Performance Analysis of Linear Precoding for Secure Multiuser MIMO Systems With a Multiple-Antenna Eavesdropper

Hao Deng†‡, Hui-Ming Wang†, Chaowen Liu†, and Wenjie Wang†
†School of Electronic and Information Engineering, Xi’an Jiaotong University
‡Ministry of Education Key Lab for Intelligent Networks and Network Security, Xi’an Jiaotong University
Xi’an, 710049, Shaanxi, P. R. China. Email: xjbswhm@gmail.com
‡School of Physics and Electronics, Henan University
Kaifeng, 475004, Henan, P. R. China. Email: gavind@163.com

Abstract—In this paper, we investigate the secrecy performance of matched-filter (MF) and zero-forcing (ZF) precoding in a multi-user massive multiple-input multiple-output (MIMO) system with a multi-antenna passive eavesdropper. For the two precoding schemes, we find that the equivalent wiretap channels are similar and thus the eavesdropper achieves the approximate same sum-rate. Closed-form expressions of ergodic secrecy sum-rate (ESSR) are derived for the both schemes in the low and high signal-to-noise ratio (SNR) regimes. We show that a positive ESSR of MF scheme may be not achieved when the BS simultaneously serves more than two users with high transmit power, while the ESSR of ZF scheme always grows with the number of the served users. On the contrast, MF scheme is better than ZF scheme in the low SNR regime. Simulation results corroborate the analytic results.

I. INTRODUCTION

The security is a critical and challenging issue in the multiuser MIMO networks due to the broadcast nature of broadcast channel. Physical layer security, which exploits the characteristics of wireless channels for guaranteeing security [1], has been widely studied. A main motivation for physical-layer security is that the main channel and wiretap channel are generally different. In the existing studies, several signal processing techniques are proposed to yield large differences between the signal quality at the destination and that at the eavesdropper so that the security is guaranteed [2]-[14]. In particular, secrecy beamforming and precoding schemes which have the ability to exploit the spatial degrees of freedom are introduced to MIMO systems. When only partial knowledge of the eavesdroppers channel is available, artificial noise (AN) or jamming signals is also introduced as a effective way to further degrade the eavesdroppers channel.

Recently, multi-user multiple-input multiple-output (MU-MIMO) systems with very large antenna arrays at the BS have received considerable attention [15]-[16]. Such systems are usually referred to massive MIMO, very large antenna arrays mean that the BS equips with tens to hundreds of antennas. For regular MIMO systems without secrecy consideration, the sum-capacity of multi-user MIMO downlink is achieved by using dirty paper coding [17], it requires high implementation complexity. However, with an increase in the number of the BS antennas, linear precoding schemes, such as matched-filter (MF) and zero-forcing (ZF), are shown to be effective in controlling interuser interference and near-optimal [18].

Motivated by this, this paper studies the secrecy performance of MF and ZF precoding in a multiuser massive MIMO system with a multi-antenna passive eavesdropper. We note that the system model studied in this paper is different from the one adopted in [10], where multiple single-antenna users cooperate and jointly eavesdrop on other users. The authors investigated performance of the MF and ZF precoding schemes assisted by AN in [11]-[12]. As shown in [19], [20], and [21], a common observation is that in low SNR regime, AN scheme does not always improve the security. Moreover, the advantage of MF precoding lies in its near-optimal and low complexity, and thus AN assisted MF precoding is not a good choice to improve security for a large transmit antennas case. Hence, we only consider the simple MF and ZF precoding schemes and give explicitly performance analysis in both low and high SNR regime.

