(\tilde{U};\tilde{Z})}$.

## ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers for their valuable comments that help improve the quality 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] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Lab. Tech. J.*, vol. 63, pp. 2135–2157, Dec. 1984.
[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, pp. 451–456, Jul. 1978.
[4] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. IT-29, pp. 439–441, May 1983.
[5] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Probl. Contr. Inf. Theory*, vol. 9, no. 1, pp. 19–31, 1980.
[6] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

# Feedback Rate-Capacity Loss Tradeoff for Limited Feedback MIMO Systems

Amir D. Dabbagh, *Student Member, IEEE,* and David J. Love, *Member, IEEE*

***Abstract*—Multiple-input–multiple-output (MIMO) communication systems can provide large capacity gains over traditional single-input–single-output (SISO) systems and are expected to be a core technology of next generation wireless systems. Often, these capacity gains are achievable only with some form of adaptive transmission. In this paper, we study the capacity loss (defined as the rate loss in bits/s/Hz) of the MIMO wireless system when the covariance matrix of the transmitted signal vector is designed using a low rate feedback channel. For the MIMO channel, we find a bound on the ergodic capacity loss when random codebooks, generated from the uniform distribution on the complex unit sphere, are used to convey the second order statistics of the transmitted signal from the receiver to the transmitter. In this case, we find a closed-form expression for the ergodic capacity loss as a function of the number of bits fed back at each channel realization. These results show that the capacity loss decreases at least as $O\left(2^{-B/(2MM_t-2)}\right)$ where $B$ is the number of feedback bits, $M_t$ is the number of transmit antennas, and $M = \min\{M_r, M_t\}$ where $M_r$ is the number of receive antennas. In the high SNR regime, we present a new bound on the capacity loss that is tighter than the previously derived bound and show that the capacity loss decreases exponentially as a function of the number of feedback bits.**

***Index Terms*—Adaptive modulation, capacity loss, limited feedback, multiple-input–multiple-output (MIMO) systems, Rayleigh channels.**

## I. INTRODUCTION

Because of their capacity and quality benefits, multiple-input–multiple-output (MIMO) wireless systems are expected to be a core technology in next evolution third-generation (3G) and fourth-generation (4G) wireless systems. In addition, the performance of MIMO systems can be significantly improved by adapting the transmitted signal to the current channel conditions (see, for example, the discussion in [1]). When the channel cannot be estimated at the transmitter, such as is the case in frequency division duplexing, systems can employ a feedback link to convey quantized channel state information (CSI) and obtain capacity performance close to the scenario when the transmitter perfectly knows the channel. The feedback rate, however, must be chosen judiciously because the feedback channel may only support a small data rate and the feedback bits are allocated as overhead on the reverse data path. To satisfy these rate constraints, low-rate (or limited) feedback has been studied in various scenarios and special cases [2]–[18]. These techniques include feedback adaptation techniques specific to transmit beamforming [6]–[8], precoded orthogonal space-time block coding [9], [11], [12], [16], and precoded spatial multiplexing [14]. Initial performance analysis of some of these techniques was given in [8], [9], and [13]. The basic idea is that a limited number of feedback bits representing some sort of CSI are transmitted from the receiver to the transmitter. The transmitter uses this small number of bits to adapt

Manuscript received March 17, 2005; revised October 11, 2005. This work was supported in part by the SBC Foundation and the National Science Foundation under Grant CCF0513916. The material in this correspondence was presented in part at the IEEE Vehicular Technology Conference, Dallas, TX, September 25–28, 2005 and the IEEE Global Telecommunications Conference, St. Louis, MO, November 28–December 2, 2005.

The authors are with the Center for Wireless Systems and Applications, School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA (email: adabbagh@ecn.purdue.edu; djlove@ecn.purdue.edu).

Communicated by R. R. Müller, Associate Editor for Communications.
Digital Object Identifier 10.1109/TIT.2006.872864