Guaranteeing Secrecy using Artificial Noise with Quantized Channel Feedback

Shih-Chun Lin, Tsung-Hui Chang, Yan-Lang Liang, Yao-Win Peter Hong and Chong-Yung Chi

This work was supported by the National Science Council, Taiwan, R.O.C., under grant NSC-98-2219-E-007-004, NSC-98-2218-E-009-008-MY3, NSC-98-2219-E-007-005 and NSC-98-2219-E-007-003. Part of this work was presented at the IEEE International Symposium on Information Theory (ISIT), Seoul, Korea, June-July, 2009.

The authors are with Institute of Communications Engineering and Department of Electrical Engineering, National Tsing Hua University, Hsinchu, Taiwan 30013, R.O.C.

E-mails : {linsc,changth}@mx.nthu.edu.tw, ylliang@erdos.ee.nthu.edu.tw, {ywhong,cychi}@ee.nthu.edu.tw

Guaranteeing Secrecy using Artificial Noise with Quantized Channel Feedback

Abstract

The impact of quantized channel direction feedback on the achievable secrecy rate is studied for multiple-antenna wiretap channels. Without knowledge of the eavesdropper's channel, we consider the scheme proposed by Goel and Negi where artificial noise (AN) is imposed in the null space of the legitimate receiver's channel to disrupt the eavesdropper's reception and, thus, guarantee secrecy. It has been shown that the secrecy rate can be made arbitrarily large by increasing the transmission power when perfect knowledge of the legitimate receiver's channel direction information (CDI) is available at the transmitter. However, in practice, this is difficult to achieve due to rate-limitations on the feedback channel. When only quantized CDI is available at the transmitter, the AN that is only intended to disrupt the eavesdropper's reception may leak into the legitimate receiver's channel, causing serious loss in the secrecy rate. Specifically, with quantized CDI, we show that the achievable secrecy rate will now be upper-bounded by a constant and the optimal power allocation between signal and AN must now be more conservative to take into consideration the effects of AN leakage. To overcome the significant rate loss compared to the perfect CDI case, we show that the number of feedback bits must scale at least logarithmically with the transmission power to maintain a constant rate loss. Moreover, we also show that additional channel quality information at the transmitter gains little at the high power regime. These theoretical claims are verified by computer simulations.

I. Introduction

Physical-layer secrecy was first introduced by Wyner [1] under the notion of wiretap channels that typically consist of a transmitter, a legitimate receiver, and an eavesdropper. Recent studies of physical-layer secrecy in the wireless channel have shown that, under perfect secrecy constraints, a non-zero secrecy capacity can always be achieved in fading environments [2] [3]. With

advances in multiple-input multiple-output (MIMO) technologies, the secrecy capacity achievable in wireless channels have been further enhanced with multiple antennas at the transmitters and/or at the receivers, e.g., in [4]–[6]. To guarantee secrecy without knowledge of the eavesdropper's channel state information, Goel and Negi proposed in [5] the use of artificial noise (AN) in the left null space of the legitimate receiver's channel to disrupt the eavesdropper's reception. It has been shown that the secrecy rate achievable by imposing AN can be made arbitrarily large by increasing the transmission power. However, this result relies on perfect knowledge of the legitimate receiver's channel direction information (CDI) at the transmitter, which is typically hard to attain in practice.

The main contribution in this document is to study the impact of quantized CDI on the achievable secrecy rate under AN-assisted beamforming. The effect of quantized channel feedback on transceiver design has been studied extensively in the literature for both single user and multi-user multiple-input, multiple-output (MIMO) downlink systems (without eavesdroppers), e.g., in [7]–[9] and references within. To study the effect of quantized channel feedback on secrecy capacity, we consider the case where the CDI at the transmitter is provided through a rate-limited feedback channel from the legitimate receiver. When only quantized CDI is available at the transmitter, the AN that is originally intended to disrupt the eavesdropper's reception may leak into the legitimate receiver's channel, causing significant loss in the achievable secrecy rate. In this document, we first focus our studies on the multiple-input single-output single-eavesdropper (MISOSE) channel, where the transmitter has multiple antennas while both the receiver and eavesdropper have only a single antenna. Our results are then extended to the multiple-input multiple-output multiple-eavesdropper (MIMOME) channel where both the receiver and eavesdropper have multiple antennas.

Specifically, due to the effect of AN leakage, we first show that the secrecy rate achievable under quantized CDI is upper-bounded by a constant when the number of feedback bits B is fixed. This is in contrast to the perfect CDI case [5] where the secrecy rate can increase

without bound by increasing the transmission power. To maintain a constant rate loss compared to the perfect CDI case, we show that the number of feedback bits B must scale logarithmically with the transmission power. These results are derived for both the MISOSE and MIMOME cases. Moreover, in the MISOSE case, we also derive the optimal power allocation between signal and AN under different number of feedback bits. We show that, when B is sufficiently large, the power should be allocated evenly among signal and AN while, when B is small, the power allocated to AN must be more conservative in order to control the amount of AN leakage in the legitimate receiver's channel. Furthermore, we show that additional channel quality information (CQI) at the transmitter provides little performance gain at high SNR, which supports the importance of our study on the CDI.

The organization is as follows. We provide the system model and backgrounds on Section II. Section III shows our results for MISOSE channel with quantized CDI, including inner and upper bounds of the secrecy rate and the optimal AN power allocation. The MISOSE feedback bit scaling law to maintain a constant rate loss is provided in Section IV. Section V extends the scaling law to MIMOME channel. Finally, Section VII concludes this document.

II. System Model and Background

A. Notations

In this document, $\mathcal{C}N(0,\sigma^2)$ denotes the distribution of a complex Gaussian random variable with mean 0 and variance σ^2 and $\beta(a,b)$ denotes a beta-distributed random variable with parameters (a,b). $\mathbf{E}[\cdot]$ stands for the statistical expectation of a random variable, $H(\cdot)$ stands for the entropy of a random variable (vector), and $I(;)$ represents the mutual information between two random variables (vectors). Almost-sure convergence is denoted by $\overset{a.s.}{\to}$. The function $[x]^+$ is equal to x when $x \geq 0$ and is equal to 0, otherwise. The norm of a vector $\mathbf{x}$ is denoted by $\|\mathbf{x}\|$.

B. Channel and signaling method

Consider a network that consists of a transmitter, a legitimate receiver and an eavesdropper. Suppose that there are n_t antennas at the transmitter, n_r antennas at the legitimate receiver and n_e antennas at the eavesdropper, such that $n_t > n_r$ and $n_t \geq n_e$. In this document, we first consider the scenario with $n_e = n_r = 1$, i.e., the MISOSE case, and then extend the results to the MIMOME case where $n_e \geq 1$ and $n_r \geq 1$ in Section V. At time index i, the transmitter sends a data vector $\mathbf{x}[i] \in \mathbb{C}^{n_t}$, such that $\mathbf{E}\left[\|\mathbf{x}[i]\|^2\right] \leq P$. The signals received at the receiver and the eavesdropper are respectively given by

$$y_r[i] = \mathbf{h}_r[i]^H \mathbf{x}[i] + z_r[i], \tag{1}$$

$$y_e[i] = \mathbf{h}_e[i]^H \mathbf{x}[i] + z_e[i], \tag{2}$$

respectively, where $\mathbf{h}_r[i], \mathbf{h}_e[i] \in \mathbb{C}^{n_t \times 1}$ denote the ergodic fading channel vectors at the receiver and eavesdropper, respectively, and $z_r[i]$, $z_e[i]$ are independent and identically distributed (i.i.d.) complex Gaussian noise. Here, $\mathbf{h}_r[i]$ is assumed to be a zero-mean complex Gaussian random vector with $E[|\mathbf{h}_r[i]|^2] = n_t$ and the direction $\mathbf{h}_e[i]/|\mathbf{h}_e[i]|$ of $\mathbf{h}_e[i]$ is assumed to be isotropically distributed. Note that as in [10], the norm $|\mathbf{h}_e[i]|$ can be arbitrary distributed. The distribution of $z_r[i]$ is assumed to be $\mathcal{C}N(0,1)$, and is known to the transmitter whereas the variance of $z_e[i]$ is in general unknown to the transmitter. Thus we consider the worst case scenario by assuming that the variance of $z_e[i]$ is zero [5]. We consider the block fading channel where $\mathbf{h}_r[i]$ and $\mathbf{h}_e[i]$ remain constant over the transmission of a codeword but vary independently from block to block. The two random fading processes are ergodic with bounded continuous distributions, and are also independent of each other. Due to finite-rate feedback, the transmitter is assumed to know only a quantized version of $\mathbf{h}_r[i]$ while perfect knowledge is assumed for both the legitimate receiver and the eavesdropper.

Suppose that the transmitter wants to send a secret message W with rate R using a length-n codeword $\mathbf{x}^n \triangleq \{\mathbf{x}[i]\}_{i=1}^n$. The perfect secrecy rate is defined as follows.

Definition 1 (Perfect secrecy rate and capacity [2], [4]) *A perfect secrecy rate R, is achievable if for any $\varepsilon > 0$, there exists a sequence of $(2^{nR}, n)$ codes such that for any $n > n(\varepsilon)$,*

$$P_e^n \leq \varepsilon, \text{ and } H(W|y_e^n, \mathbf{h}_r^n, \mathbf{h}_e^n)/n > R - \varepsilon,$$

where P_e^n is the average error probability, $\mathbf{h}_r^n \triangleq \{\mathbf{h}_r[i]\}_{i=1}^n$ and $\mathbf{h}_e^n \triangleq \{\mathbf{h}_e[i]\}_{i=1}^n$. And the perfect secrecy capacity is the supremum of all achievable secrecy rates,

Due to the lack of knowledge of channel states of $\mathbf{h}_e$*, even with full knowledge of $\mathbf{h}_r$ at the transmitter, the optimal signaling for this MISOSE channel is unknown except for very limited cases [2] [4]. Thus we consider the celebrated artificial-noise assisted beamforming signaling [5]. The transmitted signal $\mathbf{x}[i]$ is

$$\mathbf{x}[i] = \mathbf{p}s[i] + \mathbf{Q}\mathbf{a}[i], \tag{3}$$

where $s[i]$ is the message-bearing signal and $\mathbf{p} \in \mathbb{C}^{n_t \times 1}$ is normalized beamforming vector for sending $s[i]$; and $\mathbf{Q}\mathbf{a}[i]$ is the imposed AN, where the AN beamformer $\mathbf{Q} \in \mathbb{C}^{n_t \times n_t - 1}$ and $\mathbf{a}[i]$ is a $(n_t - 1) \times 1$ vector with $i.i.d.$ components and each component is distributed as $\mathcal{C}N(0, P_a)$. The noise $\mathbf{a}[i]$ is independent of $s[i]$. Beamformers $\mathbf{p}$ and $\mathbf{Q}$ are determined by available channel feedback. The optimality of adopted signaling is unknown in general. However, it is shown that with full CDI knowledge $\mathbf{h}_r/\|\mathbf{h}_r\|$ at the transmitter, this signaling method is optimal under some channel conditions [4], [6]. Consider the worst-case wiretapper channel where the eavesdropper does not suffer from additive noise. The signals received by the legitimate receiver and the eavesdropper are respectively given by

$$\begin{aligned} y_r[i] &= \mathbf{h}_r^H \mathbf{p}s[i] + \mathbf{h}_r^H \mathbf{Q}\mathbf{a}[i] + z_r[i] \\ y_e[i] &= \mathbf{h}_e^H \mathbf{p}s[i] + \mathbf{h}_e^H \mathbf{Q}\mathbf{a}[i]. \end{aligned} \tag{4}$$

*To simplify notations, we only show signals within a coherence interval and remove time indexes i in the channel vectors.