II. SYSTEM MODEL

In the multiuser massive MIMO system, a basestation (BS) composed of $N_b$ antennas transmits information to $K$ mobile users, each with a single antenna, in the presence of a eavesdropper with $N_e$ antennas. Without loss of generality, we further assume that $N_b \gg N_e > K$. We also assume perfect CSIs to the users are available at the BS. This is can be accomplished by sending a pilot signal from each of the users. However, only distribution information of the wiretap channel is available. Under the flat fading channel assumption, the received signal at the $k$-th user and the eavesdropper can...
be given respectively as
\[ y_k = h_k^H x + n_k, \]
\[ y_e = G^H x + n_e, \]  
where \( h_k \in \mathbb{C}^{N_s \times 1} \) is the channel vector between the BS and the \( k \)-th served user, and \( G \in \mathbb{C}^{N_e \times N_s} \) represents the channel matrix between the BS and the eavesdropper, \( x \) is a \( N_t \times 1 \) vector of symbols transmitted by the BS with the power constraint \( \mathbb{E}[|X|^2] = P \), \( n_k \sim \mathcal{CN}(0, \sigma_n^2) \) and \( n_e \sim \mathcal{CN}(0, \sigma_e^2) \). The additive white, zero-mean Gaussian noises at the BS and the eavesdropper, respectively. For simplicity, we assume \( \sigma_n^2 = \sigma_e^2 \) and let \( \rho = P/\sigma_n^2 \). We adopt an uncorrelated Rayleigh fading channel and hence, the entries of \( h_k \) for \( k = 1, \ldots, K \) and \( G \) are independent identically distributed (i.i.d.) complex Gaussian random variables with zero mean and unit variance.

Let \( W = [w_1, w_K] \) be the \( N_t \times K \) precoding matrix, where \( w_k \) is the \( k \)-th column of \( W \). Then the transmitted signal vector at the BS is
\[ x = \sqrt{\frac{P}{\gamma}} W s, \]  
where \( \gamma = \text{tr}\{W^H W\} \) is employed to ensure the power transmit power constraint and \( s \) are the confidential messages. We assume that the entries of \( s \) are chosen independently, following with zero-mean and unit-variance Gaussian distribution.

Basic linear precoding schemes include MF, ZF. When MF is used, i.e., \( W = H \), where \( H = [h_1, \ldots, h_K] \), the transmitted signal from the BS can be expressed as
\[ x^{MF} = \sqrt{\frac{P}{\gamma^{MF}}} H s, \]
where \( \gamma^{MF} = \text{tr}\{H^H H\} = N_t K, \) as \( N_t \to \infty \).

When ZF is used, i.e., \( W = H(H^H H)^{-1} \), the transmitted signal from the BS can be expressed as
\[ x^{ZF} = \sqrt{\frac{P}{\gamma^{ZF}}} H (H^H H)^{-1} s, \]
where \( \gamma^{ZF} = \text{tr}\{(H^H H)^{-1}\} = \frac{K}{N_t}, \) as \( N_t \to \infty \).

### III. ACHIEVABLE SECRECY SUM-RATES

Since the instantaneous CSI of the eavesdropper is not available, instantaneous secrecy rate can not be obtained. Therefore, we use ergodic secrecy rate (ESR) as the performance metric, which is defined as
\[ R_s = \left\{ \mathbb{E}[C_d] - \mathbb{E}[C_e] \right\}^+, \]
where \( \{x\}^+ = \max(0, x) \), \( C_d \) and \( C_e \) are achievable rates at the legitimate users and the eavesdropper, respectively.

In the following, we investigate the ESR of the two proposed precoding schemes.

### A. MF Scheme

In the MF scheme, the received signal at the \( k \)-th user and the eavesdropper can be rewritten as
\[ y_k^{MF} = h_k^H x^{MF} + n_k, \]
\[ y_e^{MF} = G^H x^{MF} + n_e. \]

From (7), the signal-to-interference-plus-noise ratio (SINR) at the \( k \)-th intended user is
\[ \text{SINR}_k^{MF} = \frac{\lambda ||h_k||^4}{\gamma^{MF} + \rho \sum_{j \neq k} ||h_j||^4 ||h_j^H h_j||^2}. \]

The sum-rates achieved by the legitimate users and the eavesdropper are, respectively
\[ C_d^{MF} = \sum_{k=1}^K \log \left(1 + \text{SINR}_k^{MF}\right), \]
\[ C_e^{MF} = \log \det \left( I_{N_e} + \frac{\rho}{\gamma^{MF}} G^H H H^H G \right). \]

Then the ergodic secrecy sum-rate (ESSR) of MF scheme is given by
\[ \text{ESSR}_s^{MF} = \left\{ \mathbb{E}[C_d^{MF}] - \mathbb{E}[C_e^{MF}] \right\}^+. \]

The following lemmas will help in analysis.

