Secure MIMO Communications under Quantized Channel Feedback in the presence of Jamming

Theodoros Tsiligkaridis, Member, IEEE

Abstract—We consider the problem of secure communications in a MIMO setting in the presence of an adversarial jammer equipped with $n_j$ transmit antennas and an eavesdropper equipped with $n_e$ receive antennas. A multiantenna transmitter, equipped with $n_t$ antennas, desires to secretly communicate a message to a multiantenna receiver equipped with $n_r$ antennas. We propose a transmission method based on artificial noise and linear precoding and a two-stage receiver method employing beamforming. Under this strategy, we first characterize the achievable secrecy rates of communication and prove that the achievable secure degrees-of-freedom (SDoF) is given by $d_s = n_r - n_j$ in the perfect channel state information (CSI) case. Second, we consider quantized CSI feedback using Grassmannian quantization of a function of the direct channel matrix and derive sufficient conditions for the quantization bit rate scaling as a function of transmit power for maintaining the achievable SDoF $d_s$ with perfect CSI and for having asymptotically zero secrecy rate loss due to quantization. Numerical simulations are also provided to support the theory.

Index Terms—Quantized CSI feedback, MIMO communication, linear precoding, Grassmann manifold, physical layer security, secrecy rate.

I. INTRODUCTION

Secrecy in the physical layer is concerned with maximizing the information rate of a transmitter-receiver pair such that reliable communication is possible, while keeping the information as private as possible if eavesdroppers listen. The seminal work of Wyner on the wiretap channel [1] has shown that it is possible to reliably communicate at a strictly positive rate while an eavesdropper listening to the transmitted signal through its own channel cannot decode the message. These results were generalized to Gaussian channels by Leung-Yan-Cheong and Hellman in [2] and to arbitrary broadcast channels by Csiszar and Korner in [3]. Following these important early works, various extensions to different system settings and assumptions have been made. Particularly, there has been considerable interest in studying physical layer secrecy for multiple-input multiple-output (MIMO) Gaussian channels, as the use of multiple antennas can increase secrecy capacity [4], [5]. In many works, the assumption of the transmitter knowing its channel to the eavesdropper is often impractical. As a result, transmission strategies exploiting multiple antennas and injecting controlled artificial noise into the transmitted signal have been proposed in [6] in order to enhance secrecy.

Quantized feedback schemes have been proposed and studied in the literature for single user and multiple user downlink communication systems in [7], [8]. Motivated by the quantization approach of Rezaee & Guillaud [9], [10], which considered interference alignment for the MIMO interference channel with quantized channel feedback, we study the value of quantized feedback for secrecy communications in the presence of a hostile jammer. A key motivator for our work is the paper by Krishnamachari et al. [11], where a Grassmannian feedback scheme was studied in the context of interference alignment for MIMO interference channel. It was shown that if the feedback bit rate increases fast enough as a function of signal-to-noise ratio (SNR), the quantized channel estimates can be used at the transmitters to achieve the full multiplexing gain. However, communication under secrecy was not considered in these works on quantized CSI feedback. Optimal power allocation algorithms and achievable secrecy rates have been recently studied in the context of secrecy communications with artificial noise in [12], [13], but no degree-of-freedom (DoF) analysis is performed and perfect CSI is assumed. To the best of our knowledge, the value of quantized channel feedback on the secure DoF gain has not been studied in the literature in the context of communicating under secrecy and in the presence of a hostile jammer.

The transmission model that we consider consists of transmitting a linear combination of artificial noise and desired signal to a receiver. The purpose of the artificial noise is to confuse the eavesdropper and the desired signal is the signal to be decoded by the intended receiver. The artificial noise aspect has been studied in [6], [14], [15], [16]. In [6], the approach of transmitting artificial noise in the nullspace of the direct channel matrix was proposed assuming the number of transmit antennas, $n_t$, are more than the number of receive antennas, $n_r$. Thus, the designed artificial noise has no impact on the received signal at the intended receiver, but causes degradation at the eavesdropper thus enhancing secrecy. Robust beamforming for secure MIMO communications was studied in [15] under inaccurate CSI using a second-order perturbation analysis. The effect of delayed perfect CSIT on the SDoF gain was studied in [16] in the context of the two-user broadcast MIMO channel. In [14], the optimal power allocation among artificial noise and desired signal is derived such that the ergodic secrecy rate is maximized for a fixed number of feedback bits and transmit power. In addition, a scaling law between feedback bits and power is derived to guarantee a constant secrecy rate loss compared to the perfect CSI case. Our work differs from these works since we derive explicit conditions for the quantization bit scaling that
guarantee the optimal SDoF scaling, under similar assumptions on channel values as made in [11], and in addition we consider a jammer interfering with the received signal and show that the secrecy rate loss due to quantization is asymptotically negligible as SNR grows. Furthermore, our work differs from [14] because we consider quantization of a function of the direct channel matrix using (deterministic) quantization theory on the Grassmann manifold, adopt different channel conditions as adopted in [9], [10], [11] and thus, develop different proof techniques. In addition, the SDoF performance of artificial noise transmission schemes has not been studied in [6], and we also consider the lack of instantaneous perfect CSI by assuming the availability of quantized CSI. Our work differs from [15], [16] in that we consider a jammer and the effect of Grassmannian-based quantized instantaneous CSI on SDoF gain in a point-to-point MIMO channel.

In our problem formulation, the receiver’s strategy is to null out the jammer interference and use its remaining resources to recover the information-bearing signal from the transmitter through beamforming. Under perfect CSI conditions, assuming \( n_t > n_r \), the transmitter designs the artificial noise signal to lie in the nullspace of the channel matrix \( H_d \) and the information-bearing signal to lie in the orthogonal complement of the null space of \( H_d \). Under this linear precoding strategy, the receiver sees no leakage due to artificial noise in the received signal. However, if the transmitter has imperfect CSI, then the received signal will contain a non-negligible amount of artificial noise. In the high SNR regime, this leakage will deteriorate the secrecy rate performance and drive the SDoF to zero. In order to maintain the full SDoF gain of the system, the rate of quantized feedback needs to increase appropriately as a function of SNR. In this paper, we characterize this rate and identify the key parameters associated with it. We also prove that, as the transmit power grows asymptotically, there is no loss in secrecy rate performance due to quantization.

A. Outline

The outline of this paper is as follows. Section II formulates the basic problem. Section III studies the achievable secrecy communication rates in the case of perfect CSI. Section IV studies the case of quantized CSI and derives performance bounds on the achievable secure degrees-of-freedom. The theory is illustrated by simulation in Section V and is followed by our conclusions in Section VI.

B. Notation

We use \( \mathbb{R} \) and \( \mathbb{C} \) to denote the real and complex fields. We use bold lowercase letters \( x \) to denote vectors and bold uppercase letters \( A \) for matrices. Given a matrix \( A \in \mathbb{C}^{m \times n} \), we let \( A^* \) denote its Hermitian conjugate, and \( A^T \) denote its transpose. The trace operator \( \text{tr}(\cdot) \) on a square matrix is simply the sum of its diagonal entries. Let \( \text{Nul}(A) \) and \( \text{Col}(A) \) denote the nullspace and column spaces (i.e., range) of the matrix \( A \).