We choose $\mathbf{p}$ and each column vector of $\mathbf{Q}$ with unit norm, then the transmit power constraint becomes

$$\mathbf{E}[\|\mathbf{x}[i]\|^2] = P_s + (n_t - 1)P_a \leq P.$$

We set the variances of $s[i]$ and $a[i]$ to $P_s = \alpha P$, and $P_a = \frac{1-\alpha}{n_t - 1}P$. Thus α portion of power is allocated to the signal and $(1 - \alpha)$ to the AN.

First, we will identify the importance of AN in ensuring the non-zero secrecy rate by Proposition 1 below. According to [1], [2], the following perfect secrecy rate is achievable in this ergodic block-fading channel

$$(\mathbf{E}[I(s; y_r|\mathbf{h}_r) - I(s; y_e|\mathbf{h}_r, \mathbf{h}_e)])^+. \tag{5}$$

To achieve this rate, the message is coded across m coherence intervals and the number of channel usage within each coherence interval n_1 is assumed to be large enough to invoke random coding arguments. We then have $n = mn_1$. It can be treated as first computing the secrecy rate under certain channel states $(\mathbf{h_r}, \mathbf{h_e})$, and taking the expectation over all fading states. Here is a simple observation which ensures the importance of AN in our channel (4) due to unknown eavesdropper channel parameters. In this proof, the distribution of s is not limited to Gaussian.

Proposition 1 *If the artificial noise* $\mathbf{a}[i]$ *is absent in* (3)*, that is,* $\alpha = 1$*, then the perfect secrecy rate in (5) is zero.*

Proof: When $\alpha = 1$, $a[i]$ is absent in (4) and we have the Markov chain $s \leftrightarrow y_e \leftrightarrow y_r$ for any fading states $(\mathbf{h_r}, \mathbf{h_e})$. Then $I(s; y_r|\mathbf{h_r}) - I(s; y_e|\mathbf{h_r}, \mathbf{h_e}) \leq 0$, due to the data processing inequality [11]. Thus the secrecy rate (5) is zero. ■

C. Review of secrecy rate with perfect CDI

Here we briefly review the results with perfect CDI of $\mathbf{h}_r$ [5], where CDI is defined as

$$\mathbf{g}_r = \mathbf{h}_r / \|\mathbf{h}_r\|. \tag{6}$$

The transmitted signal is

$$\mathbf{x}_p[i] = \mathbf{g}_r s[i] + \mathbf{N}_g \mathbf{a}[i], \tag{7}$$

where $s[i] \sim \mathcal{C}N(0, \alpha P)$ and the beamformers are chosen as $\mathbf{p} = \mathbf{g}_r$ and $\mathbf{Q} = \mathbf{N}_g$ with $\mathbf{g}_r^H \mathbf{N}_g = 0$. The columns of $\mathbf{N}_g$ forms an orthonormal basis for the left null space of $\mathbf{g}_r$. The received signal at the legitimate user is

$$\tilde{y}_r[i] = \mathbf{h}_r^H \mathbf{g}_r s[i] + z_r[i]. \tag{8}$$

According to (5), the associated secrecy rate is given by

$$\left(\mathbf{E} \left[\log(1 + \|\mathbf{h}_r\|^2 \alpha P) - \log \left(1 + \frac{\|\mathbf{h}_e^H \mathbf{g}_r\|^2 \alpha}{\|\mathbf{h}_e^H \mathbf{N}_g\|^2 \frac{1-\alpha}{n_t - 1}} \right) \right] \right)^+ . \tag{9}$$

It is easy to see that the secrecy rate with perfect CDI can be arbitrarily large as P approaches infinity.

III. MISOSE Secrecy Rate with Quantized CDI

In this section, the inner-bound and outer-bound of the secrecy rate with quantized CDI for the MISOSE channel will be investigated.

A. Feedback model

Following the studies on quantized channel feedback given in [7] and [8] , we assume that the legitimate receiver knows perfectly its own $\mathbf{h}_r$, but sends back only the quantization of CDI in (6) to the transmitter. We assume that the CQI $\|\mathbf{h}_r\|$ is unknown at the transmitter. However, as we will show later, lack of such information in fact has little impact on secrecy rate if the SNR at the legitimate receiver is high. Suppose that the CDI $\mathbf{g}_r$ is quantized into one of 2^B unit-norm channel vectors in the codebook $\mathcal{C} \triangleq \{\mathbf{c}_1, ..., \mathbf{c}_{2^B}\}$, and the corresponding index is sent back to the transmitter. The quantization vector is chosen according to the minimum distance criterion [7]. The feedback index and its corresponding quantized CDI vector are respectively given by

$$\ell^\star = \arg \max_{\ell = 1, ..., 2^B} \|\mathbf{g}_r^H \mathbf{c}_\ell\|, \text{ and } \hat{\mathbf{g}}_\mathrm{r} \triangleq \mathbf{c}_{\ell^\star}. \tag{10}$$

To make analytical performance characterization possible, we resort to the quantization cell approximation model used in [7], [8], [12], where each quantization cell is a Voronoi region of a spherical cap with the surface area approximately equals to 2^{-B} of the total surface area of the n_t-dimensional unit sphere. In this model, the quantization cell $\mathcal{R}_k$ corresponding to (10) is approximated with

$$\mathcal{R}_k \approx \{\mathbf{g}_r : \|\mathbf{g}_r^H \mathbf{c}_k\|^2 \geq 1-\delta\}, \text{ where } \delta = 2^{-\frac{B}{n_t-1}}. \tag{11}$$

B. Inner and outer bound of the secrecy rate with quantized CDI

We study the impact of limited channel feedback on the secrecy rate in (5) using the signal model in (3) with Gaussian signaling and AN. Unlike the full CDI case in (9) [5], this secrecy rate will be bounded even with high SNR due to the additional leakage interference from AN. With quantized CDI $\hat{\mathbf{g}}_r$ at the transmitter, we choose the transmitted signal (3) as

$$\mathbf{x}[i] = \hat{\mathbf{g}}_r s[i] + \hat{\mathbf{N}}_g \mathbf{a}[i], \tag{12}$$

where $s[i]$ is the same as that in (7), the beamformers are choosing according to quantized CDI as $\mathbf{p} = \hat{\mathbf{g}}_r$ and $\mathbf{Q} = \hat{\mathbf{N}}_g$ with $\hat{\mathbf{g}}_r^H \hat{\mathbf{N}}_g = \mathbf{0}$. The columns of $\hat{\mathbf{N}}_g$ are orthonormal basis for the left null space of $\hat{\mathbf{g}}_r$. From (4), the signals at the legitimate receiver and eavesdropper are

$$\begin{aligned} \bar{y}_r[i] &= \|\mathbf{h}_r\|(\mathbf{g}_r^H \hat{\mathbf{g}}_r) \cdot s[i] + \|\mathbf{h}_r\|(\mathbf{g}_r^H \hat{\mathbf{N}}_g)\mathbf{a}[i] + z_r[i], \\ \bar{y}_e[i] &= \mathbf{h}_e^H \hat{\mathbf{g}}_r s[i] + \mathbf{h}_e^H \hat{\mathbf{N}}_g \mathbf{a}[i]. \end{aligned} \tag{13}$$

We observe from (13) that there is an additional leakage interference from AN in the legitimate receiver, thus degrading the achievable secrecy rate. For this case, the secrecy rate can be shown to be

$$\left(\mathbf{E}\left[\log\left(1 + \frac{\|\mathbf{h_r}\|^2 (\cos\theta)^2 \cdot \alpha P}{\|\mathbf{h}_r\|^2 \cdot (\sin\theta)^2 \frac{1-\alpha}{n_t-1} P + 1} \right) - \log\left(1 + \frac{\left\|\mathbf{h}_e^H \hat{\mathbf{g}}_r\right\|^2 \cdot \alpha}{\|\mathbf{h}_e^H \hat{\mathbf{N}}_g\|^2 \frac{1-\alpha}{n_t-1}}, \right) \right] \right)^+, \tag{14}$$

where we let $|\mathbf{g}_r^H \hat{\mathbf{g}}_r| = \cos\theta$, and $\|\mathbf{g}_r^H \hat{\mathbf{N}}_g\| = \sin\theta$ from the fact that $\|\mathbf{g}_r^H \hat{\mathbf{g}}_r\|^2 + \|\mathbf{g}_r^H \hat{\mathbf{N}}_g\|^2 = 1$.

Now we can show the constant outer-bound of the secrecy rate in (9) as follows. The detail proofs for theorems in this section are all given in the Appendix.

Theorem 1 *With perfect legitimate channel quality information $\|\mathbf{h}_r\|$ at the transmitter, for any AN assisted beamforming signal $\mathbf{x}[i] = \hat{\mathbf{g}}_r s[i] + \hat{\mathbf{N}}_g \mathbf{a}[i]$ under power constraint P, the secrecy rate in (5) is upper-bounded by*

$$\mathbf{E}\left[\left(\log \frac{\|\mathbf{g}_r^H \hat{\mathbf{g}}_r\|^2}{\|\mathbf{g}_r^H \hat{\mathbf{N}}_g\|^2} \frac{\|\mathbf{g}_e^H \hat{\mathbf{N}}_g\|^2}{\|\mathbf{g}_e^H \hat{\mathbf{g}}_r\|^2}\right)^+\right], \tag{15}$$

where $\mathbf{g}_e = \mathbf{h}_e/\|\mathbf{h}_e\|$. That is, even with **additional perfect CQI** at the transmitter, for any message-bearing signal distribution (not limited to Gaussian), the achievable secrecy rate is upper-bounded. This is due to the fact that the leakage interference also increases with P when P increases. The result is in strong contrast to that in (9) with perfect CDI [5].

