Security Tradeoffs in Rate Splitting Multiple Access: Optimal Signal Splitting vs Revealing

Abdelhamid Salem*, Christos Masouros* and Bruno Clerckx*
*Dept of Electronic and Electrical Engineering, University College London, London, UK
*Dept of Electronic and Electrical Engineering, Imperial College London, London, UK
E-mails:{a.salem, c.masouros}@ucl.ac.uk and b.clerckx@imperial.ac.uk

***Abstract*—This paper considers the secrecy performance of rate splitting (RS) scheme in multi-user multiple-input single-output (MU-MISO) systems. The split of the users' messages into common and private parts can enhance the sum-rate of the communication systems. However, this split of the messages reveals part of the users' messages making them prone to eavesdropping. Thus, to consider the tradeoff between the sum-rate and the secrecy of RS, new analytical expressions for the ergodic sum-rate and ergodic secrecy rate are derived. Then, based on the analytical expressions of the ergodic rates, novel power allocation strategy that maximizes the sum-rate subject to a target secrecy rate is proposed and investigated. Our Monte Carlo simulations show a close match with our theoretical derivations. They also reveal that, by tuning the portion of the split signals, our power allocation approach provides a scalable tradeoff between sum-rate benefits and secrecy.**

***Index Terms*—Rate splitting, physical layer security, ZF.**

I. Introduction

Rate-Splitting Multiple Access (RSMA), based on multi-antenna rate splitting (RS) at the transmitter, is a known solution to enhance the achievable sum-rate in multi-user multiple-input single-output (MU-MISO) systems [1], [2], [3], [4]. In RS the users' messages are split into a common part and private parts, and then superimposed in a common transmission. At the reception, the common stream is first decoded by the all users. Then, each private stream is decoded by the intended user using Successive Interference Cancellation (SIC) technique. RS technique has received a growing attention in the literature. For instance, in [1] the gain performed by RS over conventional transmission scheme, e.g., without using RS (NoRS), under imperfect channel state information (CSI) at the base-station (BS) has been investigated. In [2], RS has been designed for a multiple antennas multi-cell systems with imperfect CSI; in this work RS scheme showed the superiority in a Degrees-of-Freedom sense over NoRS. The performance of RS with practical finite constellation transmission was investigated in [4]. The secrecy of RS technique has been considered in [5], [6] for two users MISO systems in the presence of an external eavesdropper.

However, the split of the users' signals into common and private parts reveals part of the users' messages making them prone to eavesdropping. This implicates vulnerabilities in terms of the security of the information, not only to external eavesdroppers, but also relating to privacy of the messages between the legitimate users of RSMA. It further raises interesting tradeoffs, where increasing the split towards the common signals may increase the sum rate of RS, while revealing the users' signals may deteriorate the security performance. Accordingly this paper investigates the secrecy performance of RS scheme in MU-MISO systems. In this regard, by applying maximum ratio transmission (MRT) technique for the common message, and zero forcing (ZF) precoding technique for the private messages the ergodic sum-rate and ergodic secrecy rate are analyzed based on imperfect CSI at the BS. Then, a power allocation scheme tailored for secure RS that maximizes the sum-rate subject to a target secrecy rate is proposed. The numerical results show clearly that the proposed power allocation scheme can provide a scalable tradeoff between the achievable sum-rate benefits and the secrecy of RS.

II. System Model

We consider a downlink MU-MISO system, in which an $N-$antennas BS communicates with K-single antenna users using RS technique. The channels are modeled as independent identically distributed (i.i.d) Rayleigh fading channels. The channel matrix between the BS and the users is denoted by $\mathbf{H} \in \mathbb{C}^{K\times N}$. The relation between the real and estimated channels can be written as, $\mathrm{H} = \hat{\mathrm{H}} + \tilde{\mathbf{H}}$, where $\hat{\mathrm{H}} \sim \mathcal{CN}(0,\hat{\boldsymbol{D}})$ is the estimated channel matrix, and $\tilde{\mathbf{H}} \sim \mathcal{CN}(0,\tilde{\mathbf{D}})$ is the estimation error matrix, while $\tilde{\mathbf{D}}$ and $\hat{\boldsymbol{D}}$ are a diagonal matrices with $[\tilde{\mathbf{D}}]_{kk} = \hat{\sigma}^2_{ek}$ and $[\hat{\boldsymbol{D}}]_{kk} = \hat{\sigma}^2_k$, which are the variances of the error and estimated channel, respectively.