**Lemma 1:** When \( N_t \) is large, the ergodic achievable sum-rate of the legitimate users can be lower bounded by
\[ \mathbb{E}[C_d^{MF}] \gtrsim K \log \left(1 + \rho(N_t - 1)(N_t - 2)/N_t(K + \rho(K - 1))\right). \]

**Proof:** Please see Appendix A.

**Lemma 2:** In the high SNR regime, i.e., \( \rho \to \infty \), when \( N_t \) is large, the ergodic achievable sum-rate of the eavesdropper can be given by
\[ \mathbb{E}[C_e^{MF}] = \sum_{i=1}^K \psi(N_e - i + 1) + K \log(K \rho), \]
where \( \psi(r) = \sum_{j=1}^{r-1} 1/j - \gamma \) is the digamma function and \( \gamma = 0.57721566 \cdots \) is the Euler-Mascheroni constant.
In the low SNR regime, i.e., $\rho \to 0$, when $N_t$ is large, the ergodic achievable sum-rate of the eavesdropper can be given by

$$\mathbb{E}[C_{e}^{MF}] = N_e \rho.$$  \hfill (15)

**Proof:** Please see Appendix B.

As can be seen from Appendix B, the wiretap channel is equivalent to a $K \times N_e$ MIMO channel. Obviously, the sum-rate achieved at the eavesdropper grows with $N_e$ and $K$ in the high SNR regime. However, sum-rate achieved in the low SNR regime do not rely on the number of the served users, that is, the sum-rate will approach to a constant with given $\rho$ and $N_e$.

**Theorem 1:** In the high SNR regime, when $N_t$ is large, the ESSR of MF scheme is approximately given as

$$R_s^{MF} \approx \log N_t - \psi(N_e), \ K = 1, \ \{\Phi(N_t, K, \rho) - \Psi(K, N_e)\}^+, K \geq 2.$$  \hfill (16)

where $\Phi(N_t, K, \rho) = K \log \frac{N_t}{\rho K (K-1)}$ and $\Psi(K, N_e) = \sum_{i=1}^{K} \psi(N_e - i + 1)$.

**Proof:** As $\rho \to \infty$, it holds that $K + \rho (K-1) \approx \rho (K-1)$ when $K \geq 2$. Therefore, we can rewrite (13) as

$$\mathbb{E}[C_{d}^{MF}] \geq K \log \left(1 + \frac{(N_t - 1)(N_t - 2)}{N_t (K - 1)}\right) \approx K \log \left(\frac{N_t}{K - 1}\right),$$  \hfill (17)

which implies that the achievable sum-rate of the legitimate users do not rely on the transmit power as $K \geq 2$. We first consider the case $K = 1$. In such case, we have

$$\mathbb{E}[C_{d}^{MF}] \geq \log \left(1 + \frac{\rho (N_t - 1)(N_t - 2)}{N_t}\right) \approx \log (N_t \rho).$$

Since $\psi(N_e) \leq \log (N_e - 1) + 1/(2 N_e) < \log N_t$, the ESSR of MF scheme for $K = 1$ can be given by

$$R_s^{MF} = \log N_t - \psi(N_e).$$  \hfill (18)

As for $K \geq 2$, the ESSR of MF scheme is given by

$$R_s^{MF} = \left\{K \log \left(\frac{N_t}{K(K-1) \rho}\right) - \sum_{i=1}^{K} \psi(N_e - i + 1)\right\}^+.$$  \hfill (19)

We complete the proof.

When $K = 1$, the MF scheme is equivalent to the ZF scheme, and thus the achievable ESSR of the two schemes are the same, which can be verified in Theorem 3. As for $K \geq 2$, positive secrecy sum-rate can be achieved at least when it holds that $N_t \geq \rho K (K - 1)$. Suppose that $\rho = 30 \text{ dB}$, then it needs to satisfy $N_t \geq 1000 K (K - 1)$, which is not unrealistic in practical systems. That is, MF schemes fails to simultaneously serve more than two users in the high SNR regime.

**Theorem 2:** In the low SNR regime, when $N_t$ is large, the ESSR of MF scheme is lower bounded by

$$R_s^{MF} \geq \left\{K \log \left(1 + \frac{\rho (N_t - 2)}{K}\right) - N_e \rho\right\}^+. \hfill (20)$$

**Proof:** Using the results in Lemma 1 and Lemma 2, we can easily obtain the result in Theorem 2.

Different from the behaviour in the high SNR regime, the ESSR of MF scheme grows with the number of served users in the low SNR regime. Based on Theorem 2, the relations between ESSR and $N_t$ as well as $N_e$ can be well investigated.