C. Artificial noise power allocation

In Proposition 1, we have shown that the AN is necessarily to achieve a non-zero secrecy rate. However, in Theorem 1 we have also shown that the interference leakage from AN caused by quantized CDI feedback would limit the achievable secrecy rate. It is therefore important to investigate the optimal power allocation of AN for maximizing the secrecy rate. With the aids of large transmit antennas analysis (n_t approaches infinity), this power allocation is found analytically in this subsection. First we present a useful lemma as follows:

Lemma 1 *When number of transmitter antennas approaches infinity, $n_t \to \infty$, the second term in (14) will converge to a fixed value as follows*

$$\mathbf{E}\left[\log\left(1 + \frac{|\mathbf{h}_e^H \hat{\mathbf{g}}_r|^2}{|\mathbf{h}_e^H \hat{\mathbf{N}}_g|^2} \frac{\alpha}{(1-\alpha)/(n_t-1)}\right)\right] \to \log \frac{1}{1-\alpha}. \tag{16}$$

With Lemma 1, we can solve optimal α as stated in the following Theorem.

Theorem 2 *When $n_t \to \infty$, the optimal AN power allocation coefficient $\alpha^\star$ that maximizes the secrecy rate in (14) satisfies the following equation*

$$\mathbf{E}\left[\frac{h_s P(h_a P + 1)(1-\alpha^\star)}{(h_a(1-\alpha^\star)P + 1)((h_s\alpha^\star P + h_a(1-\alpha^\star)P + 1)}\right] = 1, \tag{17}$$

where $h_s \triangleq \|\mathbf{h}_r\|^2(\cos\theta)^2$ and $h_a \triangleq \|\mathbf{h}_r\|^2(\sin\theta)^2/(n_t-1)$.

Proof: With (16) in (14), the target rate function of α becomes

$$R(\alpha) = \mathbf{E}\left[\log\left((1-\alpha) + \frac{h_s P\alpha(1-\alpha)}{h_a P(1-\alpha)+1}\right)\right].$$

This function is concave when $\alpha \in [0,1]$ by the following two facts. First, the concavity in α of function $(1-\alpha) + \frac{h_s P\alpha(1-\alpha)}{h_a P(1-\alpha)+1}$, since its second derivatives $-\frac{2h_s P(h_a P+1)}{(h_a P(1-\alpha)+1)^3}$ is always negative when $\alpha \in [0,1]$. Second, $\mathbf{E}\log(.)$ conserves concavity. Then we know the optimal α must satisfy $\partial R(\alpha)/\partial\alpha = 0$ due to the concavity, which can be shown to be (17). ■

In general we can find the closed-form solution of α by explicitly computing the expectation in (17), but the result is expected to be very complicated. However, we can get insights by studying two special cases below. One is the case with weak noise leakage and the other is the case with strong noise leakage. The weak noise leakage situation is that the noise leakage $h_a(1-\alpha)P$ can be neglected compared to the additive noise at the legitimate receiver in (14). It happens when the number of feedback bits per transmitter antenna B/n_t scales with P. In this case, we have the following observation:

Observation 1 *Suppose that n_t is sufficiently large and B/n_t satisfying $B/n_t > \log P$. Then the optimal α will approach 1/2 as B increases.*

Reasons: If $h_a(1-\alpha)P \ll 1$ for all channel realizations, the optimal condition (17) reduces to

$$\mathbf{E}\left[\frac{h_s P(1-\alpha)}{h_s\alpha P+1}\right] = \mathbf{E}\left[\frac{\frac{\|\mathbf{h}_r\|^2}{n_t}(\cos\theta)^2(1-\alpha)P}{\frac{\|\mathbf{h}_r\|^2}{n_t}(\cos\theta)^2\alpha P + \frac{1}{n_t}}\right] = 1. \tag{18}$$

Since as $n_t \to \infty$, $\frac{1}{n_t} \overset{a.s.}{\to} 0$, and $\frac{\|\mathbf{h}_r\|^2}{n_t}(\cos\theta)^2 \overset{a.s.}{\to} (\cos\theta)^2$ due to law of large numbers, (18) equals to

$$\mathbf{E}\left[\frac{1-\alpha}{\alpha}\right] = \frac{1-\alpha}{\alpha} = 1. \tag{19}$$

Then $\alpha = 1/2$ is optimal. We now show that the sufficient condition of weak noise leakage is $B/n_t \gg \log P$. To make the noise leakage weak with $h_a(1-\alpha)P \ll 1$, from the definition of h_a we ensure

$$\frac{\|\mathbf{h}_r\|^2}{n_t} \cdot (\sin\theta)^2 P \ll \frac{n_t - 1}{n_t}, \tag{20}$$

for all random realizations. Note that we have replaced $(1-\alpha)P$ with P in above equation since $0 \leq \alpha \leq 1$, $(1-\alpha)P \leq P$. From law of large numbers, $\lim_{n_t \to \infty} \frac{\|\mathbf{h}_r\|^2}{n_t} = \frac{\mathbf{E}[\|\mathbf{h}_r\|]^2}{n_t} = 1$. According to the quantization model in (11), it has been shown that $(\sin\theta)^2 \leq 2^{\frac{-B}{n_t-1}}$ [7], [8]. Thus $h_a(1-\alpha)P \ll 1$ suffices to

$$2^{\frac{-B}{n_t-1}} P \ll \frac{n_t-1}{n_t}.$$

Since $\frac{n_t-1}{n_t} \to 1$ when $n_t \to \infty$, the above condition is in general met when $B/n_t > \log P$, and the noise leakage is weak.

On the other hand, in the case with strong leakage, the contribution of the artificial noise leakage $h_a(1-\alpha)P$ dominates that of the additive noise in (14). It occurs when B/n_t is not sufficient or B/n_t is fixed but P is high. Now we have the property of optimal α as

Observation 2 *With sufficient large n_t and P, for fixed B/n_t with $B/n_t \geq 1$, the optimal α is close to* 1.

Reasons: Note that if we reduce the value of the left-hand-side of (17) by removing all "1"s in the denominator, the left-hand-side of (17) can be recast as

$$\mathbf{E}\left[\frac{h_s P(h_a P+1)(1-\alpha)}{h_a(1-\alpha)P(h_s\alpha P + h_a(1-\alpha)P)}\right] - \epsilon(\alpha) = \mathbf{E}\left[\frac{h_s/h_a(1+\frac{1}{h_a P})}{\alpha * h_s/h_a + (1-\alpha)}\right] - \epsilon(\alpha), \quad (21)$$

where $\epsilon(\alpha) > 0$. Note that by definition, $h_s/h_a = (\cot\theta)^2(n_t-1)$. From [7], $\cot^2\theta \geq 2^{\frac{B}{n_t-1}} - 1$, which is larger than 1 if $B/n_t \geq 1$, then h_s/h_a is large when n_t is large. The term $(1-\alpha)$ in the denominator of the right-hand-side of (21) can be neglected. When P is large, the impact of $1/h_a P$ in the numerator can also be neglected, then the optimal condition (17) from (21) becomes

$$\frac{1}{\alpha} - 1 = \epsilon(\alpha). \quad (22)$$

Observing (21), when P is large, the noise leakage is strong for fixed B/n_t and $\epsilon(\alpha)$ is very small. However, the left-hand-side of (22) equals to small value only when α is close to 1. Thus we know that the optimal $\alpha^\star$ which satisfies (22) is close to 1.

From the above observations, when the channel state information is sufficiently accurate or when the number of feedback bits are sufficient, one should allocate half of the power for the signal and the other half for the AN to jam the reception of the eavesdropper. Note that for the extreme case when $B/n_t \to \infty$ (full CDI), the optimal α is exactly 1/2. However, when the channel quantization is coarse, one should allocate less power for transmitting the AN since severe noise leakage would occur, causing significant loss in the secrecy rate.

D. Gap between inner and outer bound of secrecy rate

With perfect AN power allocation $\alpha^\star$, now we can study the gap between secrecy rate inner bound (14) with $\alpha^\star$ and outer bound (15). We will show that the gap is small in some situations. It means that our inner bound, derived with optimized Gaussian s and no CQI information, is very close to the highest secrecy rate over all other possible s distributions can achieve with additional CQI.

To this end, let us assume that the transmitter has full CQI. In that case, the transmitter is able to allocate the AN power depending on the CQI and adopt the variable rate coding in [2]. Specifically the achievable secrecy rate is given by

$$\mathbf{E}\left[\left(\log\left(1+\frac{\|\mathbf{h}_r\|^2(\cos\theta)^2\cdot\alpha(\|\mathbf{h}_r\|)P}{\|\mathbf{h}_r\|^2\cdot\frac{\sin\theta^2}{n_t-1}(1-\alpha(\|\mathbf{h}_r\|))P+1}\right)-\log\left(1+\frac{\|\mathbf{h}_e^H\hat{\mathbf{g}}_r\|^2\cdot\alpha(\|\mathbf{h}_r\|)}{\frac{\|\mathbf{h}_e^H\hat{\mathbf{N}}_g\|^2}{n_t-1}(1-\alpha(\|\mathbf{h}_r\|)}\right)\right)^+\right],$$

of which (14) is strictly lower. In this coding, CQI $\|\mathbf{h}_r\|$ are used to adapt secrecy rate with the AN power coefficient $\alpha(\|\mathbf{h}_r\|)$ in every fading states. However, from the following corollary we show that CQI is not so important to approach (15) at high SNR with large n_t.

Corollary 1 *With large enough n_t and P with $B \geq n_t$, the difference between the inner bound (14) and the outer bound (15) is less than $|\log\alpha^\star|$, where $\alpha^\star$ is the optimal power allocation that maximizes the secrecy rate in (14).*

For any fixed B/n_t, when P is large, the noise leakage is strong. From Observation 2, $\alpha^\star$ will be close to 1 with large P, thus the gap is small.

IV. MISOSE NUMBER OF FEEDBACK BITS SCALING LAW

To control the AN leakage, we investigate the required number of feedback bits for the constant secrecy rate loss compared to the perfect CDI case by analyzing the secrecy rate loss due to imperfect CDI. We first show the secrecy rate loss due to imperfect CDI

$$\Delta \mathrm{C}_{\mathrm{sec}} \triangleq \left[\mathbf{E}[I(s;\tilde{y}_r|\mathbf{h}_r)] - \mathbf{E}[I(s;\tilde{y}_e|\mathbf{h}_r,\mathbf{h}_e)]\right]^+ - \left[\mathbf{E}[I(s;\bar{y}_r|\mathbf{h}_r)] - \mathbf{E}[I(s;\bar{y}_e|\mathbf{h}_r,\mathbf{h}_e)]\right]^+ \quad (23)$$

is upper-bounded by a function which only depends on the information at the legitimate receiver. To upper-bound the rate loss, we set both power allocation coefficients α with perfect and quantized CDI as $\alpha_P^\star$, the optimal one with perfect CDI. Second, we show that B has to be increased at least logarithmically with P to maintain a constant secret rate degradation.