In RS the resulting symbols of a given channel use can be grouped in a vector defined by $\mathbf{x} = [x_c, x_1, ..., x_K]^T \in \mathbb{C}^{K+1}$, where x_c and x_k are encoded common and private symbols, respectively, and $\mathcal{E}\left\{\mathbf{x}\mathbf{x}^H\right\} = \mathrm{I}$. Then the symbols are mapped to the BS antennas through a linear precoding matrix $\mathbf{W} = [\mathbf{w}_c, \mathbf{w}_1, ...\mathbf{w}_K]$ where $\mathbf{w}_c \in \mathbb{C}^N$ is the common precoder and $\mathbf{w}_k \in \mathbb{C}^N$ denotes the k^{th} private precoder. Accordingly, the transmitted signal can be written as $\mathbf{s} = \sqrt{P_c}\mathbf{w}_c x_c + \sum_{i=1}^{K} \sqrt{P_p}\mathbf{w}_i x_i$, where P_c and P_p are the power allocated to the common and private messages, where $P_c = (1-t)\,P$ and $P_p = \dfrac{tP}{K}$, $0 < t \leq 1$ and P is the total power. The received signal at the k^{th} user can be expressed as,

$$y_k = \sqrt{P_c}\mathbf{h}_k\mathbf{w}_c x_c + \sum_{i=1}^{K} \sqrt{P_p}\mathbf{h}_k\mathbf{w}_i x_i + n_k, \quad (1)$$

where $\mathbf{h}_k$ is the channel vector from the BS to the k^{th} user, n_k is the additive wight Gaussian noise (AWGN) at the user with zero mean and variance σ_k^2, i.e., $n_k \sim \mathcal{CN}\left(0,\, \sigma_k^2\right)$. After removing the common part, the received signal at user k can be written as,

$$y_k^p = \sum_{i=1}^{K} \sqrt{P_p}\mathbf{h}_k\mathbf{w}_i x_i + n_k. \quad (2)$$

The ergodic sum rate can be evaluated by [7]

$$\mathbb{E}\left\{R\right\} = \min_j \left(\mathbb{E}\left\{R_j^c\right\}\right)_{j=1}^{K} + \sum_{k=1}^{K} \mathbb{E}\left\{R_k^p\right\}, \quad (3)$$

where $\mathbb{E}\left\{R_k^c\right\}$ and $\mathbb{E}\left\{R_k^p\right\}$ are the ergodic rates of the common and private messages at the k^{th} user. In addition to the above sum rates, in this work we are interested in the particular vulnerabilities of RS to eavesdropping. In this model the eavesdropper can be any user, i , in the system trying to decode the private message of user k by exploiting the common message together with the leakage caused by the imperfect knowledge of the CSI. Therefore, the ergodic secrecy rate can be defined as

$$R_s = \mathbb{E}\left[\left(R^c + R_k^p\right) - \max\left(R^c + R_{i\to k}^p\right), i \neq k\right] \quad (4)$$

where $R_{i\to k}^p$ is the rate at which user i can decode user k signal.