**B. ZF Scheme**

In the ZF scheme, the received signal at the $k$-th user and the eavesdropper can be rewritten as

$$y_k^{ZF} = h_k^H x_k^{ZF} + n_k,$$

$$y_e^{ZF} = G^H x_e^{ZF} + n_e,$$

$$= \sqrt{P \gamma_{ZF}} G^H \mathbf{H} (\mathbf{H}^H \mathbf{H})^{-1} s + n_e.$$  \hfill (21)

The sum-rates achieved by the legitimate users and the eavesdropper are, respectively

$$C_d^{ZF} = \sum_{k=1}^{K} \log \left(1 + \frac{P}{\gamma_{ZF}}\right)$$

$$= K \log \left(1 + \frac{N_t - K \rho}{K}\right),$$  \hfill (22)

$$C_e^{ZF} = \log \det \left(I_{N_e} + \frac{P}{\gamma_{ZF}} G^H \mathbf{H} (\mathbf{H}^H \mathbf{H})^{-1} G\right).$$  \hfill (23)

Similar as the MF scheme, we present the following Lemmas to characterize ESSR of the legitimate users and the eavesdropper.

**Lemma 3:** When $N_t$ is large, the ergodic achievable sum-rate of the legitimate users for ZF scheme is

$$\mathbb{E}[C_d^{ZF}] = K \log \left(1 + \frac{N_t - K \rho}{K}\right).$$  \hfill (24)

**Lemma 4:** In the high SNR regime, when $N_t$ is large, the ergodic achievable sum-rate of the eavesdropper for ZF scheme can be given by

$$\mathbb{E}[C_e^{ZF}] = \sum_{i=1}^{K} \psi(N_e - i + 1) + K \log \frac{(N_t - K) \rho}{N_t K}. \hfill (25)$$

In the low SNR regime, i.e., $\rho \to 0$, when $N_t$ is large, the ergodic achievable sum-rate of the eavesdropper can be given by

$$\mathbb{E}[C_e^{MF}] = \frac{(N_t - K) N_e \rho}{N_t}. \hfill (26)$$
Proof: Since $N_t$ is large, then from the law of large numbers, it holds that
\[ \mathbf{H}^H \mathbf{H} \approx N_t \mathbf{I}_{N_t}. \] (27)

Then we have
\[
\mathbb{E}[C_e^{ZF}] = \mathbb{E}
\left[
\log \det \left( \mathbf{I}_{N_e} + \frac{\rho}{N_t^2 \gamma_{ZF}} \mathbf{G}^H \mathbf{H}^H \mathbf{G} \right) \right]
= \mathbb{E}
\left[
\log \det \left( \mathbf{I}_{N_e} + \frac{(N_t - K)\rho}{N_t K} \mathbf{B}^H \mathbf{B} \right) \right]. \tag{28}
\]

Similar as the proof of Lemma 2, we can further have
\[
\mathbb{E}[C_e^{ZF}] = \sum_{i=1}^{K} \psi(N_e - i + 1) + K \log \left( \frac{(N_t - K)\rho}{N_t K} \right), \tag{29}
\]
\[
\lim_{\rho \to \infty} \mathbb{E}[C_e^{ZF}] = \frac{(N_t - K)N_e\rho}{N_t}, \tag{30}
\]

We complete the proof. 

It is interesting that the equivalent channel of the eavesdropper in ZF scheme is similar with that in MF scheme, but with different transmit power per user.

**Theorem 3:** In the high SNR regime, i.e., it holds that $\rho \to \infty$, when $N_t$ is large, the ESSR of ZF scheme is given by
\[ R_s^{ZF} = K \log N_t - \sum_{i=1}^{K} \psi(N_e - i + 1). \] (31)

Proof: Using the results in Lemma 3 and 4, we can easily obtain the result in Theorem 3.

Theorem 3 shows that the ESSR of ZF scheme grows with $N_t$ and $K$. While in MF scheme, positive secrecy rate may be achieved when only one user is served. We should note that the ESSR do rely on the transmit power, implying that increasing power can not improve the secrecy performance in the high SNR regime.

**Theorem 4:** In the low SNR regime, when $N_t$ is large, the ESSR of ZF scheme is given by
\[ R_s^{ZF} = \left\{ K \log \left( 1 + \frac{\rho(N_t - K)}{K} \right) - \frac{(N_t - K)N_e\rho}{N_t} \right\}^+. \] (32)

By observing Theorem 2 and theorem 4, we can find that MF outperforms ZF in the low SNR regime. This is not surprised, similar behaviour has been shown in the communication scenario without secrecy considerations [16].