To this end, first we show that

$$\Delta \mathrm{C}_{\mathrm{sec}} \leq \mathbf{E}[I(s;\tilde{y}_r|\mathbf{h}_r)] - \mathbf{E}[I(s;\bar{y}_r|\mathbf{h}_r)], \quad (24)$$

which indeed only depends on $\mathbf{h}_r$. First we show

$$\mathbf{E}[I(s;\tilde{y}_e|\mathbf{h}_r,\mathbf{h}_e)] = \mathbf{E}[I(s;\bar{y}_e|\mathbf{h}_r,\mathbf{h}_e)]. \quad (25)$$

It is noted from [7] that, for any two independent and isotropically distributed unit-norm vectors $\mathbf{w}_1, \mathbf{w}_2 \in \mathbb{C}^{n_t}$, the inner product $|\mathbf{w}_1^H \mathbf{w}_2|^2$ is Beta-distributed as $\beta(1, n_t - 1)$. For the numerator of $\mathbf{E}[I(s;\bar{y}_e|\mathbf{h}_r,\mathbf{h}_e)]$ which equals to the second term in (14), since $\hat{\mathbf{g}}_r$ and $\mathbf{h}_e$ are independent and isotropically distributed in $\mathbb{C}^{n_t}$, $|\mathbf{h}_e^H \hat{\mathbf{g}}_r|^2 = \|\mathbf{h}_e\|^2 \beta(1, n_t - 1)$. As for the denominator, $\|\mathbf{h}_e^H \hat{\mathbf{N}}_g\|^2$ equals to $\|\mathbf{h}_e\|^2 - \|\mathbf{h}_e^H \hat{\mathbf{g}}_r\|^2$, then

$$\mathbf{E}[I(s;\bar{y}_e|\mathbf{h}_r,\mathbf{h}_e)] = \mathbf{E}\left[1 + \frac{\beta(1, n_t - 1)\alpha_P^\star (n_t - 1)}{(1 - \beta(1, n_t - 1))(1 - \alpha_P^\star)}\right].$$

The above arguments hold also for $\mathbf{E}[I(s;\tilde{y}_e|\mathbf{h}_r,\mathbf{h}_e)]$. Therefore, (25) is valid. Using (25) and the fact that $\mathbf{E}[I(s;\tilde{y}_r|\mathbf{h}_r)] \geq \mathbf{E}[I(s;\bar{y}_r|\mathbf{h}_r)]$ in (23) we have (24). It is worthwhile to remark that this bound is tight when (14) is non-negative, which typically happens when P or B is large.

With (24), we can upper bound (23) as

$$\Delta \mathrm{C}_{\mathrm{sec}} \leq \mathbf{E}[\log(1+\|\mathbf{h}_r\|^2 \cdot \alpha_P^\star P)] - \mathbf{E}\left[\log\left(1+\frac{\|\mathbf{h}_r\|^2(\cos\theta)^2 \cdot \alpha_P^\star P}{\|\mathbf{h}_r\|^2(\sin\theta)^2\left((1-\alpha_P^\star)/(n_t-1)P\right)+1}\right)\right]. \tag{26}$$

By further upper-bounding (26), we have the following theorem and corollary. From (28), the number of feedback bits B must increase with the order of $O(\log_2 P)$ in order to maintain a constant Δ_r.

Theorem 3 *The secrecy rate loss between quanitzed and perfect CDI is upper-bounded by*

$$\Delta \mathrm{C}_{\mathrm{sec}} < \log\left[\left(\frac{n_t(1-\alpha_P^\star)P}{(n_t-1)(2^{\frac{B}{n_t-1}}-1)}+\frac{1}{1-2^{\frac{-B}{n_t-1}}}\right)\left(1+\frac{1}{(n_t-1)\alpha_P^\star P}\right)\right]. \tag{27}$$

Corollary 2 *To maintain a constant secrecy rate loss Δ_r, let $\Delta_r' = (2^{\Delta_r})/(1+1/((n_t-1)\alpha_P^\star P))$, then the number of feedback bits B must satisfy*

$$B \geq (n_t-1)\log\left[\frac{n_t}{n_t-1}\frac{(1-\alpha_P^\star)P}{\Delta_r'}+\frac{\Delta_r'}{\Delta_r'-1}\right]. \tag{28}$$

Proof: We further upper-bound (26) as follows

$$\Delta \mathrm{C}_{\mathrm{sec}} < \mathbf{E}[\log(1+\|\mathbf{h}_r\|^2 \cdot \alpha_P^\star P)] - \mathbf{E}\left[\log\left(\frac{(\|\mathbf{h}_r\|^2\alpha_P^\star P)(\cos\theta)^2}{\|\mathbf{h}_r\|^2(\sin\theta)^2\left((1-\alpha_P^\star)/(n_t-1)\right)P+1}\right)\right], \tag{29}$$

$$= \mathbf{E}\left[\log\left(\frac{\|\mathbf{h}_r\|^2 \cdot (\sin\theta)^2(1-\alpha_P^\star)/(n_t-1)P+1}{(\cos\theta)^2}\right)\right] + \mathbf{E}\left[\log(\frac{1+\|\mathbf{h}_r\|^2\alpha_P^\star P}{\|\mathbf{h}_r\|^2\alpha_P^\star P})\right].$$

We upper-bound the first term by Jensen inequality [11] as

$$\log \mathbf{E}\left[\left(\frac{\|\mathbf{h}_r\|^2 \cdot (\sin\theta)^2(1-\alpha_P^\star)/(n_t-1)P+1}{(\cos\theta)^2}\right]\right). \tag{30}$$

We define $P' \triangleq \|\mathbf{h}_r\|^2(1-\alpha_P^\star)/(n_t-1)P$, and using $\sin^2\theta = 1-\cos^2\theta$ to simplify (30) as

$$\log \mathbf{E}\left[\frac{P'+1}{1-(\sin\theta)^2}-P'\right] = \log(\mathbf{E}[P'+1]\mathbf{E}\left[\frac{1}{1-(\sin\theta)^2}\right]-\mathbf{E}[P']), \tag{31}$$

where the last equality comes from the fact that $\|\mathbf{h}_r\|^2$ and $\sin^2\theta$ are statistically independent [8]. We will upper-bound (31) by upper-bounding $\mathbf{E}[1/(1-\sin^2\theta)]$. From [7] the probability

density function of $\sin^2\theta$ is $2^B(n_t-1)x^{n_t-2}$ when $0 \le x \le \delta$, and is zero elsewhere, where $\delta = 2^{\frac{-B}{n_t-1}}$. Thus

$$\mathbf{E}\left[\frac{1}{1-(\sin\theta)^2}\right] = 2^B(n_t-1)\int_0^\delta \frac{1}{1-x}x^{n_t-2}dx = 2^B(n_t-1)\delta^{n_t-1}\int_0^1 \frac{1}{1-\delta x}x^{n_t-2}dx,$$

where change of variables is applied in the integral. Since $0<\delta<1$, $1/(1-\delta x) < 1/(1-\delta)\ \ \forall x \in [0,1]$,

$$\mathbf{E}\left[\frac{1}{1-(\sin\theta)^2}\right] \le 2^B(n_t-1)\delta^{n_t-1}\int_0^1 \frac{1}{1-\delta}x^{n_t-2}dx = \frac{1}{1-2^{\frac{-B}{n_t-1}}}. \tag{32}$$

Finally, substituting (31) with (32) and the fact that $\mathbf{E}[|\mathbf{h}_r|]^2 = n_t$ by assumption, we can upper-bound the first term of (29) by

$$\log\left(\frac{n_t(1-\alpha_P^\star)P}{(n_t-1)(2^{\frac{B}{n_t-1}}-1)} + \frac{1}{1-2^{\frac{-B}{n_t-1}}}\right). \tag{33}$$

For the second term of (29), by Jensen inequality

$$\mathbf{E}\left[\log(\frac{1+\|\mathbf{h}_r\|^2\alpha_P^\star P}{\|\mathbf{h}_r\|^2\alpha_P^\star P})\right] \le \log\mathbf{E}\left[\frac{1+\|\mathbf{h}_r\|^2\alpha_P^\star P}{\|\mathbf{h}_r\|^2\alpha_P^\star P}\right] = \log\left(1+\frac{\mathbf{E}\left(1/|\mathbf{h}_r\|^2\right)}{\alpha_P^\star P}\right).$$

Finally, with (33) in (30) and the fact that $\mathbf{E}\left(\frac{1}{\|\mathbf{h}_r\|^2}\right) = \frac{1}{n_t-1}$ [13], we have (27) . ■

V. Impact of Quantized CDI on the MIMOME Wiretap Channel

In the section, we will investigate the impact of the quantization CDI feedback on the MIMOME secrecy rate, and analyze the number of required feedback bits B for a constant secrecy rate loss.

A. MIMOME signal model and secrecy rate

Consider the MIMOME signal model where $n_r, n_e \ge 1$. The received signal models within certain coherence interval are given by

$$\mathbf{y}_r[i] = \mathbf{H}_r\mathbf{x}[i] + \mathbf{z}_r[i], \tag{34a}$$

$$\mathbf{y}_e[i] = \mathbf{H}_e\mathbf{x}[i], \tag{34b}$$

where $\mathbf{H}_r \in \mathbb{C}^{n_r \times n_t}$ and $\mathbf{H}_e \in \mathbb{C}^{n_e \times n_t}$ denote the MIMO channel matrices between the transmitter and the legitimate receiver and the eavesdropper, respectively. Similar to the MISOSE case in Section II, we assume that the channels are ergodic and the elements of $\mathbf{H}_r$ and $\mathbf{H}_e$ are i.i.d. complex Gaussian distributed with zero mean and unit variance.