We let \( \mathcal{N}_c(\mu, \Sigma) \) denote the complex multivariate normal distribution with mean \( \mu \) and covariance \( \Sigma \). Consider two sequence of real numbers \( \{a_p\} \) and \( \{b_p\} \) indexed by \( P \). Consider two sequences \( \{a_p\} \) and \( \{b_p\} \). The asymptotic notation \( a_p = O(b_p) \) as \( P \to \infty \) implies that there exists \( K > 0, P_0 \) such that for all \( P \geq P_0 \), we have \( |a_p| \leq K|b_p| \). The asymptotic notation \( a_p = o(b_p) \) means that for all \( \epsilon > 0 \), there exists \( P_0(\epsilon) = P_0 \) such that for all \( P \geq P_0 \), we have \( |a_p| \leq \epsilon |b_p| \). We use \( \log(\cdot) \) to denote the logarithm with base 2 and \( \log_e(\cdot) \) to denote the natural logarithm. Define the thresholding operator \( (\cdot)_+ = \max(\cdot, 0) \).

II. Problem Formulation

We consider the point-to-point MIMO channel with a transmitter (Tx) and a legitimate receiver (Rx). There is a jammer (J) degrading the received signal at Rx and an eavesdropper (Eve) observing a noisy version of the transmitted signal. Define the channel matrices \( H_d \in \mathbb{C}^{n_r \times n_t} \) as the channel between Tx and Rx, \( H_e \in \mathbb{C}^{n_e \times n_t} \) as the channel between the Tx and Eve and \( H_j \in \mathbb{C}^{n_j \times n_t} \) as the channel between J and the Rx. The received signals at the legitimate receiver and Eve are respectively given by:

\[
\begin{align*}
\mathbf{y} &= \mathbf{H}_d \mathbf{x} + \mathbf{H}_j \mathbf{x}_j + \mathbf{n} \quad \text{(Rx)} \\
\hat{\mathbf{y}} &= \mathbf{H}_e \mathbf{x} + \tilde{\mathbf{n}} \quad \text{(Eve)}
\end{align*}
\]

where \( \mathbf{x} \) is the transmitted signal and \( \mathbf{x}_j \) is the jammer signal. The additive receiver noises \( \mathbf{n} \) and \( \tilde{\mathbf{n}} \) are assumed to be white and Gaussian distributed, i.e., \( \mathbf{n} \sim \mathcal{N}_c(0, \sigma^2 \mathbf{I}_{n_e}) \), \( \tilde{\mathbf{n}} \sim \mathcal{N}_c(0, \sigma^2 \mathbf{I}_{n_e}) \).

In this paper, we assume that Eve and J and cooperative in the sense that the jammer does not interfere with the eavesdropper signal. This can be realized in one of two ways. One way that this can be realized is if Eve and J are one simultaneous-transmit-and-receive unit, comprised of \( n_e \) receive antennas and \( n_j \) transmit antennas as depicted in Figure I. Another way that this can be realized is to have Eve and J be separate nodes with Eve having \( N_e = n_e + n_j \) receive antennas and J having \( n_j \) transmit antennas. Then, Eve can null out the undesired jammer interference by projecting its received signal in a subspace of dimension \( n_e \), leading to the linear observation model (2). To illustrate this, say that Eve has \( N_e \) receive antennas and observes:

\[
\mathbf{y}_e = \mathbf{G}_e \mathbf{x} + \mathbf{G}_j \mathbf{x}_j + \mathbf{n}_e
\]

where \( \mathbf{G}_e \) is the channel from Tx to Eve, \( \mathbf{G}_j \) is the channel from J to Rx and \( \mathbf{n}_e \) is the receiver thermal noise at Eve. Considering the SVD of \( \mathbf{G}_j = \mathbf{U}_j \mathbf{S}_j \mathbf{V}_j^T \), we can choose \( \mathbf{U}_{0,j} \in \mathbb{C}^{N_e \times n_e} \) to consist of the columns of \( \mathbf{U}_j \) corresponding to zero singular values. Then, defining the projection \( \tilde{\mathbf{y}} = \mathbf{U}_{0,j}^T \mathbf{y}_e \) [1] we obtain the model (2) with \( \mathbf{H}_e = \mathbf{U}_{0,j} \mathbf{G}_e \) and \( \tilde{\mathbf{n}} = \mathbf{U}_{0,j} \mathbf{n}_e \). Under the assumption that channel matrix elements are drawn i.i.d. from a continuous distribution, it follows that with probability 1, \( \mathbf{H}_e \) is full-rank and the equivalent model (2) can be used without loss of generality.

As in [11], [9], [10], we assume all elements of the channel matrices are drawn i.i.d. from a continuous distribution, and the channel values do not change during the signal transmission. The receiver is assumed to have perfect knowledge of

\[\text{Here, } \text{Nul}(\mathbf{U}_{0,j}^T) = \text{Col}(\mathbf{G}_j) \text{ is the nullspace condition that is used in the nulling operation.} \]
Fig. 1: Block diagram of secrecy communication problem in the presence of a jammer.

**A. Transmitter Strategy**

Assuming $n_t > n_r$, the channel matrix $H_d$ has rank equal to $n_r$, which implies that there are $n_t - n_r$ dimensions available for artificial noise and $n_r$ dimensions for information transmission.

We assume the transmitter splits its available power $P$ into two components, the artificial noise and the information-bearing signal, using a linear combination:

$$x = \sqrt{\rho}W_1x_s + \sqrt{1-\rho}W_2x_{an}$$  \hspace{1cm} (3)

where $x_s \in \mathbb{C}^{n_r}$ is the information bearing signal, $x_{an} \in \mathbb{C}^{n_t-n_r}$ is artificial noise and $\rho$ is the percentage of power allocated to $x_s$. The linear precoding matrices $W_1 \in \mathbb{C}^{n_r \times n_r}$ and $W_2 \in \mathbb{C}^{n_t \times n_t-n_r}$ are assumed to be truncated unitary matrices. We also assume that $x_s$ is independent of $x_{an}$. We let the covariance matrices of $x_s$ and $x_{an}$ be given by $K_{x_s} \in \mathbb{C}^{n_r \times n_r}$ and $K_{x_{an}} \in \mathbb{C}^{(n_t-n_r) \times (n_t-n_r)}$, respectively.

In order to design $(W_1, W_2)$ such that the artificial noise component cancels out at the receiver, the columns of $W_2$ must lie in the null space of $H_d \in \mathbb{C}^{n_r \times n_t}$. This can be accomplished through the singular value decomposition (SVD) of $H_d$. Then, $H_dW_2 = 0$.

**B. Receiver Strategy**

The receiver has instantaneous knowledge of $H_d$ and $H_j$. To null out the jammer’s signal, the post-processing truncated unitary matrix $V \in \mathbb{C}^{n_t \times n_r-n_j}$ at the receiver is applied:

$$\hat{y} = V^* y = V^*H_d x + \hat{n}$$  \hspace{1cm} (4)

where $\hat{n} = V^*n \sim \mathcal{N}(0, \sigma^2I)$ since $V^*V = I_{n_r-n_j}$.

Consider the SVD of $H_j$:

$$H_j = U(H_j)\Sigma(H_j)V(H_j)^*$$

$$= [U_1(H_j)]U_0[H_j] \begin{bmatrix} \Sigma_1(H_j) \\ 0_{n_r-n_j \times n_j} \end{bmatrix} V(H_j)^*$$

Choosing the columns of $V$ span the left nullspace of $H_j$, i.e.,

$$V = U_0(H_j)$$  \hspace{1cm} (5)

yields the desired nulling condition $V^*H_j = 0$.