III. Ergodic Sum-Rate and Ergodic Secrecy-Rate

In this section we analyze the ergodic sum-rate and the ergodic secrecy rate for MU-MISO systems using RS scheme. MRT and ZF precoding schemes are implemented for the common and private streams. Thus, the precoding vector for the common part can be expressed by $\mathbf{w}_c = \dfrac{\sum_{i=1}^{K} \hat{\mathbf{h}}_i^H}{\left\|\sum_{i=1}^{K} \hat{\mathbf{h}}_i^H\right\|}$. The pseudo-inverse of the estimated channel is, $\mathbf{F}^p = \hat{\mathbf{H}}^H\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)^{-1}$; thus, the precoding vector for the k^{th}private message, $\mathbf{w}_k^p$, can be expressed by $\mathbf{w}_k^p = \dfrac{\mathbf{f}_k^p}{\left\|\mathbf{f}_k^p\right\|}$, where $\mathbf{f}_k^p$ is the k^{th} vector in $\mathbf{F}^p$.

A. Ergodic rate for the common part

After applying MRT/ZF precoders, the received signal at user k in (1) can be expressed as

$$y_k = \sqrt{P_c}\mathbf{w}_c x_c(\hat{\mathbf{h}}_k - \tilde{\mathbf{h}}_k) + \sqrt{P_p}(\beta_{p_k} x_k - \sum_{i=1}^{K} \tilde{\mathbf{h}}_k\mathbf{w}_i^p x_i) + n_k \quad (5)$$

where $\beta_{p_k} = \frac{1}{\|\hat{\mathbf{f}}_k^p\|}$. Now, the SINR of the common part at the k^{th} user can be written as

$$\gamma_k^c = \frac{P_c \left| \frac{\hat{\mathbf{h}}_k \sum_{i=1}^{K} \hat{\mathbf{h}}_i^H}{\left\| \sum_{i=1}^{K} \hat{\mathbf{h}}_i^H \right\|} \right|^2 + P_c \sigma^2_{\tilde{\mathbf{h}}_k}}{\frac{P_p}{\left[\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)^{-1}\right]_{k,k}} + K P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}. \quad (6)$$

Theorem 1. *The ergodic rate of the common part at user k can be calculated as a function of the common and private signal powers P_c, P_p as in (7) where z_i and H_i are the i^{th} zero and the weighting factor, respectively, of the Laguerre polynomials.*

Proof: The proof is presented in Appendix A. ■

B. Ergodic rate for the private part

After implementing ZF precoder, the private signal at the k^{th} user in (2) can also be expressed as

$$y_k^p = \beta_{p_k} \sqrt{P_p} x_k - \sum_{i=1}^{K} \sqrt{P_p} \tilde{\mathbf{h}}_k \mathbf{w}_i^p x_i + n_k \quad (8)$$

Now, the SINR of the k^{th} user can be written as

$$\gamma_k^p = \frac{\frac{P_p}{\left[\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)^{-1}\right]_{k,k}} + P_p \sigma^2_{\tilde{\mathbf{h}}_k}}{(K-1) P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}. \quad (9)$$

Theorem 2. *The ergodic rate of the private part at user k can be evaluated by (10) where z_i and H_i are the i^{th} zero and the weighting factor, respectively, of the Laguerre polynomials.*

Proof: The proof is presented in Appendix B. ■

C. Ergodic secrecy rate

The ergodic secrecy rate can be calculated by [8, Eq(5)]

$$\mathbb{E}[R_s] = \left[\mathbb{E}[R_{\mathrm{k}}^p] - \mathbb{E}\left[\max\{R_{i\to k}^p\}\right]\right]^+. \quad (11)$$

User i (the eavesdropper) detects first his own messages (common and private), then removes them using SIC to eavesdrop the k^{th} user's signal by exploiting the leakage caused by the imperfect knowledge of the CSI. Therefore, the received signal at user i to detect user k signal is

$$y_{i\to k}^p = \sqrt{P_p} \tilde{\mathbf{h}}_i \mathbf{w}_k^p x_k + \sum_{\substack{j=1 \\ j\neq i}}^{K} \sqrt{P_p} \tilde{\mathbf{h}}_i \mathbf{w}_j^p x_j + n_i. \quad (12)$$

Thus the SINR can be written as

$$\gamma_{i\to k}^p = \frac{P_p \sigma^2_{\tilde{\mathbf{h}}_i}}{(K-1) P_p \sigma^2_{\tilde{\mathbf{h}}_i} + \sigma_i^2}. \quad (13)$$