Assume that $n_t \geq n_r + n_e$. It follows from [5] that the transmitted signal vector $\mathbf{x}$ is given by

$$\mathbf{x}[i] = \mathbf{P}\mathbf{s}[i] + \mathbf{Q}\mathbf{a}[i], \tag{35}$$

where $\mathbf{s}[i]$ is the message-bearing signal with distribution $\mathcal{C}N(0, P_s\mathbf{I}_{n_r})$, $\mathbf{a}[i]$ is the imposed artificial noise with distribution $\mathcal{C}N(0, P_a\mathbf{I}_{n_t-n_r})$, and $\mathbf{P} \in \mathbb{C}^{n_t \times n_r}$ and $\mathbf{Q} \in \mathbb{C}^{n_t \times (n_t-n_r)}$ are the precoding matrices for $\mathbf{s}[i]$ and $\mathbf{a}[i]$, respectively. Let the SVD of $\mathbf{H}_r$ be $\mathbf{H}_r = \mathbf{V}\mathbf{\Sigma}\mathbf{U}^H$, where $\mathbf{V} \in \mathbb{C}^{n_r \times n_r}$ is a unitary matrix, $\Sigma \in \mathbb{C}^{n_r \times n_r}$ is a diagonal matrix with the singular values of $\mathbf{H}_r$ being the diagonal elements, and $\mathbf{U} \in \mathbb{C}^{n_t \times n_r}$ is a semi-unitary matrix. Denote by $\mathbf{Z} \in \mathbb{C}^{n_t \times (n_t-n_r)}$ whose column vectors form an orthonormal basis for the orthogonal complement of $\mathbf{U}$. Then the transmitter employs the "matched" precoder by choosing $\mathbf{P} = \mathbf{U}$ and $\mathbf{Q} = \mathbf{Z}$ (therefore $\mathbf{U}^H\mathbf{Q} = \mathbf{0}$). Under this setting, the received signal models in (34) become

$$\begin{aligned}
\mathbf{y}_r[i] &= \mathbf{H}_r\left(\mathbf{U}\mathbf{s}[i] + \mathbf{Z}\mathbf{a}[i]\right) + \mathbf{z}_r[i] = \left(\mathbf{V}\mathbf{\Sigma}\right)\mathbf{s}[i] + \mathbf{z}_r[i] \\
\mathbf{y}_e[i] &= \mathbf{H}_e\mathbf{U}\mathbf{s}[i] + \mathbf{H}_e[i]\mathbf{Z}\mathbf{a}[i],
\end{aligned} \tag{36}$$

and the associated achievable MIMOME perfect secrecy rate [5] can be shown as $(E[R_{s,p,M}])^+$, where $R_{s,p,M}$ is given by

$$\log\left|\mathbf{I}_{n_r} + \mathbf{\Sigma}^2 P_s\right| - \log\left|P_s\mathbf{U}^H\mathbf{H}_e^H\left(P_a\mathbf{H}_e\mathbf{Z}\mathbf{Z}^H\mathbf{H}_e^H\right)^{-1}\mathbf{H}_e\mathbf{U}\right|, \tag{37}$$

where $P_s = \left(\frac{\alpha}{n_r}\right)P$ and $P_a = \frac{(1-\alpha)}{n_t-n_r}P$. As seen from (37), the MIMOME secrecy rate can be made arbitrarily large by increasing P.

Suppose that the transmitter has a quantized CDI feedback $\hat{\mathbf{U}} \in \mathbb{C}^{n_t \times n_r}$. Then we have $\mathbf{P} = \hat{\mathbf{U}}$ in (35). Moreover, the associated AN precoder $\mathbf{Q}$ would be chosen as the basis matrix for the orthogonal complement of $\hat{\mathbf{U}}$, which is denoted by $\hat{\mathbf{Z}}$. Since $\mathbf{U}^H\hat{\mathbf{Z}} \neq \mathbf{0}$, we instead have an

undesired AN leakage term $\mathbf{V}\mathbf{\Sigma}\mathbf{V}^H\hat{\mathbf{Z}}\mathbf{v}[i]$ in $\mathbf{y}_r[i]$ from (36), and therefore the achievable perfect secrecy rate under quantized CDI feedback is $(E[R_{s,q,M}])^+$, where $R_{s,q,M}$ is given by

$$\log\left|\mathbf{I}_{n_r}+P_s\hat{\mathbf{U}}^H\mathbf{U}\mathbf{\Sigma}\left(\mathbf{I}+P_a\mathbf{\Sigma}\mathbf{U}^H\hat{\mathbf{Z}}\hat{\mathbf{Z}}^H\mathbf{U}\mathbf{\Sigma}\right)^{-1}\mathbf{\Sigma}\mathbf{U}^H\hat{\mathbf{U}}\right| - \log\left|P_s\hat{\mathbf{U}}^H\mathbf{H}_e^H\left(P_a\mathbf{H}_e\hat{\mathbf{Z}}\hat{\mathbf{Z}}^H\mathbf{H}_e^H\right)^{-1}\mathbf{H}_e\hat{\mathbf{U}}\right|. \quad (38)$$

The quantization codebook model will be presented in next subsection.

B. Random quantization codebook model

The MIMOME quantization codebook is a set of $n_t\times n_r$ semi-unitary matrices $\{\mathrm{C}_1,\ldots,\mathbf{C}_{2^B}\}$. With the perfect knowledge of $\mathbf{H}_r$ at the legitimate receiver, the quantized CDI $\hat{\mathbf{U}}$ is obtained by

$$\hat{\mathbf{U}}=\arg\min_{\mathbf{C}\in\{\mathbf{C}_1,\ldots,\mathbf{C}_{2^B}\}} d^2(\mathbf{U},\mathbf{C}), \quad (39)$$

where $d(\mathbf{U},\mathbf{C})=n_r-\mathrm{Tr}(\mathbf{U}^H\mathbf{C}\mathbf{C}^H\mathbf{U})$ is the chordal distance between $\mathbf{U}$ and $\mathbf{C}$ [14]. For ease of analysis, we consider the random quantization codebook model [14] where the 2^B semi-unitary codewords are chosen independently and isotropically over the $n_t\times n_r$ Grassmann manifold (which is the set of all n_r dimensional subspaces in an n_t dimensional space). With this codebook model, the average distortion between $\hat{\mathbf{U}}$ and $\mathbf{U}$ can be upper bounded as [14]

$$D\triangleq\mathbf{E}[d^2(\mathbf{U},\hat{\mathbf{U}})]\le\frac{\Gamma(\frac{1}{T})}{T}\Phi^{\frac{-1}{T}}2^{\frac{-B}{T}}, \quad (40)$$

where $\Gamma(\cdot)$ is the Gamma function and

$$T=n_r(n_t-n_r),\Phi=\begin{cases}\frac{1}{\Gamma(T+1)}\prod_{i=1}^{n_r}\frac{n_t-i+1}{n_r-i+1}, & n_r\le\frac{n_t}{2},\\ \frac{1}{\Gamma(T+1)}\prod_{i=1}^{n_t-n_r}\frac{n_t-i+1}{n_t-n_r-i+1}, & n_r\ge\frac{n_t}{2}.\end{cases}$$

Moreover, the quantized CDI $\hat{\mathbf{U}}$ and the true CDI $\mathbf{U}$ have the following relation [9]

$$\mathbf{U}=\hat{\mathbf{U}}\mathbf{X}\mathbf{Y}+\hat{\mathbf{S}}\mathbf{R}, \quad (41)$$

where $\mathbf{X}\in\mathbb{C}^{n_r\times n_r}$ is a unitary matrix, $\mathbf{Y}\in\mathbb{C}^{n_r\times n_r}$ is a upper triangular matrix satisfying $\mathrm{Tr}(\mathbf{Y}^H\mathbf{Y})=n_r-d^2(\mathbf{U},\hat{\mathbf{U}})$, $\hat{\mathbf{S}}\in\mathbb{C}^{n_t\times r}$ where $r=\min\{n_t-n_r,n_r\}$ is an orthonormal basis

for an isotropically distributed r-dimensional plane in the range space of $\hat{\mathbf{Z}}$, and $\mathbf{R} \in \mathbb{C}^{r\times n_r}$ satisfies $\mathrm{Tr}(\mathbf{R}^H\mathbf{R}) = d^2(\hat{\mathbf{U}}, \mathbf{U})$. In addition, one can show that [9]

$$\mathbf{U}^H\hat{\mathbf{Z}}\hat{\mathbf{Z}}^H\mathbf{U} = \mathbf{R}^H\mathbf{R},\ \mathbf{E}\left(\mathbf{R}^H\mathbf{R}\right) = \frac{D}{n_r}\mathbf{I}_{n_r}, \tag{42}$$

$$\mathbf{U}^H\hat{\mathbf{U}}\hat{\mathbf{U}}^H\mathbf{U} = \mathbf{Y}^H\mathbf{Y},\ \mathbf{E}\left(\mathbf{Y}^H\mathbf{Y}\right) = \left(1 - \frac{D}{n_r}\right)\mathbf{I}_{n_r}. \tag{43}$$

C. Analysis of the secrecy rate loss

Now we are ready to analyze the MIMOME secrecy rate loss due to quantized CDI. Since the elements of $\mathbf{H}_r$ are complex i.i.d. Gaussian, $\mathbf{U}$ is isotropically distributed in the n_t by n_r Grassmann manifold and thus $\mathbf{Z}$ is isotropically-distributed in the n_t by $n_t - n_r$ Grassmann manifold. Under random quantization codebook, codeword $\hat{\mathbf{U}}$ is of the same distribution as $\mathbf{U}$. Moreover, $\mathbf{Z}\mathbf{Z}^H = \mathbf{I} - \mathbf{U}\mathbf{U}^H$ and $\hat{\mathbf{Z}}\hat{\mathbf{Z}}^H = \mathbf{I} - \hat{\mathbf{U}}\hat{\mathbf{U}}^H$. Hence, using similar arguments as for the MISOSE case in Section IV, the second terms in (37) and (38) have the same distribution, and the MIMOME secrecy rate loss $\Delta\mathrm{C}_{\text{sec}} \triangleq \mathrm{C}_{\text{sec}} - \hat{\mathrm{C}}_{\text{sec}}$ can be upper-bounded by

$$\begin{aligned}\Delta\mathrm{C}_{\text{sec}} &\le \mathbf{E}\left(\log\left|\mathbf{I}_{n_r} + \mathbf{\Sigma}^2 P_s\right|\right) - \mathbf{E}\left(\log\left|\mathbf{I}_{n_r} + P_s\hat{\mathbf{U}}^H\mathbf{U}\mathbf{\Sigma}\left(\mathbf{I} + P_a\mathbf{\Sigma}\mathbf{U}^H\hat{\mathbf{Z}}\hat{\mathbf{Z}}^H\mathbf{U}\mathbf{\Sigma}\right)^{-1}\mathbf{\Sigma}\mathbf{U}^H\hat{\mathbf{U}}\right|\right)\\ &\le \mathbf{E}\left(\log\left|\mathbf{I}_{n_r} + \mathbf{\Sigma}^2 P_s\right|\right) - \mathbf{E}\left(\log\left|P_s\hat{\mathbf{U}}^H\mathbf{U}\mathbf{\Sigma}\left(\mathbf{I} + P_a\mathbf{\Sigma}\mathbf{U}^H\hat{\mathbf{Z}}\hat{\mathbf{Z}}^H\mathbf{U}\mathbf{\Sigma}\right)^{-1}\mathbf{\Sigma}\mathbf{U}^H\hat{\mathbf{U}}\right|\right),\end{aligned} \tag{44}$$

where $P_s = \left(\frac{\alpha_P^\star}{n_r}\right)P$ and $P_a = \frac{(1-\alpha_P^\star)}{n_t - n_r}P$ and $\alpha_P^\star$ is the optimum power allocation for (37).