**C. Secrecy Degrees-of-Freedom (SDDoF)**

The secrecy capacity is known as a quantity measuring the maximal rate of reliable communication while maintaining secrecy to Eve [3]. The secrecy capacity is generally known to be [3, 5, 17]:

$$C_s = \max_{K_{x_s} \succeq 0, ||K_{x_s}|| \leq P} (I(x_s; y) - I(x_s; y)_{+})$$

where $I(X; Y)$ denotes the mutual information between $X$ and $Y$ [18].

For a given input covariance matrix $K_{x_s}$ satisfying the power constraint $tr(K_{x_s}) \leq P$, the achievable secrecy rate under the models (3) and (4) is given by:

$$R_s(K_{x_s}) = (I(x_s; \hat{y}) - I(x_s; \hat{y})_{+})$$  \hspace{1cm} (6)

As Theorem 1 shows (see Appendix A), $R_s(K_{x_s})$ will be positive for $P$ large enough under certain assumptions, and thus the thresholding operator $(-)_+$ can be omitted for the high SNR analysis to be presented in this paper. The (achievable) secure degrees-of-freedom (SDDoF) are defined as:

$$d_s = \lim_{P \to \infty} \frac{R_s(K_{x_s})}{\log P}$$

The intuitive meaning of this metric is that there are $d_s$ data streams that can be reliably communicated to the receiver without having the eavesdropper being able to decode the transmitted information.

**III. Perfect CSI: Achievable Secrecy Rate & SDDoF**

For the case of perfect CSI at the transmitter, the precoding matrix $W_2$ can be designed as $W_2 = V_0(H_d) \in \mathbb{C}^{n_t \times n_t-n_r}$, where the SVD of $H_d \in \mathbb{C}^{n_r \times n_t}$ is given by:

$$H_d = U(H_d)\Sigma(H_d)V(H_d)^*$$

$$= U(H_d) \begin{bmatrix} \Sigma_1(H_d) \\ 0_{n_r \times n_t-n_r} \end{bmatrix} V_0(H_d)^*$$

In that case, we can also choose $W_1 = V_1(H_d) \in \mathbb{C}^{n_r \times n_r}$ in order to guarantee orthogonality between the information bearing signal $W_1 x_s$ and the artificial noise signal $W_2 x_{an}$. Then, the post-processed received signal at Rx and the received signal at Eve become:

$$\hat{y} = \sqrt{\rho}V^* H_d W_1 x_s + \tilde{n}$$

$$= \sqrt{\rho}V^* U(H_d) \Sigma_1(H_d) V_1(H_d)^* V_0(H_d) x_s + \tilde{n}$$

$$= \sqrt{\rho}V^* U(H_d) \Sigma_1(H_d) x_s + \tilde{n}$$

$$= \sqrt{\rho} \tilde{H}_e x_s + \tilde{n}$$

$$\tilde{y} = \sqrt{\rho} V^* H_d W_1 x_s + \tilde{n}$$

$$= \sqrt{\rho} V^* U(H_d) \Sigma_1(H_d) V_1(H_d)^* V_0(H_d) x_s + \tilde{n}$$

$$= \sqrt{\rho} H e, x_s + \sqrt{1-\rho} H e, an x_{an} + \tilde{n}$$

where we defined $H = V^* U(H_d) \Sigma_1(H_d)$ as the transformed $(n_r-n_j) \times n_r$ channel matrix after post-processing. We also defined $H_{e,x} = H e, V_1(H_d)$ and $H_{e,an} = H e, V_0(H_d)$. 
Using these expression for the received signals and the Gaussian noise assumptions, along with [5], we obtain an expression for the achievable secrecy rate under perfect CSI:

\[
R_s(K_{x_c}) = \log \det \left( I + \frac{\rho}{\sigma^2} HK_{x_c} H^* \right) - \log \left( \frac{\det(\rho H_{c,a} K_{x_c} H^*_{c,a} + (1-\rho) P H_{c,a} H^*_{c,a} + \sigma^2 I)}{\det((1-\rho \rho) P H_{c,a} H^*_{c,a} + \sigma^2 I)} \right)
\]

where we used \( K_{x_c} = \text{Cov}(x_s) \) and \( K_{x_{an}} = \text{Cov}(x_{an}) = \frac{P}{n_t - n_r} I_{n_t - n_r} \).

The next theorem shows that \( n_t - n_j \) SDoF are achievable under several mild assumptions.

**Theorem 1.** Assume the following:
- there exists constants \( c_0, c_1 \in [0, 1/n_t] \) such that
  \[
  c_0 P I \leq K_{x_c} \leq c_1 P I
  \]  \tag{7}
- \( n_t > n_r > n_j \)
- \( n_c \leq n_t - n_r \)

In the case of perfect CSI, it is possible to achieve up to \( d_s = n_t - n_j \) SDoF at most.

**Proof:** See Appendix A.

We remark that the SDoF \( d_s \) is independent of \( n_c \) because the eavesdropper’s rate \( I(X; Y) \) converges to a constant, dependent on \( n_e \), and thus it has an asymptotically vanishing contribution to the SDoF, i.e., \( \frac{I(X; Y)}{\log P} \to 0 \) as \( P \to \infty \).

The achievable \( d_s = n_t - n_j \) secure DoF is optimal since the jammer signal lies in a \( n_j \)-dimensional space and to null it out without any knowledge of its intrinsic dimension, receive beamforming leaves \( n_t - n_j \) effective number of antennas at the receiver to use for successful decoding of the transmitted message.

The sufficient conditions of Thm. 1 are very mild, given our goal of achieving \( n_t - n_j \) SDoF. If the condition \( n_t > n_r \) is violated, the right nullspace of \( H_d \) is empty, which implies that no precoding matrix \( W_2 \) exists such that \( H_d W_2 = 0 \). If \( n_r > n_j \) is violated, then no post-processing matrix \( V \) exists such that \( V^* H_j = 0 \), i.e., the receiver does not have enough antennas to cancel the jammer’s signal. If \( n_e > n_t - n_r \), then the eavesdropper has enough antennas to recover at least one data stream containing information because the artificial noise signal spans at most a \( (n_t - n_r) \)-dimensional space, leading to zero secrecy. The assumption \( n_c + n_e \leq n_t \) was also made in Section VI in [14]. Thus, all assumptions are necessary to proceed.

### IV. Quantized CSI: Achievable Secrecy Rate & SDoF

When there is imperfect CSI knowledge at the transmitter, the condition \( H_d W_2 = 0 \) will be violated and there will be some leakage of artificial noise at the receiver. As a consequence, the result of Theorem 1 no longer holds. In this section, we show that the same number of secure degrees-of-freedom can be achieved if the feedback rate scales fast enough as a function of transmit power.