Theorem 3. *The ergodic secrecy rate in this case can be calculated by (14).*

Proof: The proof is presented in Appendix C. ■

IV. Power Allocation for Secure RS

In this section, based on the ergodic sum-rate and secrecy rate expressions, power allocation schemes are considered to split the signals with the aim of maximizing the ergodic sum-rate while achieving a target secrecy rate. Accordingly, we can formulate the optimization problem as

$$\max_{0<t\leq 1} \mathbb{E}\{R_c\} + \sum_{k=1}^{K} \left(\mathbb{E}\{R_k^p\}\right)$$

$$\text{s.t. } \left[\mathbb{E}[R_{\mathrm{k}}^p] - \mathbb{E}\left[\max\{R_{i\to k}^p\}\right]\right]^+ > r_s, \forall_{i,k}$$

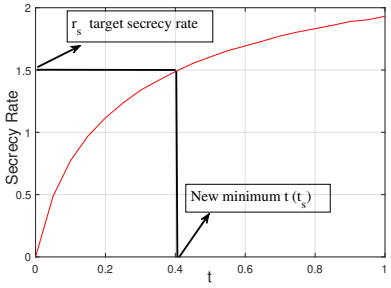
$$P_c + K P_p \leq P \quad (15)$$

where r_s is target secrecy rate. We propose a low complexity heuristic approach to solve this problem by first finding the value (t_s) of t that achieves the target secrecy rate, r_s. Clearly, any value above t_s will satisfy the secrecy constraint. Then the optimal value of t will be in the region $[t_s, 1]$ as illustrated in Fig. 1 below. In this case the value of t_s is the value that can fulfill the secrecy constraint in (15). This value can be obtained numerically by changing t from 0 to 1. To gain some insights, we can derive the value of t_s as follows. Using the first order Laguerre polynomial, the secrecy constraint in (15) holds when

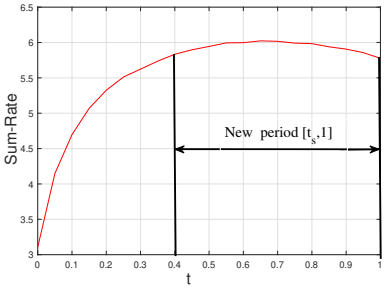
$$\mathbb{E}\left[R_k^c\right] = \frac{1}{\ln\left(2\right)} \sum_{i=1}^{n} \mathrm{H}_i \frac{1}{z_i} \left(1 - \left(\left(1 + \frac{P_c \theta_k \, z_i}{\beta}\right)^{-K}\right) e^{-z P_c \sigma^2_{\tilde{\mathbf{h}}_k}}\right) \left(\left(1 + \frac{P_p \Psi_k \, z_i}{\beta}\right)^{-1+K-N}\right) \tag{7}$$

$$\mathbb{E}\left[R_k^p\right] = \sum_{i=1}^{n} \mathrm{H}_i \frac{1}{z_i} \log_2\left(1 + \frac{P_p y_i + P_p \sigma^2_{\tilde{\mathbf{h}}_k}}{\left(K-1\right) P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}\right) \frac{y_i^{(N-K)} \left(\Psi_k\right)^{N-K+1} e^{-\Psi_k y_i}}{\Gamma\left(N-K+1\right)} \tag{10}$$

$$\begin{aligned} \mathbb{E}\left[R_s\right] \;=\; & \sum_{i=1}^{n} \mathrm{H}_i \frac{1}{z_i} \log_2\left(1 + \frac{P_p y_i + P_p \sigma^2_{\tilde{\mathbf{h}}_k}}{\left(K-1\right) P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}\right) \frac{y_i^{(N-K)} \left(\Psi_k\right)^{N-K+1} e^{-\Psi_k y_i}}{\Gamma\left(N-K+1\right)} \\ & - \log_2\left(1 + \frac{P_p \sigma^2_{\tilde{\mathbf{h}}_i}}{\left(K-1\right) P_p \sigma^2_{\tilde{\mathbf{h}}_i} + \sigma_i^2}\right) \end{aligned} \tag{14}$$



(a) Ergodic secrecy rate versus t.