By (41), we have $\hat{\mathbf{U}}^H\mathbf{U} = \hat{\mathbf{U}}^H\hat{\mathbf{U}}\mathbf{X}\mathbf{Y} = \mathbf{X}\mathbf{Y}$ due to $\hat{\mathbf{U}}^H\hat{\mathbf{U}} = \mathbf{I}_{n_r}$. Since $\mathbf{X}$ and $\mathbf{Y}$ are independent to each other [9], it is with probability one that $\hat{\mathbf{U}}^H\mathbf{U}$ is of full rank [13]. Hence one can further upper-bound the secrecy rate loss in (44) as follows

$$\begin{aligned}\Delta\mathrm{C}_{\text{sec}} &\le \mathbf{E}\left(\log\left|\mathbf{I}_{n_r} + \mathbf{\Sigma}^{-2}P_s^{-1}\right|\right) + \mathbf{E}\left(\log\left|\mathbf{I}_{n_r} + P_a\mathbf{\Sigma}\mathbf{U}^H\hat{\mathbf{Z}}\hat{\mathbf{Z}}^H\mathbf{U}\mathbf{\Sigma}\right|\right) - \mathbf{E}\left(\log\left|\mathbf{U}^H\hat{\mathbf{U}}\hat{\mathbf{U}}^H\mathbf{U}\right|\right)\\ &\le \log\left|\mathbf{I}_{n_r} + \mathbf{E}\left(\mathbf{\Sigma}^{-2}\right)P_s^{-1}\right| + \log\left|\mathbf{I}_{n_r} + P_a\mathbf{E}\left(\mathbf{\Sigma}^2\right)\cdot\mathbf{E}\left(\mathbf{R}^H\mathbf{R}\right)\right| - \mathbf{E}\left(\log\left|\mathbf{Y}^H\mathbf{Y}\right|\right),\end{aligned} \tag{45}$$

where the second inequality is due to the Jensen's inequality and the statistical independence between $\mathbf{\Sigma}$, $\mathbf{U}$ and $\hat{\mathbf{Z}}$ [9], and the results in (42) and (43). Since $\mathbf{H}_r\mathbf{H}_r^H$ is a $n_r \times n_r$ central

Wishart matrix with n_t degrees of freedom, $\mathbf{E}\left(\mathbf{\Sigma}^2\right)$ can then be shown as [9]

$$\mathbf{E}\left(\mathbf{\Sigma}^2\right) = n_t \mathbf{I}_{n_r}. \tag{46}$$

Besides, since $\mathbf{E}\left(\mathrm{Tr}[(\mathbf{H}_r\mathbf{H}_r^H)^{-1}]\right) = \mathbf{E}\left(\mathrm{Tr}[\mathbf{\Sigma}^{-2}]\right) = n_r/(n_t - n_r)$ [13], we have that

$$\log\left|\mathbf{I}_{n_r} + \mathbf{E}\left(\mathbf{\Sigma}^{-2}\right) P_s^{-1}\right| \leq n_r \log\left(\frac{\mathrm{Tr}\left(\mathbf{I}_{n_r} + \mathbf{E}\left(\mathbf{\Sigma}^{-2}\right) P_s^{-1}\right)}{n_r}\right) = n_r \log\left(1 + \frac{P_s^{-1}}{n_t - n_r}\right), \tag{47}$$

where the inequality is due to $|\mathbf{A}|^{\frac{1}{nr}} \leq \frac{\mathrm{Tr}(\mathbf{A})}{n_r}$ for any $n_r \times n_r$ Hermitian positive semidefinite $\mathbf{A}$.

The third term $-\mathbf{E}\left(\log\left|\mathbf{Y}^H\mathbf{Y}\right|\right)$ in (45) is, however, difficult to be evaluated or to be further upper-bounded. Considering that both $\log\left|\mathbf{Y}^H\mathbf{Y}\right|$ and $\log\left|\mathbf{E}\left(\mathbf{Y}^H\mathbf{Y}\right)\right|$ (see (43)) approach to zero when B is sufficiently large, we instead approximate $-\mathbf{E}\left(\log\left|\mathbf{Y}^H\mathbf{Y}\right|\right)$ as

$$-\mathbf{E}\left(\log\left|\mathbf{Y}^H\mathbf{Y}\right|\right) \approx -\log\left|\mathbf{E}\left(\mathbf{Y}^H\mathbf{Y}\right)\right| = -n_r \log\left(1 - \frac{D}{n_r}\right) \tag{48}$$

by (43). By substituting (42), (46), (47) and (48) into (45), one thus obtains

$$\Delta \mathrm{C}_{\mathrm{sec}} \lesssim n_r \log\left(\frac{n_r + P_a n_t D}{n_r - D}\right) + \gamma(P_s^{-1}) \tag{49}$$

where $\gamma(P_s^{-1}) = n_r \log\left(1 + \frac{P_s^{-1}}{n_t - n_r}\right)$. To ensure the secrecy rate loss $\Delta \mathrm{C}_{\mathrm{sec}}$ to be less than a preassigned Δ_r, by (49) and (40) the number of feedback bits B to maintain a rate loss Δ_r can be shown to be scaled as

$$B \gtrsim (n_t - n_r) n_r \left[\log\left(1 + \frac{P n_t \left(\frac{1-\alpha_P^\star}{n_t - n_r}\right) + 1}{2^{(\Delta_r - \gamma(P_s^{-1}))/n_r} - 1}\right) + \log\left(\frac{\Gamma(\frac{1}{n_r(n_t-n_r)})\Phi^{-1/(n_r(n_t-n_r))}}{n_r^2(n_t - n_r)}\right)\right]. \tag{50}$$

We therefore see that B must also be scaled with the order of $O(\log P)$ in order to have the MIMOME secrecy rate loss smaller than Δ_r.

VI. Simulation Results and Discussions

In this section, we present simulation results to illustrate the impact of quantized CDI feedback on the secrecy rate. We set the number of transmit antennas n_t to 4. To verify our results and save simulation time as [9], we use the method in [9] to generate the quantized codeword for a certain channel realization of the legitimate receiver with adopted random quantization codebooks. Each simulation result is obtained by averaging over 10000 channel realizations.

Fig. 1 presents the simulation results of the MISOSE secrecy rate versus the AN power allocation ratio α for SNR$= 25$ dB. The secrecy rate is zero when $\alpha = 1$ as stated in Proposition 1. As observed in subsection III-C, the optimal $\alpha^\star$ decreases from 0.9 to 0.5 when number of feedback bits B increases. Moreover, as in Observation 1, the optimal $\alpha^\star$ with $B = 32$ is nearly the same as the optimal one with perfect CDI. Fig. 2 shows the simulation results of the secrecy rate versus SNR for $\alpha = 0.9$ and different B. As expected, the secrecy rate with quantized CDI is upper-bounded, in sharp contrast to that with perfect CDI. Also at high SNR for any fixed B, the secrecy rate inner-bound is close to the upper-bound in Theorem 1, which means that additional CQI at the transmitter gains little at this region. From these figures, our results from large n_t analysis in subsection III-D is still valid for practical n_t. Fig. 3 shows the simulation results of MISOSE feedback bit scaling to verify our analysis in Section IV. As power increases, we try to increase feedback bits B satisfying (28) at the same time to fit a constant secrecy rate loss Δ_r between perfect CDI and quantized CDI. Note that when Δ_r decreases, the bits predicted in (28) from our outer-bound in Theorem 3 is more efficient. It results from that small Δ_r requires larger B which makes upper-bound (24) tighter.

For the MIMOME case, we set the antennas at the legitimate receiver and eavesdropper to $n_r = n_e = 2$. In Fig. 4 we can see that the secrecy rate still behaves similarly as MISOSE case, that is, $\alpha^\star$ decreases to 0.5 when B increases. In addition, from the figure we can find that the secrecy rate of MIMOME is better than that of MISOSE. It means that in our setting, the number of multiple antennas at the eavasdropper is not large enough to overcome the benefits of multiple legitimate receive antennas. The results for MIMOME feedback bit scaling law are shown in Fig. 5. Although we only provide an approximation to the required bits for constant rate loss at the MIMOME case, one can see from this figure that the predictions are still very accurate.

VII. Conclusions

We have presented the impact of quantized channel feedback on the secrecy rate achievable using artificial-noise assisted beamforming. Significant secrecy rate loss may occur due to AN leakage without perfect CDI. More specifically, the secrecy rate achievable under quantized CDI will be upper-bounded by a constant when the number of feedback bits is fixed. To maintain a constant rate loss compared to the perfect CDI case, the required scaling of B with respect to the increase of transmission power P has been derived. Moreoever, we also have shown how the optimal power allocation between signal and AN should be adjusted with respect to B in order to limit the effect of AN leakage. The theoretical results have been verified through computer simulations.