#### A. Quantization on the Grassmann manifold

We assume that the receiver has perfect knowledge of the channel \( H_d \). Thus, it can perform the QR decomposition of the conjugate transpose of the channel matrix, i.e., \( H^*_d \):

\[
H^*_d = FC
\]  \tag{8}

where \( C \in \mathbb{C}^{n_r \times n_r} \) is an invertible matrix and \( F \in \mathbb{C}^{n_r \times n_r} \) is a tall orthonormal matrix whose columns span the same column space of \( H^*_d \). Thus, from the invertibility of \( C \), the condition \( H_d W_2 = 0 \) is equivalent to \( F^* W_2 = 0 \). A similar decomposition approach was considered in [10] for the MIMO interference channel. As in [10], a quantizer at the receiver uses \( N_f \) bits to describe the columns of \( F \) and transmits the index of the quantized codeword back to the transmitter through a noiseless feedback link. The transmitter and receiver share a predefined codebook \( S = \{ S_1, \ldots, S_{2^{N_f}} \} \) consisting of truncated unitary matrices of size \( n_t \times n_r \), which is designed using Grassmannian subspace packing. The quantization of the matrix \( F \) on the Grassmann manifold \( \mathcal{G}_{n_t, n_r} \) is mathematically described by the minimum distance problem:

\[
\hat{F} = \arg \min_{S \in \mathcal{S}} d_c(S, F)
\]  \tag{9}

where \( d_c(S, F) = \frac{1}{\sqrt{\rho}} ||SS^* - FF^*||_F \) is the chordal distance between \( S \) and \( F \) in \( \mathcal{G}_{n_t, n_r} \).

#### B. Transmitter Strategy under Quantized CSI

Given the quantized matrix \( \hat{F} \in \mathbb{C}^{n_t \times n_r} \), the transmitter designs the linear precoding matrices \( W_{1, Q} \) and \( W_{2, Q} \). Let the matrix \( W_{2, Q} \in \mathbb{C}^{n_r \times n_t - n_r} \) be chosen such that

\[
\hat{F}^* W_{2, Q} = 0_{n_r \times n_t - n_r}
\]  \tag{10}

This can be accomplished if the columns of \( W_{2, Q} \) are chosen to span the nullspace of \( \hat{F}^* \). We thus let \( W_{2, Q} \) be chosen such that its columns form a basis for \( \text{Null}(\hat{F}^*) \).

In order to maximize the amount of information being sent over the noisy channel \( H_d \), the precoded information signal \( W_{1, Q} x_s \) must always be orthogonal to the precoded artificial noise signal \( W_{2, Q} x_{an} \). In order for this to hold irrespective of the signals \( x_s \) and \( x_{an} \), \( W_{1, Q} \) must be orthogonal to \( W_{2, Q} \). This orthogonality implies that the matrix \( W_{1, Q} \in \mathbb{C}^{n_t \times n_r} \) must lie in the orthogonal complement of \( \text{Null}(\hat{F}^*) \). In other words, we let the columns of \( W_{1, Q} \) form a basis for \( \text{Col}(\hat{F}) \), i.e., \( W_{1, Q} = \hat{F} \).

#### C. Receiver Strategy under Quantized CSI

Given \( y \), the receiver uses a post-processing matrix to form the transformed vector:

\[
\tilde{y} = G^* V^* y
\]  \tag{11}

where \( V \) is the nulling matrix for the jammer defined in [5] and \( y \) is the received signal in (11). Given that \( V \) is already chosen using (5), we want to design \( G \in \mathbb{C}^{d_s \times d_s} \) as a function of \( V, F, C \) (all of which are available at the receiver). Let us choose \( G \) as:

\[
G^* = B^* FCV(V^* C^* CV)^{-1}
\]  \tag{12}
where \( B \in \mathbb{C}^{n_t \times d_s} \) is a tall truncated unitary matrix of full rank.

Let the leakage term be given by
\[
e_L = \sqrt{1 - \rho} G^* V^* H_d W_{2,Q} x_{an}
\]
The post-processed received signal can be written as
\[
\hat{y} = G^* (V^* H_d x + \tilde{n}) = \sqrt{\rho} G^* V^* H_d W_{1,Q} x_s + e_L + G^* \tilde{n}
\]

**D. Controlling the Leakage Power**

The next lemma bounds the power of the leakage term.

**Lemma 1.** Assuming a quantization codebook construction based on sphere-packing using \( N_f \) bits, the leakage power is bounded as:
\[
L(P) := \mathbb{E} \| e_L \|^2_2 \leq \frac{2(1 - \rho) P}{n_t - n_r} \left( \frac{2}{\rho^2 N_f} \right)^2 \left( 1 + o(2^{-N_f/N}) \right)
\]
where \( N = 2n_r(n_t - n_r) \) and \( c \) is a constant.

**Proof:** See Appendix B.

The corollary that follows provides a sufficient condition on the feedback rate to ensure that the leakage power stays bounded. This will be a key condition that will be used to prove the optimal SDoF scaling.

**Corollary 1.** Assume that the quantization with \( N_f \) feedback bits scales as:
\[
N_f = \frac{N}{2} \log_2 P = n_r(n_t - n_r) \log_2 P
\]
Then, the leakage power \( L(P) \) stays bounded as \( P \to \infty \), i.e., \( L(P) = O(1) \) as \( P \to \infty \).

**Proof:** See Appendix C.

We note that boundedness of the leakage power does not necessarily imply the achievability of the optimal SDoF. However, it provides a grasp on the feedback bit scaling that can possibly guarantee such a claim. Next, we show that the scaling condition \( (14) \) is sufficient to guarantee the optimal SDoF gain.

**E. SDoF Analysis**

Here, we show that the secrecy rate of the quantized CSI scheme achieves the same SDoF as the corresponding scheme with perfect CSI as derived in Theorem 1. In other words, there is no performance loss for large enough SNR.

Under the transmitter and receiver strategies proposed for quantized CSI, the achievable secrecy rate when CSI is perfect is given in (15) by:
\[
R_{s,G}^p = R_{s,G}^p (K_{x_s}) = I(x_s; y) - I(x_s; \hat{y}),
\]
where the subscript \( s \) denotes secrecy and the subscript \( G \) denotes post-processing with the matrix \( G^* \) in addition to \( V^* \) (recall (14)). Similarly, when only quantized CSI is available, the achievable secrecy rate is given by \( R_{s,G}^q \) in (16), where \((W_{1,Q}, W_{2,Q})\) are the designed precoding matrices under imperfect CSI. We note that in general \( W_1 \neq W_{1,Q} \) and \( W_2 \neq W_{2,Q} \), although they have the same rank.

Before proving the main result, we will need a few technical lemmas. We first recall the variational representation of the log-determinant function.

**Lemma 2.** Let \( E \in \mathbb{C}^{n \times n} \) be a positive definite matrix. Then,
\[
\log \det (E^{-1}) = \max_{S \geq 0} \left\{ -tr(SE) + \log \det(S) + n \right\}
\]
and the optimal solution is \( S^* = E^{-1} \).

**Lemma 2** implies the following perturbation bounds, which will be crucial for analyzing the secrecy rate performance.

**Lemma 3.** Let \( A \) and \( A + \Delta \) be positive definite matrices. Then, the following bounds hold:
\[
\log \det(A + \Delta) - \log \det(A) \leq tr(A^{-1} \Delta)
\]
\[
\log \det(A + \Delta) - \log \det(A) \geq tr((A + \Delta)^{-1} - A^{-1})
\]
We will need a technical lemma that yields an asymptotic lower bound to a remainder term that will be crucial for proving the main result of the paper (Theorem 3).