**IV. SIMULATIONS**

So far, we have presented closed-form ESSR of the proposed schemes. In this section, simulation results are provided to verify the accuracy of the derived theoretical results. In all the simulations, all the users were assumed to have the same average SNR and experience independent Rayleigh fading. We fix the parameters as: $N_t = 40$ and $N_e = 10$. We perform Monte Carlo experiments consisting of 10000 independent trials to obtain the average results.

Fig. 1 plots the approximations of ergodic sum-rate of the eavesdropper in Lemma 2 and the corresponding numerical results for the high SNR case, where we let $\rho = 30dB$. While Fig. 2 plots the low SNR case and the SNR is fixed as $\rho = -20dB$. It is seen that the analytical results are quite consistent with the simulation results. In the both low and high SNR case, we can see that the ergodic sun-rates for the MF and ZF schemes are not exactly the same but very close, implying that the eavesdropper channels of the two schemes indeed share the similar equivalent channel. Meanwhile, we can also see that the ergodic sum-rate grows with the number of the served users for the high SNR case, while it is almost a constant for the low SNR case.

To illustrate our analytical results in Theorem 1 and Theorem 3, we plot the approximations of ESSR and the corresponding numerical results in Fig. 3 for the high SNR case where $\rho = 30dB$. It can be seen that the ESSR of ZF scheme grows with the number of the served users while MF scheme falls to work even when $K = 2$. Since the ZF scheme returns to MF scheme when $K = 1$, it is not surprised that they achieve the same ESSR when only one user is permitted to serve.

In Fig. 4, we plots the analytical and numerical results of the two schemes for the low SNR case where the SNR is also...
MF scheme may fail to provide a positive ESSR when the BS
able sum-rate at the legitimate users. In the high SNR regime,
the secrecy performances depends on the behaviour of achiev-
We found that the wiretap channels in the two precoding
also presented, respectively in the high and low SNR regime.
results of achievable ergodic sum-rate at the eavesdropper were
legitimate users of MF and ZF schemes were derived. Explicit
coding scheme in multiuser MIMO wiretap channels. The
high SNR regime.
Fig. 4. Achievable secrecy sum-rate vs. the number of served users in the
low SNR regime.

fixed as \( \rho = -20\mathrm{dB} \). Although there is a gap between the
analytical result and the numerical result for the MF scheme,
they have a similar behavior as each other. This is because
the analytical result given in Theorem 2 is a lower bound of
the actual ESSR. Both ESSR of the proposed schemes are an
increasing function with respect to the number of the served
users, as can be seen, the MF scheme can achieve a higher
ESSR than the ZF scheme. That is, MF scheme is better in the
low SNR regime. On the contrast, MF scheme fails to work
for almost all the cases in the high SNR regime.

V. CONCLUSION

In this paper, we studied the performance of linear pre-
coding scheme in multiuser MIMO wiretap channels. The
closed-form expression of achievable ergodic sum-rate at the
legitimate users of MF and ZF schemes were derived. Explicit
results of achievable ergodic sum-rate at the eavesdropper
were also presented, respectively in the high and low SNR regime.
We found that the wiretap channels in the two precoding
schemes have the similar equivalent channel model and thus
the secrecy performances depends on the behaviour of achiev-
able sum-rate at the legitimate users. In the high SNR regime,
MF scheme may fail to provide a positive ESSR when the BS
simultaneously serves more than two users while the ESSR of
ZF scheme grows with the number of the served users. While
in the low SNR regime, MF scheme achieves higher ESSR
than ZF scheme, implying that MF scheme is a better choice
due to its secrecy performance and low complexity.