Appendix

A. Proof of Theorem 1

According to Definition 1, we can upper bound R as

$$\begin{aligned} nR - n\varepsilon < H(w|\bar{y_e}^n, \mathbf{h}_r^n, \mathbf{h}_e^n) &\leq I(w; \bar{y_r}^n|\bar{y_e}^n, \mathbf{h}_r^n, \mathbf{h}_e^n) + n\delta_1 \quad (51) \\ &\leq I(s^n; \bar{y_r}^n|\bar{y_e}^n, \mathbf{h}_r^n, \mathbf{h}_e^n) + n\delta_1, \quad (52) \end{aligned}$$

where $\delta_1 > 0$, the first inequality follows [2] and the second one is due to the data processing inequality [11] according to the Markov chain $w \leftrightarrow s^n \leftrightarrow (\bar{y_r}^n, \bar{y_e}^n)$. Now, following [2]

$$nR \leq \int\int [I(s; \bar{y_r}|\mathbf{h_r}, \mathbf{h_e}) - I(s; \bar{y_e}|\mathbf{h_r}, \mathbf{h_e})]^+ N(\mathbf{h_r}, \mathbf{h_e}) d\mathbf{h_r} d\mathbf{h_e} + n\delta, \quad (53)$$

where $N(\mathbf{h_r}, \mathbf{h_e})$ denotes the number of times the channel is in fading state $(\mathbf{h_r}, \mathbf{h_e})$ over the interval $[0, n]$ and $\delta = \delta_1 + \varepsilon$. Here we use the notation $\int(\cdot)d\mathbf{h_r}$ to simplify the multi-dimensional integral over $n_t \times 1$ vector $\mathbf{h_r}$. We will focus on the upper-bound

$$[I(s; \bar{y_r}|\mathbf{h_r}, \mathbf{h_e}) - I(s; \bar{y_e}|\mathbf{h_r}, \mathbf{h_e})]^+. \quad (54)$$

Since with fixed fading state, the channel (4) is equivalent to a scalar Gaussian channel we know that Gaussian s optimizes (54) [15]. Now we will further upper-bound (54) to find the

closed-form upper-bound as in the Theorem statement. We let the power of message-carrying signal of fading state $(\mathbf{h_r}, \mathbf{h_e})$ be as $P_s^n = \mathbf{E}[\Sigma_{i=1}^n |s_w(i)|^2 \mathbf{1}_{\mathbf{h_r}(i)=\mathbf{h_r}, \mathbf{h_e}(i)=\mathbf{h_e}}]$, where s_w are the codewords corresponding to the message w and the expectation is taken over all codewords. The power of artificial noise P_a^n is defined similarly. To simplify notations, we also define the equivalent channel gains from (4) as $h_r^s \triangleq \mathbf{h_r}^H \hat{\mathbf{g}}_\mathbf{r}$, $\mathbf{h_r^a} \triangleq \mathbf{h_r}^H \hat{\mathbf{N}}_\mathbf{g}$, $h_e^s \triangleq \mathbf{h_e}^H \hat{\mathbf{g}}_r$ and $\mathbf{h_e^a} \triangleq \mathbf{h_e}^H \hat{\mathbf{N}}_\mathbf{g}$. From (54), we have

$$\begin{aligned} I(s;\bar{y_r}|\mathbf{h_r},\mathbf{h_e}) - I(s;\bar{y_e}|\mathbf{h_r},\mathbf{h_e}) \leq & I(s; h_r^s s + \mathbf{h_r^a a}|\mathbf{h_r},\mathbf{h_e}) - I(s;\bar{y_e}|\mathbf{h_r},\mathbf{h_e}) \\ = & H(h_r^s s + \mathbf{h_r^a a}) - H(\mathbf{h_r^a a}) - H(\mathbf{h_e^a a} + h_e^s s) + H(\mathbf{h_e^a a}), \end{aligned} \tag{55}$$

where the inequality comes from the data processing inequality due to the Markov chain $s \leftrightarrow h_r^s s + \mathbf{h_r^a a} \leftrightarrow \bar{y_r}$. It can be easily checked that taking $[]^+$ operation on both sides of inequality (55) will not change its ordering, then

$$[I(s;\bar{y_r}|\mathbf{h_r},\mathbf{h_e}) - I(s;\bar{y_e}|\mathbf{h_r},\mathbf{h_e})]^+ \leq \left[\log \frac{P_a^n + \frac{|h_r^s|^2}{\|\mathbf{h_r^a}\|^2} P_s^n}{P_a^n + \frac{|h_e^s|^2}{\|\mathbf{h_e^a}\|^2} P_s^n}\right]^+. \tag{56}$$

Now from (53)(54)(56),

$$R - \delta \leq \int\int \left[\log \frac{P_a^n + \frac{|h_r^s|^2}{\|\mathbf{h_r^a}\|^2} P_s^n}{P_a^n + \frac{|h_e^s|^2}{\|\mathbf{h_e^a}\|^2} P_s^n}\right]^+ \frac{N(\mathbf{h_r},\mathbf{h_e})}{n} d\mathbf{h_r} d\mathbf{h_e} = \mathbf{E}\left[\left(\log \frac{P_a + \frac{|h_r^s|^2}{\|\mathbf{h_r^a}\|^2} P_s}{P_a + \frac{|h_e^s|^2}{\|\mathbf{h_e^a}\|^2} P_s}\right)^+\right] \tag{57}$$

where we denote the limits of P_s^n and P_a^n when $n \to \infty$ as P_s and P_a, respectively, and the last equality holds as $n \to \infty$ due to the ergodicity of the channel [2].

Now we optimize (57) under the constraint $\mathbf{E}_{\mathbf{h}_r,\mathbf{h}_e}[P_s + (n_t - 1)P_a] \leq P$. Note that the pair (P_s, P_a) varies for each fading states since CQI $\|\mathbf{h_r}\|$ is known at Tx. Since P_s and P_a are not negative, for each fading state, whenever $(|h_r^s|^2/\|\mathbf{h_r^a}\|^2) \geq (|h_e^s|^2/\|\mathbf{h_e^a}\|^2)$,

$$\left[\log \frac{P_a + \frac{|h_r^s|^2}{\|\mathbf{h_r^a}\|^2} P_s}{P_a + \frac{|h_e^s|^2}{\|\mathbf{h_e^a}\|^2} P_s}\right]^+ \tag{58}$$

is positive. And from

$$\log \frac{P_a + \frac{|h_r^s|^2}{\|\mathbf{h_r^a}\|^2} P_s}{P_a + \frac{|h_e^s|^2}{\|\mathbf{h_e^a}\|^2} P_s} = \log \left[1 + \frac{(\frac{|h_r^s|^2}{\|\mathbf{h_r^a}\|^2} - \frac{|h_e^s|^2}{\|\mathbf{h_e^a}\|^2}) P_s}{P_a + \frac{|h_e^s|^2}{\|\mathbf{h_e^a}\|^2} P_s}\right],$$

it is easy to see that in this case (58) is less than

$$\left[\log\left(\frac{|h_r^s|^2}{\|\mathbf{h_r^a}\|^2}/\frac{|h_e^s|^2}{\|\mathbf{h_e^a}\|^2}\right)\right]^+. \tag{59}$$

Otherwise, if $(|h_r^s|^2/\|\mathbf{h_r^a}\|^2) < (|h_e^s|^2/\|\mathbf{h_e^a}\|^2)$, (58) will be zero, it is still less than (59). Thus we have the final bound as

$$R \leq \mathbf{E}\left(\left[\log\left(\left(\frac{|h_r^s|^2}{\|\mathbf{h_r^a}\|^2}/\frac{|h_e^s|^2}{\|\mathbf{h_e^a}\|^2}\right)^2\right)\right]^+\right) + \delta. \tag{60}$$

Since $\delta \to 0$ as $n \to \infty$, (15) is valid. Although we have only proved the case where n is sufficiently large, with the same reason as [2], the above bound still holds for any n and it concludes the proof.

B. Proof of Lemma 1

We will show that when $n_t \to \infty$

$$\frac{\|\mathbf{h}_e^H \hat{\mathbf{g}}_r\|^2}{\|\mathbf{h}_e^H \hat{\mathbf{N}}_g\|^2} \xrightarrow{a.s.} \frac{1}{n_t - 1}. \tag{61}$$

Since the left-hand-side of (61) does not depend on $\|\mathbf{h}_e\|^2$, without loss of generality, we assume that $\mathbf{h}_e$ has i.i.d. complex Gaussian elements due to the isotropic fading assumption [10]. We recast left-hand-side of (61) as

$$\frac{\frac{1}{n_t}\mathbf{h}_e^H(\hat{\mathbf{g}}_r\hat{\mathbf{g}}_r^H)\mathbf{h}_e}{\frac{1}{n_t}\mathbf{h}_e^H(\hat{\mathbf{N}}_g\hat{\mathbf{N}}_g^H)\mathbf{h}_e}.$$

Since $\hat{\mathbf{g}}_r$ and $\hat{\mathbf{N}}_g$ are independent of $\mathbf{h}_e$, and matrices $\hat{\mathbf{g}}_r\hat{\mathbf{g}}_r^H$ and $\hat{\mathbf{N}}_g\hat{\mathbf{N}}_g^H$ both have uniformly bounded spectral radius for all n_t (as 1), following the proof of [16, Corollary 1]

$$\frac{\frac{1}{n_t}\mathbf{h}_e^H(\hat{\mathbf{g}}_r\hat{\mathbf{g}}_r^H)\mathbf{h}_e}{\frac{1}{n_t}\mathbf{h}_e^H(\hat{\mathbf{N}}_g\hat{\mathbf{N}}_g^H)\mathbf{h}_e} \xrightarrow{a.s.} \frac{\mathrm{Tr}(\hat{\mathbf{g}}_r\hat{\mathbf{g}}_r^H)}{\mathrm{Tr}(\hat{\mathbf{N}}_g\hat{\mathbf{N}}_g^H)} = \frac{1}{n_t - 1},$$

where the last equality comes from that both $\hat{\mathbf{g}}_r$ and $\hat{\mathbf{N}}_g$ are unit norm vectors. And (61) is valid. As [4], it is then easy to see that the convergence in expectation in Lemma 1 holds with the almost-surely convergence in (61).

C. Proof of Corollary 1

First we investigate the outer-bound. When $n_t \to \infty$, following the proof of Lemma 1, $\|\mathbf{g}_e^H \hat{\mathbf{g}}_r\|^2 / \|\mathbf{g}_e^H \hat{\mathbf{N}}_g\|^2 \stackrel{a.s.}{\to} \frac{1}{n_t - 1}$. The outer-bound becomes

$$\mathbf{E}\left[\log\left(\frac{(n_t-1)\|\mathbf{g}_r^H \hat{\mathbf{g}}_r\|^2}{\|\mathbf{g}_r^H \hat{\mathbf{N}}_g\|^2}\right)\right]^+ = \mathbf{E}\left[\log\left(\frac{(n_t-1)(\cos\theta)^2}{(\sin\theta)^2}\right)\right]^+.$$

Since $(\cot\theta)^2 \geq 2^{\frac{B}{n_t-1}} - 1$ [7], which is larger than 1 if $B \geq n_t$. The outer bound then becomes

$$\mathbf{E}\left[\log((n_t-1)(\cot\theta)^2)\right]. \tag{62}$$

As for the inner bound, from Lemma 1 and (14), when $n_t \to \infty$ it becomes

$$\mathbf{E}\left[1 + \log\left(\frac{\|\mathbf{h}_r\|(\cos\theta)^2\alpha^*}{\frac{\|\mathbf{h}_r\|^2}{n_t-1}(\sin\theta)^2 + \frac{1}{(1-\alpha^*)P}}\right)\right] > \mathbf{E}\left[\log\left(\frac{\|\mathbf{h}_r\|(\cos\theta)^2\alpha^*}{\frac{\|\mathbf{h}_r\|^2}{n_t-1}(\sin\theta)^2 + \frac{1}{(1-\alpha^*)P}}\right)\right].$$

When $P \to \infty$, $1/((1-\alpha^*)P) \stackrel{a.s.}{\to} 0$, the right-hand-side approaches

$$\mathbf{E}\left[\log((n_t-1)(\cot\theta)^2)\right] + \log(\alpha^*).$$

Thus from (62), we know that the difference between inner and outer bounds are bounded by $|\log(\alpha^*)|$.