**Lemma 4.** Consider the transmitter and receiver strategies described in Section IV. Assume the same conditions as in Theorem 1. In addition, assume (14). Define the auxiliary variable \( \beta(P) \) as:
\[
\beta(P) = \log \det \left( \rho P \rho^* V^* H_d W_{1,Q} W_{1,Q}^* H_d^* V G \right.
\]
\[
+ \left. (1 - \rho) \frac{P}{n_t - n_r} G^* V^* H_d W_2 Q W_2^* H_d^* V G + \sigma^2 G^* G \right)
\]
\[
- \log \det \left( \rho P G^* V^* H_d W_{1,Q} W_{1,Q}^* H_d^* V G + \sigma^2 G^* G \right)
\]
Then, there exists a non-negative sequence \( \{\epsilon(P)\} \) converging to zero such that for all \( P \):
\[
\beta(P) \geq -\epsilon(P)
\]

**Proof:** See Appendix D.

The main result of the paper is provided in Theorem 2 where the optimal SDoF is shown to be obtained under the quantized feedback of CSI. In addition, it is shown that there is no secrecy rate loss due to quantization asymptotically as \( P \to \infty \).

**Theorem 2.** Consider the transmitter and receiver strategies described in Section IV. Assume the same conditions as in Theorem 1

1) Assuming (14), i.e.,
\[
N_f = \frac{N}{2} \log_2 P
\]
then, the full \( d^2 \) SDoF are achievable.

2) Assuming for some \( \epsilon > 0 \),
\[
N_f = (1 + \epsilon) \frac{N}{2} \log_2 P
\]
then, the full \( d^2 \) SDoF are achievable and the asymptotic rate gap due to quantization \( \delta_{\text{GAP}} \) is zero.
\[ R^P_{s,G} = \log \left( \frac{\det(\rho \mathbf{G}^* \mathbf{V}^* \mathbf{H}_a \mathbf{W}_1 \mathbf{K}_x \mathbf{W}_1^* \mathbf{H}_c^* \mathbf{V} G + \sigma^2 \mathbf{G}^* \mathbf{G})}{\det(\sigma^2 \mathbf{G}^* \mathbf{G})} \right) - \log \left( \frac{\det(\rho \mathbf{H}_c \mathbf{W}_1 \mathbf{K}_x \mathbf{W}_1^* \mathbf{H}_c^* + \frac{(1-\rho)\rho}{n_t-n_r} \mathbf{H}_c \mathbf{W}_2 \mathbf{W}_2^* \mathbf{H}_c^* + \sigma^2 \mathbf{I}_{n_c})}{\det(\frac{(1-\rho)\rho}{n_t-n_r} \mathbf{H}_c \mathbf{W}_2 \mathbf{W}_2^* \mathbf{H}_c^* + \sigma^2 \mathbf{I}_{n_c})} \right) \]

\[ R^Q_{s,G} = \log \left( \frac{\det(\rho \mathbf{G}^* \mathbf{V}^* \mathbf{H}_a \mathbf{W}_1 \mathbf{K}_x \mathbf{W}_1^* \mathbf{H}_c^* + \frac{(1-\rho)\rho}{n_t-n_r} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_a \mathbf{W}_2 \mathbf{W}_2^* \mathbf{H}_c^* \mathbf{V} G + \sigma^2 \mathbf{G}^* \mathbf{G})}{\det(\frac{(1-\rho)\rho}{n_t-n_r} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_a \mathbf{W}_2 \mathbf{W}_2^* \mathbf{H}_c^* \mathbf{V} G + \sigma^2 \mathbf{G}^* \mathbf{G})} \right) - \log \left( \frac{\det(\rho \mathbf{H}_c \mathbf{W}_1 \mathbf{K}_x \mathbf{W}_1^* \mathbf{H}_c^* + \frac{(1-\rho)\rho}{n_t-n_r} \mathbf{H}_c \mathbf{W}_2 \mathbf{W}_2^* \mathbf{H}_c^* + \sigma^2 \mathbf{I}_{n_c})}{\det(\frac{(1-\rho)\rho}{n_t-n_r} \mathbf{H}_c \mathbf{W}_2 \mathbf{W}_2^* \mathbf{H}_c^* + \sigma^2 \mathbf{I}_{n_c})} \right) \]

\[ U(P) = P \cdot \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_2 \mathbf{Q} \mathbf{W}_2^* \mathbf{H}_d^* \mathbf{V} G \to 0 \]

which implies that \( \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_2 \mathbf{Q} \mathbf{W}_2^* \mathbf{H}_d^* \mathbf{V} G = o(1) \). The condition \( N_f \to \infty \) alone only implies \( \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_2 \mathbf{Q} \mathbf{W}_2^* \mathbf{H}_d^* \mathbf{V} G = o(1) \) and does not guarantee \( U(P) \to 0 \). Necessary conditions that guarantee the results of Theorem 2 remain an open problem.

**V. Simulations**

This section contains a few illustrative simulations that validate the methodology presented throughout the paper. The elements of all channels were generated as i.i.d. random complex-normal \( \mathcal{N}(0,1) \) random variables as in [9], [10].

Figure 2 shows the secrecy rate performance as a function of transmit SNR for \( n_r = 2, 3, 4 \) where \( n_t = 1 \) and \( n_t = 2n_r, n_e = n_t - n_r = n_r \). The feedback bit rate increases as a function of \( P \) according to (14) for the left panel and according to (17) for the right panel. The secrecy rate for the perfect CSI and quantized CSI schemes were calculated using the expressions in (15) and (16) with the choices \( \mathbf{K}_x = \rho \mathbf{I}_{n_r} \) and \( \mathbf{K}_{x,n} = \frac{(1-\rho)\rho}{n_t-n_r} \mathbf{I}_{n_r-n_e} \). Due to the high complexity associated with implementing (9) for large bit rates \( N_f \), we adopt the random perturbation scheme of (10) to generate the quantized matrices \( \mathbf{F}^\mathcal{Q} \). It was shown numerically in [10] that this approximation is fairly accurate for a wide range of SNR. It is evident from Figure 2 that the slopes of the secrecy rate curves become identical as SNR grows, implying that the SDoF become identical, as expected from Theorem 2.

In addition, for \( N_f = \frac{(1+\epsilon)N}{2} \log_2 P \) with \( \epsilon = 0.5 \), the right panel of Figure 2 shows that the secrecy rate gap converges to zero as \( P \) grows to infinity.

Figure 3 shows the secrecy rate performance as a function of \( N_r = 3 \) where \( n_t = 2n_r \) and \( n_e = n_t - n_r \). The feedback bit rate is fixed to \( N_f = 30, 60, 90 \) and it is observed that the secrecy rate converges to a limiting value as the transmit SNR grows to infinity. Similar behavior is observed for the communication rate performance with finite rate feedback without secrecy or jamming in [9], [10], [7], [8] and without jamming in [14]. This phenomenon is due to the fact that finite quantization bit rate allows the artificial noise to dominate at the receiver and as a result, the secure multiplexing gain becomes zero.

Figure 4 shows the loss in secrecy rate due to quantization, for fixed SNR and number of antennas, as a function of number of feedback bits \( N_f \). The SNR is fixed to \( SNR = 10, 20, 30 \) dB and we observe that the secrecy rate loss converges to zero fast as \( N_f \) grows. We conjecture that this rate gap converges to zero exponentially fast as a function of \( N_f \).

**VI. Conclusion**

We studied the value of quantized feedback for MIMO secrecy communications in the presence of a jammer. We proposed transmitter and receiver strategies based on linear precoding and receive beamforming to simultaneously combat jammer interference, imperfect CSI at the transmitter and eavesdropping. Under this MIMO communication model, we characterized the achievable secrecy rate performance of the system. We derived sufficient conditions on the feedback bit rate scaling as a function of transmit power that guarantees the same secure degrees-of-freedom as the corresponding scheme with perfect CSI. We also showed that there is no secrecy rate loss due to quantization asymptotically as \( P \to \infty \) under
the same conditions. Simulations were shown to validate the theoretical analysis.