APPENDIX A

By the convexity of \( \log (1 + \frac{1}{x}) \) and using Jensen’s inequal-
ity, we have
\[
\mathbb{E}[C_d^{MF}] = K \log (1 + \sinh^{MF})
\geq K \log \left(1 + \left(\mathbb{E} \left[ \frac{\rho \sum_{j \neq k} |h^H_k h_j|^2}{\rho |h_k|^4} \right] \right)^{-1}\right)
\]
From the Lindeberg-Lévy central limit theorem, it holds that
\( \frac{\sum_{j \neq k} |h^H_k h_j|^2}{\rho |h_k|^4} \sim \mathcal{CN}(0, 1) \), as \( N_t \rightarrow \infty \). Conditioned
on \( h_j \), \( h^H_k h_j \) is a Gaussian random variable with zero mean and variance \( N_t \)
which does not depend on \( h_j \). That is, \( h^H_k h_j \) is independent
of \( h_j \). We can easily obtain that
\[
\mathbb{E} \left[ \sum_{j \neq k} |h^H_k h_j|^2 \right] = N_t (K - 1).
\]
Let \( X = ||h_k||^2 \). Obviously, \( X \) follows with central chi-
square distribution with \( 2N_t \) degrees of freedom. For a \( \chi^2_{2n} \) variable, the probability density function (PDF) is given by
\[
f_n(x) = \frac{x^{n-1} e^{-x}}{\Gamma(n)},
\]
where \( \Gamma(n) \) denotes the complete gamma function. Therefore, we have
\[
\mathbb{E} \left[ \left( \frac{1}{||h_k||^4} \right) \right] = \int_0^\infty \frac{e^{-x} x^{N_t-1}}{x^2 \Gamma(N_t)} \, dx = \frac{1}{(N_t-1)(N_t-2)} \int_0^\infty x^{N_t-3} e^{-x} \frac{dx}{\Gamma(N_t-2)} = \frac{1}{(N_t-1)(N_t-2)}.
\]
Based on the results of (33) and (35), we have
\[
\mathbb{E}[C_d^{MF}] \geq K \log \left(1 + \frac{\rho (N_t - 1)(N_t - 2)}{N_t(K + \rho(K - 1))} \right).
\]
We complete the proof.

APPENDIX B

Let \( B = \frac{1}{\sqrt{N_t}} H^H G \), then \( [B]_{i,j} = \frac{1}{\sqrt{N_t}} h^H_i g_j \), where \( [B]_{i,j} \)
is the \((i,j)\)-th element of \( B \) and \( g_j \) is the \( j \)-th column of \( G \). From
the Lindeberg-Lévy central limit theorem, it holds that
\( \frac{1}{\sqrt{N_t}} h^H_i g_j \sim \mathcal{CN}(0, 1) \), as \( N_t \rightarrow \infty \). Then in the high SNR
regime, we have
\[
\mathbb{E}[C_e^{MF}] = \mathbb{E} \left[ \log \det \left( I_{N_c} + \frac{\rho}{N_t K} G^H H H^H G \right) \right]
= \mathbb{E} \left[ \log \det \left( I_{N_e} + \frac{\rho}{K} B B^H B \right) \right]
= \mathbb{E} \left[ \log \det \left( I_K + \frac{\rho}{K} B B^H B \right) \right].
\]
In the high SNR regime, we have
\[ E[C_{e}^{MF}] = \mathbb{E} \left[ \log \det \left( \mathbf{BB}^H \right) \right] + K \log(K \rho). \tag{38} \]

Let the LQ decomposition of \( \mathbf{B} \) be
\[ \mathbf{B} = \mathbf{LQ}, \tag{39} \]
where \( \mathbf{Q} \) is a \( N_e \times K \) orthonormal matrix with \( \mathbf{QQ}^H = \mathbf{I}_{N_e} \) and \( \mathbf{L} \) is a \( K \times K \) lower-triangular matrix whose diagonal entries \( [\mathbf{L}]_{i,i} \) are independent random variables following with
\[ [\mathbf{L}]_{i,i} \sim \chi^2(N_e - i + 1), \quad i = 1, \ldots, K. \tag{40} \]

Therefore, we have \[ E \left[ \log \det \left( \mathbf{BB}^H \right) \right] = E \left[ \log \det \left( \mathbf{LL}^H \right) \right] \]
\[ = \sum_{i=1}^{K} \log \chi^2(N_e - i + 1) \]
\[ = \sum_{i=1}^{K} \psi(N_e - i + 1). \tag{41} \]

Then the achievable rate of the eavesdropper in the high SNR regime can be given by
\[ E[C_{e}^{MF}] = \sum_{i=1}^{K} \psi(N_e - i + 1) + K \log(K \rho). \tag{42} \]

In the low SNR regime, we have
\[ E[C_{e}^{MF}] = \lim_{\rho \to 0} \frac{\rho}{K} \mathbb{E} \left[ \text{tr}(\mathbf{BB}^H) \right] \]
\[ = N_e \rho. \tag{43} \]

We complete the proof.

**References**