REFERENCES

[1] A. Wyner, "The wiretap channel," Bell System Technical Journal, vol. 54, pp. 1355–1387, 1975.

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

[3] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *submitted to IEEE Trans. Inform. Theory*, 2007.

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

[6] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output gaussian broadcast channels with confidential messages," *submitted to IEEE Trans. Inform. Theory*, March, 2009.

[7] T. Yoo, N. Jindal, and A. Goldsmith, "Multi-antenna downlink channels with limited feedback and user selection," *IEEE J. Select. Areas Commun.*, vol. 25, no. 7, pp. 1478–1491, 2007.

[8] N. Jindal, “MIMO broadcast channels with finite-rate feedback,” *IEEE Trans. Inform. Theory*, vol. 52, no. 11, pp. 5045–5060, 2006.

[9] N. Ravindran and N. Jindal, “Limited feedback-based block diagonalization for the MIMO broadcast channel,” *IEEE J. Select. Areas Commun.*, vol. 26, no. 8, pp. 1473–1482, 2008.

[10] S. Jafar and A. Goldsmith, “Isotropic fading vector broadcast channels: The scalar upper bound and loss in degrees of freedom,” *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 848–857, 2005.

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

[12] K. Mukkavilli, A. Sabharwal, E. Erkip, and B. Aazhang, “On beamforming with finite-rate feedback in multiple-antenna systems,” *IEEE Trans. Inform. Theory*, vol. 49, pp. 2562–2579, 2003.

[13] A. M. Tulino and S. Verdu, *Random Matrix Theory and Wireless Communications*. Delft, Netherlands: now Publisher Inc., 2004.

[14] W. Dai, Y. Liu, and B. Rider, “Quantization bounds on Grassmann manifolds and applications to MIMO communications,” *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 1108–1123, 2008.

[15] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[16] J. Evans and D. Tse, “Large system performance of linear multiuser receivers in multipath fading channels,” *IEEE Trans. Inform. Theory*, vol. 46, no. 6, pp. 2059–2078, 2000.

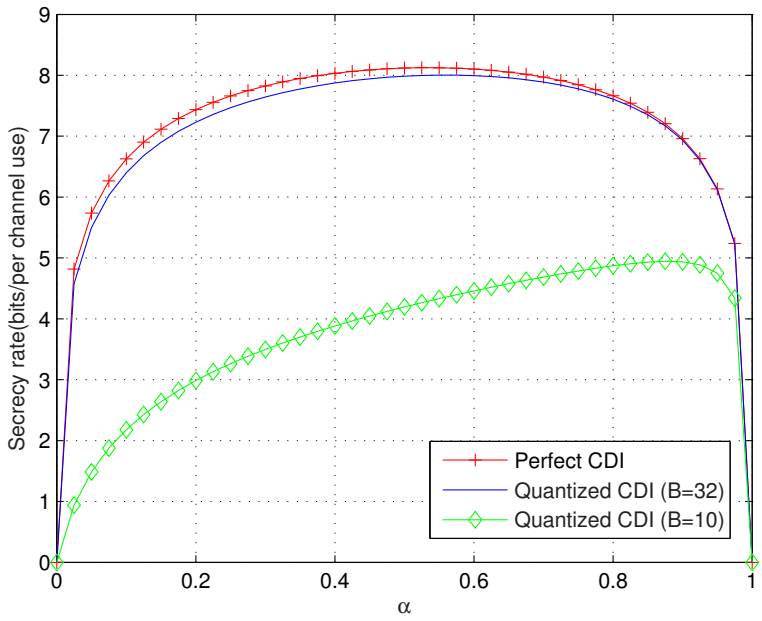

Fig. 1: Secrecy rate versus α with AN for SNR$= 25dB$ and $n_r = n_e = 1$.

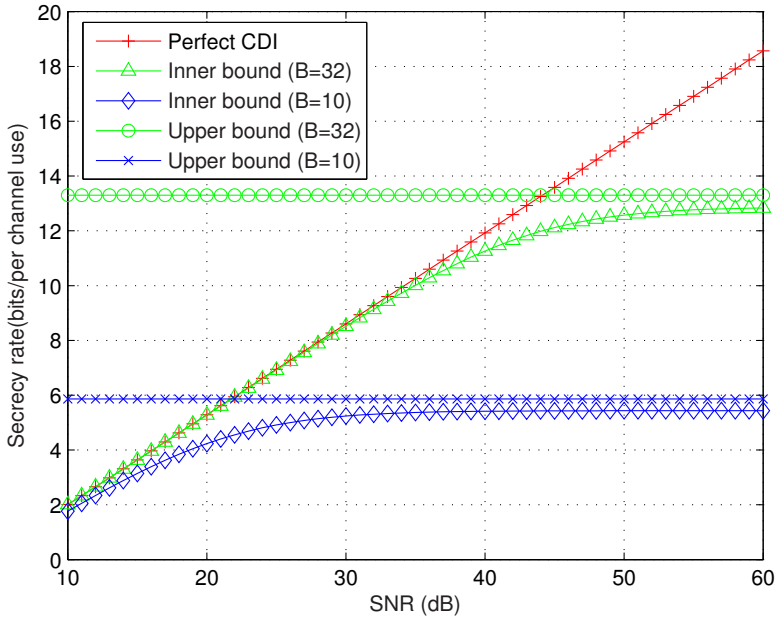

Fig. 2: Secrecy rate versus SNR with AN for $\alpha = 0.9$ and $n_r = n_e = 1$.

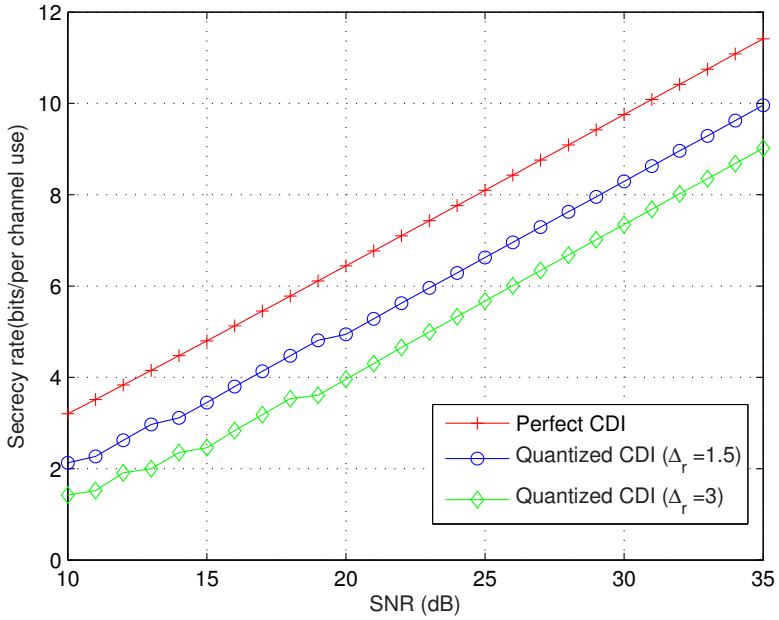

Fig. 3: Secrecy rate versus SNR when $n_r = n_e = 1$.

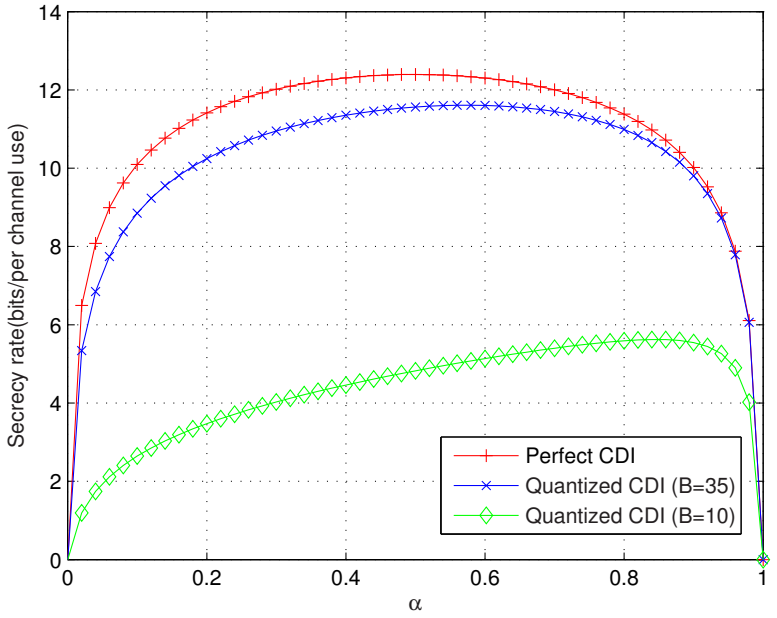

Fig. 4: Secrecy rate versus α with AN for SNR$= 25dB$ and $n_r = n_e = 2$.

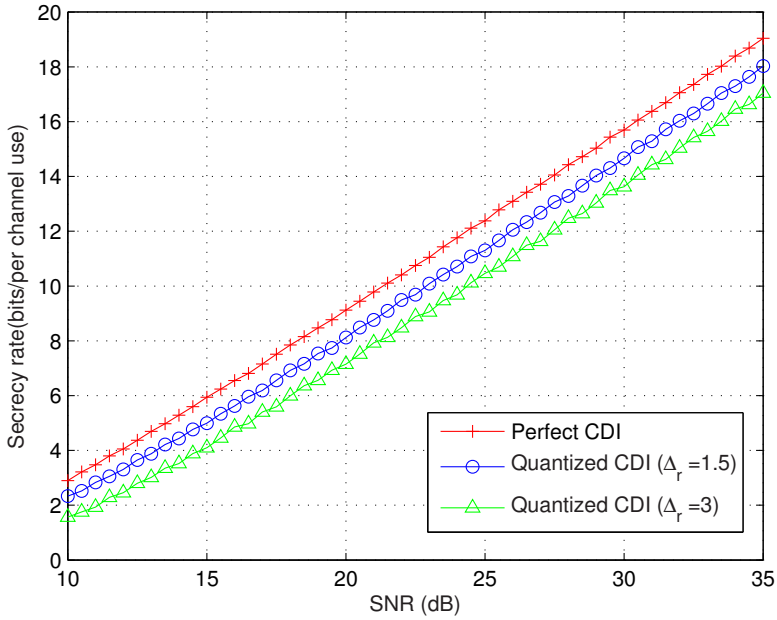

Fig. 5: Secrecy rate versus SNR when $n_r = n_e = 2$.