Future work may include deriving necessary conditions on the feedback bit rate to maintain the optimal secure degrees-of-freedom and developing efficient power allocations algorithms to improve performance in the low SNR regime. Another worthwhile open problem is to bound the secrecy rate gap as a function of finite power $P$ and number of feedback bits $N_f$. This type of analysis would provide insight into how many feedback bits are needed to achieve an arbitrarily small secrecy rate gap.

ACKNOWLEDGMENT

The author gratefully acknowledges discussions with David Browne and Keith W. Forsythe.

APPENDIX A
PROOF OF THEOREM 2

Proof: Decompose $R_s$ into two components $R_s = R_s^d - R_s^E$ where

$$R_s^d = \log \left( \frac{\det(\rho H_{e,s} K_{x,s} H_{e,s}^* + \frac{(1-\rho)P}{n_t-n_r} H_{e,an} H_{e,an}^* + \sigma^2 I)}{\det(\frac{(1-\rho)P}{n_t-n_r} H_{e,an} H_{e,an}^* + \sigma^2 I)} \right)$$

$$R_s^E = \log \left( \frac{\det(\rho H_{e,s} K_{x,s} H_{e,s}^* + \frac{(1-\rho)P}{n_t-n_r} H_{e,an} H_{e,an}^* + \sigma^2 I)}{\det(\frac{(1-\rho)P}{n_t-n_r} H_{e,an} H_{e,an}^* + \sigma^2 I)} \right)$$

Expanding $R_s^d$, we obtain:

$$R_s^d = \sum_{i=1}^{n_r-n_j} \log \left( 1 + \frac{\rho}{\sigma^2} \lambda_i(HK_{x,s} H^*) \right) = d_s \log(P) + \sum_{i=1}^{d_s} \log \left( P^{1-\frac{\rho}{\sigma^2}} \frac{\lambda_i(HK_{x,s} H^*)}{P} \right)$$

(18)

Using (7), it is guaranteed that all eigenvalues $\lambda_i(HK_{x,s} H^*)$ satisfy the bounds:

$$c_0 \rho \lambda_i(HH^*) \leq \lambda_i(HK_{x,s} H^*) \leq c_1 \rho \lambda_i(HH^*)$$

(19)

Since the matrix $HH^*$ is positive definite almost surely, using (19) into (18) and taking the limit as $P \rightarrow \infty$, we obtain

$$\lim_{P \rightarrow \infty} \frac{\log(P)}{R_s^E} = d_s \log(P) \rightarrow 0.$$ To prove this, note that $R_s^E$ converges to a constant as $P \rightarrow \infty$:

$$R_s^E = \log \left( I + \rho H_{e,s} K_{x,s} H_{e,s}^* \left( \frac{(1-\rho)PH_{e,an} H_{e,an}^* + \sigma^2 I}{n_t-n_r} \right)^{-1} \right)$$

$$\leq \log \left( I + c_1 \rho PH_{e,s} H_{e,s}^* \left( \frac{(1-\rho)PH_{e,an} H_{e,an}^* + \sigma^2 I}{n_t-n_r} \right)^{-1} \right)$$

$$= \log \left( I + c_1 \rho H_{e,s} H_{e,s}^* \left( \frac{(1-\rho)H_{e,an} H_{e,an}^* + \sigma^2 P^{-1} I}{n_t-n_r} \right)^{-1} \right)$$

$$= \log \left( I + c_1 \rho \frac{(n_t-n_r)}{1-\rho} H_{e,s} H_{e,s}^* \left( H_{e,an} H_{e,an}^* \right)^{-1} \right)$$

$$\rightarrow \infty$$
Fig. 3: Monte Carlo simulation for secrecy rate loss due to quantization as a function of SNR for $N_f = 30, 60, 90$. The transmitter has $n_t = 2n_r$ antennas and the receiver has $n_r = 3$ antennas. The jammer and the eavesdropper are both equipped with one antenna, i.e., $n_j = n_e = 1$. Equal power allocation $\rho = 1/2$ was used. The secrecy rate saturates to a limiting value as SNR grows, implying zero SDoF gain.

Fig. 4: Monte Carlo simulation for secrecy rate loss due to quantization as a function of $N_f$ for fixed SNR. The transmitter has $n_t = 2n_r$ antennas and the receiver has $n_r = 3$ antennas. The jammer has $n_j = 1$ antenna and the eavesdropper has $n_e = n_t - n_r = 2$ antennas. Equal power allocation $\rho = 1/2$ was used. The secrecy rate gap converges to zero fast as the number of feedback bits increase.

Note that we used the fact that $n_e \leq n_t - n_r$, implying that $H_{e,an}H_{e,an}^\dagger$ is full rank. Using a similar argument and (7) again, it follows that $R_x^E$ is bounded below by a constant as $P \to \infty$ as well. Thus, $R_x^E/\log(P) \to 0$ and the proof is complete.

**APPENDIX B**

**PROOF OF LEMMA 1**

Proof: The transmitter has access to $\hat{F}$, a quantized version of $F$, which is obtained using (9). The transmitter designs $W_{2,Q}$ such that $\hat{F}\hat{W}_{2,Q} = 0$ (recall (10)). Letting $\hat{M} = \hat{F}U$, we also have $\hat{M}\hat{W}_{2,Q} = 0$. Using this, we obtain:

$$G^*V^*H_dW_{2,Q} = G^*V^*C^*F^*W_{2,Q}$$

$$= B^*F(CV^*C^*)^{-1}(CV)^*F^*W_{2,Q}$$

Consider the square invertible positive definite matrix

$$P = CV(CV^*C^*)^{-1}(CV)^*$$

This matrix can be seen as a projection onto the column space of $CV$. Write the eigendecomposition of $P$ as $UAU^\dagger$. Then, continuing:

$$G^*V^*H_dW_{2,Q} = B^*FPF^*W_{2,Q}$$

$$= B^*FUAU^\dagger F^*W_{2,Q}$$

$$= B^*MAM^*W_{2,Q} - B^*MM^*W_{2,Q}$$

$$= B^*(MAM^* - MM^*)W_{2,Q}$$

The leakage power can then be bounded as:

$$L = E\|\sqrt{1 - \rho}G^*V^*H_dW_{2,Q}X_{an}\|_2^2$$

$$\leq (1 - \rho)E\|X_{an}\|_2^2 \|G^*V^*H_dW_{2,Q}\|_F^2$$

$$= (1 - \rho)P \frac{n_t - n_r}{n_t} \|B^*(MAM^* - MM^*)W_{2,Q}\|_F^2$$

$$\leq (1 - \rho)P \frac{n_t - n_r}{n_t} \|B^*\|_F^2 \|MAM^* - MM^*\|_F^2 \|W_{2,Q}\|_2^2$$

$$= (1 - \rho)P \frac{n_t - n_r}{n_t} \|MAM^* - MM^*\|_F^2$$

where we used the fact that $\|B^*\|_F = \|W_{2,Q}\|_2 = 1$ since they are truncated unitary matrices.

Since $P$ is a projection matrix, it follows its eigenvalues $[\Lambda]_{i,i}$ are either 1 or 0. As a result, we have:

$$\|MAM^*\|_F^2 \leq \|MM^*\|_F^2$$

(23)

and since $I - M = D$ consists of zeros or ones on the diagonal, we also have:

$$\text{tr}(\hat{M}^*M(I - \Lambda)(\hat{M}^*M)^*) = \text{tr}(\hat{M}^*M)(I - \hat{M}^*M)$$

$$= \sum_i [D_{i,i}]_{i,i} = 0$$

Using (23) and (24), we obtain:

$$\|MAM^* - MM^*\|_F^2 \leq \|MM^* - MM^*\|_F^2$$

(25)

Using the bound (25) in (22), we obtain:

$$L \leq (1 - \rho)P \frac{n_t - n_r}{n_t} \|MM^* - MM^*\|_F^2$$

$$= (1 - \rho)P \frac{n_t - n_r}{n_t} \|FF^* - \hat{F}\hat{F}^*\|_F^2$$

$$= 2(1 - \rho)P \frac{n_t - n_r}{n_t} d_e(F, \hat{F})^2$$

(26)
where we used $U U^* = I_n$, and the definition of the chordal distance.

Assuming a sphere-packing codebook construction, Thm. 5 in [20] yields a bound on the maximum quantization error:

$$
\max_{F \in G_{n_t,n_r}} d_c(F, \hat{F}) \leq \frac{2}{(e \sqrt{N_f})^{1/4}} (1 + o(2^{-N_f})) \tag{27}
$$

where $\hat{F}$ is obtained using [9] and $c$ is the coefficient of the ball volume in $G_{n_t,n_r}$. Using the quantization error bound [27] in [26], we obtain the desired bound in [13].

**APPENDIX C**

**PROOF OF COROLLARY**

Proof: With the choice $N_f = N/2 \log_2 P$, Lemma [1] implies

$$
L \leq \frac{2(1-\rho)P}{nt - nr} \frac{4/c^2}{P} (1 + o(P^{-1/2}))
$$

$$
P \to \infty \quad \frac{8(1-\rho)/c^2}{nt - nr}
$$

The proof is complete.

**APPENDIX D**

**PROOF OF LEMMA**

Proof: We want to show that $\beta(P)$ is positive asymptotically as $P \to \infty$. Define the matrices

$$
M_1(P) = \rho P G^* V H_d W_1 W_1^T H_d^* VG
$$

$$
M_2(P) = (1 - \rho) P \frac{n_t - n_r}{nt - nr} G^* V H_d W_2, q W_2^* H_d^* VG
$$

$$
A(P) = M_1(P) + M_2(P) + \sigma^2 G^* G
$$

$$
\Gamma(P) = W_{1,q} W_{1,q}^* - W_1 W_1^*
$$

$$
Z = G^* V H_d
$$

and the scalar $\delta = \rho P$. Then, we can write:

$$
\beta(P) = \log \det (A(P) + \delta(P) Z \Gamma(P) Z^*) - \log \det (A(P)).
$$

Recall the choice $W_{1,q} = \hat{F}$ and $W_1 = F$. Thus, the matrix $\Gamma(P)$ can be rewritten as:

$$
\Gamma(P) = \hat{F} \hat{F}^* - FF^*
$$

If $\hat{F} \hat{F}^* \preceq FF^*$, then it follows that $\beta(P) \geq 0$ for all $P$, but there is not necessarily true in general. Instead, we show $\beta(P) \geq 0$ for large $P$. Using the perturbation Lemma [3] with $\Delta(P) = \delta(P) Z \Gamma(P) Z^*$, we obtain

$$
\beta(P) \geq \operatorname{tr}(\Delta(P)(A(P) + \Delta(P))^{-1}) \log(e)
$$

$$
\geq -\|\Delta(P)\|_F \| (A(P) + \Delta(P))^{-1} \|_F \log(e) \tag{28}
$$

The constant $c$ is given by [21]:

$$
c = \frac{1}{(nt - nr)!} \prod_{i=1}^{nt} \frac{(nt - i)!}{(nr - i)!}
$$

We conclude the proof by showing that $\|\Delta(P)\|_F \| (A(P) + \Delta(P))^{-1} \|_F = o(1)$ as $P \to \infty$. To this end, first note the bounds:

$$
\|\Delta(P)\|_F = \delta(P) \| Z \Gamma(P) Z^* \|_F
$$

$$
\leq \delta(P) \| Z \|_F^2 \| \Gamma(P) \|_F
$$

$$
= \sqrt{2\rho P} \| Z \|_F^2 \| F, \hat{F} \|_F
$$

$$
\leq \sqrt{2P} \| Z \|_F^2 (2 - N_f/N) \frac{n_t - n_r}{c N_f^{1/2}} (1 + o(2^{-N_f/N}))\]

$$
\| \Delta(P) \|_F \| (A(P) + \Delta(P))^{-1} \|_F = o(1) \quad \text{as } P \to \infty
$$

(30)

where we used the upper bound [27] on the chordal distance in [29]. Next, consider the positive semidefinite matrix $M_2(P)$. Using the bounds in the proof of Lemma [1] (see [21]), it follows that:

$$
\operatorname{tr}(M_2(P))
$$

$$
= \frac{(1 - \rho) P}{n_t - n_r} \operatorname{tr}(G^* V H_d W_2, q W_2^* H_d^* VG)
$$

$$
= \frac{(1 - \rho) P}{n_t - n_r} \| G^* V H_d W_2, q \|_F^2
$$

$$
\leq \frac{2(1 - \rho) P}{n_t - n_r} d_c(F, \hat{F})^2
$$

$$
\leq \frac{4(1 - \rho) P}{e^{2N_f(n_t - n_r)} (1 + o(2^{-N_f/N})^2 (1 + o(P^{-1/2})}
$$

$$
= O(1) \quad \text{as } P \to \infty
$$

(31)

On the other hand, the sequence of matrices $M_2(P)$ converges to infinity as $P \to \infty$ since $M_1(P) = \rho P K_{const}$ for some constant strictly positive definite matrix $K_{const}$. Thus, we have:

$$
\| (A(P) + \Delta(P))^{-1} \|_F
$$

$$
= \| \left( \rho P K_{const} + M_2(P) + \sigma^2 G^* G + \Delta(P) \right)^{-1} \|_F
$$

$$
= P^{-1} \left\| \left( \rho K_{const} + \left\{ M_2(P) + \sigma^2 G^* G + \Delta(P) \right\} \right)^{-1} \right\|_F \tag{32}
$$

Next, we notice that the term in the brackets above is $O(P^{-1/2})$ since $G$ is independent of $P$ and from [31] and [30]:

$$
\operatorname{tr} \left( \frac{M_2(P)}{P} \right) = O(P^{-1})
$$

$$
\| \Delta(P) \|_F = O(P^{-1/2})
$$

(32)

Since the trace of the sequence of positive semidefinite matrices $\{M_2(P)\}$ tends to zero, the sequence of the matrices must

4In fact, the matrix $K_{const}$ can be shown to be

$$
K_{const} = G^* V C^* CVG = B^* M A M^* B
$$

where we used the definition of $G$ from [12], $M = FU$, the eigendecomposition of $P$ from [20] and the QR decomposition $H_2^* = FC$. 


converge to zero as well at the same rate \[ [22]. \] Substituting these back into \[ (32) \text{, we obtain:} \]
\[
\|\Delta\|_F \left\| (A(P) + \Delta(P))^{-1} \right\|_F \\
= O(\sqrt{\frac{1}{T} P^{-1}} \left\| \rho K_{\text{const}} + O(P^{-1/2}) I \right\|_F^{-1} ) \\
= O(P^{-1/2}) = o(1)
\]
We thus conclude from \[ (33) \] and the lower bound \[ (28) \] that choosing \( \epsilon(P) = \|\Delta(P)\|_F \|\| (A(P) + \Delta(P))^{-1} \|_F \log(e) \) yields the desired lower bound since \( \epsilon(P) \) converges to zero and \( \beta(P) \geq -\epsilon(P) \). The proof is complete. \]

**APPENDIX E**

**PROOF OF THEOREM 2**

**Proof:** Let \( R_{s,G}^P \) denote the achievable rate assuming perfect CSI and \( R_{s,G}^Q \) denote the achievable rate under the quantized CSI communication scheme.

The first part of the Theorem will be proven first. With perfect CSI, a similar argument as the one presented in Theorem \[ 1 \] can be used to show:
\[
\frac{R_{s,G}^P}{\log P} \rightarrow d_s (34)
\]
Of course, the fact that \( G^* G \) is full rank (a.s.) is also used.

Define the secrecy rate difference:
\[
\Delta R_{s,G} := R_{s,G}^P - R_{s,G}^Q = T_P^P - T_P^Q + T_Q^P + T_Q^Q (35)
\]
where the terms \( T_P^P, T_P^Q, T_Q^P, T_Q^Q \) are defined in \[ (15) \] and \[ (16) \].

We note that the term \( -T_P^P + T_Q^Q \) is asymptotically negligible since \( -T_P^P + T_Q^Q = o(1) \) as \( P \rightarrow \infty \). To see this, note:
\[
T_P^P = \log \det \left( I + \frac{\rho}{\rho} \frac{H_e W_1 W_1^* H_e^*}{n_t - n_r} \right) \\
\times \left( \frac{1 - \rho}{n_t - n_r} H_e W_2 W_2^* H_e^* + \frac{\sigma^2}{P} I_{n_e} \right)^{-1} \\
= \log \det \left( I + \frac{\rho}{1 - \rho} \frac{n_t}{n_t - n_r} H_e W_1 W_1^* H_e^* \\
\times (H_e W_2 W_2^* H_e^*)^{-1} \right) =: t_\infty
\]
where we used the condition \( n_e \leq n_t - n_r \), implying that \( H_e W_2 W_2^* H_e^* \) is invertible. Using the fact that \( \lim_{P \rightarrow \infty} N_f = \infty \), it follows that \( W_1, Q \rightarrow W_1 \) and \( W_2, Q \rightarrow W_2 \) as the loss due to quantization becomes asymptotically negligible. Therefore, using a similar technique and taking the limit as \( P \rightarrow \infty \), it follows that \( T_Q^Q \rightarrow t_\infty \). Thus, we have \( -T_P^P + T_Q^Q \rightarrow -t_\infty + t_\infty = 0 \). Using this in \[ (35) \], we obtain:
\[
\Delta R_{s,G} = T_P^P - T_Q^Q + o(1) (36)
\]
Without loss of generality, let us assume \( K_{x_s} \sim c P I \) for the purposes of analysis since \( c_0 P I \leq K_{x_s} \leq c_1 P I \). Using the definitions of \( T_P^P \) and \( T_Q^Q \), after some algebra, we obtain:
\[
\Delta R_{s,G} \sim \log \det \left( \frac{(1 - \rho) P}{n_t - n_r} G^* V^* H_d W_{1,Q} W_{1,Q}^* H_d^* V G + \sigma^2 G^* G \right) \\
- \log \det (\sigma^2 G^* G) \\
- \left[ \log \det \left( \frac{P}{n_t - n_r} G^* V^* H_d W_{1,Q} W_{1,Q}^* H_d^* V G + \sigma^2 G^* G \right) \\
+ (1 - \rho) \frac{P}{n_t - n_r} G^* V^* H_d W_{2,Q} W_{2,Q}^* H_d^* V G + \sigma^2 G^* G \right] \\
- \log \det (\rho P G^* V^* H_d W_{1,Q} W_{1,Q}^* H_d^* V G + \sigma^2 G^* G) \right] + o(1)
\]
The term in the brackets is exactly the remainder term \( \beta(P) \) defined in Lemma \[ 4 \]. Using the result of Lemma \[ 4 \], there exists a sequence \( \epsilon(P) \) converging to zero such that:
\[
\Delta R_{s,G} \sim \log \det \left( \frac{M_2(P)}{\sigma^2} + \sigma^2 G^* G \right) \\
- \log \det (\sigma^2 G^* G) - \beta(P) + o(1)
\]
\[
\leq d_s \log \left( \frac{M_2(P)}{\sigma^2} + \sigma^2 G^* G \right) + \epsilon(P) + o(1)
\]
\[
\leq d_s \log \left( \frac{\lambda_{\max}(G^* G)}{\lambda_{\min}(G^* G)} + \|M_2(P)\|_2 \right) + \epsilon(P) + o(1)
\]
\[
\leq d_s \log \left( \frac{\kappa(G^* G)}{\sigma^2 \lambda_{\min}(G^* G)} \right) + \epsilon(P) + o(1)
\]
The term given by \( P \|G^* V^* H_d W_{2,Q}^*\|_F \) is \( O(1) \) as \( P \rightarrow \infty \), as the bounds in \[ (31) \] show. Thus, dividing both sides of \[ (37) \] by \( \log P \) and taking the limit as \( P \rightarrow \infty \), we obtain:
\[
d_s := \lim_{P \rightarrow \infty} \frac{R_{s,G}^Q}{\log P} \\
\geq \lim_{P \rightarrow \infty} \frac{R_{s,G}^Q}{\log P} - \lim_{P \rightarrow \infty} \frac{d_s \log(\kappa(G^* G) + O(1)) + \epsilon(P) + o(1)}{\log P}
\]
where we used \[ (34) \]. Since the rate of the quantized CSI scheme is less than the rate of the perfect CSI scheme, it follows that \( d_s^Q \leq d_s \). Thus, we conclude that \( d_s^Q = d_s \).

The second part of the Theorem now easily follows. Note that from \[ (36) \], we have:
\[
\delta_{\text{GAP}} = \lim_{P \rightarrow \infty} \{ R_{s,G}^P - R_{s,G}^Q \} \\
= \lim_{P \rightarrow \infty} \{ T_P^P - T_Q^Q \} \\
\leq \lim_{P \rightarrow \infty} \log \det \left( I + \frac{1 - \rho}{\sigma^2} U(P)(G^* G)^{-1} \right)
\]
where
\[
U(P) := PG^* V^* H_d W_{2,Q} W_{2,Q}^* H_d^* V G
\]
is a positive semidefinite matrix depending on \( P \). From the development in (31), using the scaling in (17), we obtain:

\[
\text{tr}(U(P)) = P\|G^*V^*H_d W_{2,q}\|^2_F \\
\leq 2Pd_c(F, \hat{F})^2 \\
\leq \frac{8P}{C^2/Nc^2} 2^{-2N_f/N(1 + o(2^{-N_f}))} N_f = O(P^{-\epsilon})
\]

As a result, \( \text{tr}(U(P)) = o(1) \), implying \( U(P) \to 0 \) as \( P \to \infty \). Using this result in (38), we have \( \delta_{\text{GAP}} \leq 0 \). The final result following by noting that \( \delta_{\text{GAP}} \) is always nonnegative. The proof is complete.

---

**References**