(b) Ergodic sum-rate versus t.

Figure 1: Power-Allocation scheme.

$$\begin{aligned} r_s \;=\; & \Xi \log_2\left(1 + \frac{t_s P y_1 + t_s P \sigma^2_{\tilde{\mathbf{h}}_k}}{\left(K-1\right) t_s P \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}\right) \\ & - \log_2\left(1 + \frac{t_s P \sigma^2_{\tilde{\mathbf{h}}_i}}{\left(K-1\right) t_s P \sigma^2_{\tilde{\mathbf{h}}_i} + \sigma_i^2}\right) \end{aligned} \tag{16}$$

where $\Xi = \mathrm{H}_1 \frac{1}{y_1} \frac{y_1^{(N-K)} (\Psi_k)^{N-K+1} e^{-\Psi_k y_1}}{\Gamma(N-K+1)}$. Then t_s can be obtained by

$$t_s = \frac{\left(2^{\varrho} - 1\right)\left(\sigma_k^2\right)}{P y_1 + P \sigma^2_{\tilde{\mathbf{h}}_k} - \left(2^{\varrho} - 1\right)\left(K-1\right) P \sigma^2_{\tilde{\mathbf{h}}_k}}. \tag{17}$$

where $\varrho = \frac{1}{\Xi}\left(r_s + \log_2\left(1 + \frac{\sigma^2_{\tilde{\mathbf{h}}_i}}{(K-1)\sigma^2_{\tilde{\mathbf{h}}_i}}\right)\right)$. Now, the optimization problem can be reformulated as

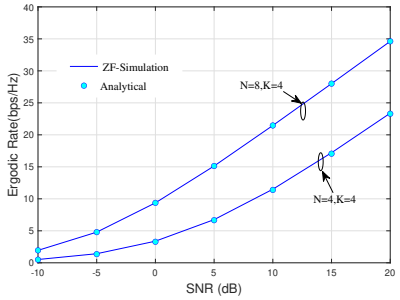
$$\max_{t_s < t \leq 1} \mathbb{E}\left\{R_c\right\} + \sum_{k=1}^{K} \left(\mathbb{E}\left\{R_k^p\right\}\right)$$

$$\text{s.t. } P_c + K P_p \leq P \tag{18}$$

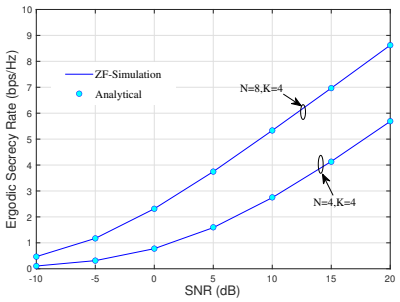
The optimal value of t can be found by a simple one dimensional search techniques, such as golden section method, over $t_s \leq t \leq 1$.

V. Numerical Results

In this section some numerical results are presented, and Monte-Carlo simulations are conducted to confirm our analysis. Assuming the users have same noise power σ^2, the transmit signal to noise ratio (SNR) is defined as SNR = $\frac{p}{\sigma^2}$. The channel error variance considered in this Section is given by $\hat{\sigma}^2_{ek} = \beta P^{-\alpha}$, where $\beta \geq 0$ and $\alpha \in [0, 1]$ are varied to represent different CSI accuracies and SNR scaling [7].

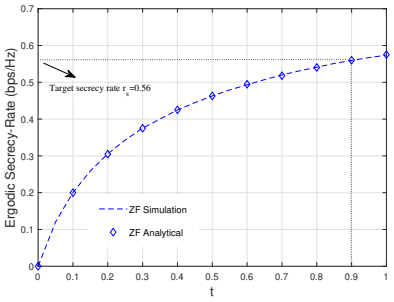


(a) Ergodic sum-rate of RS versus transmit SNR.

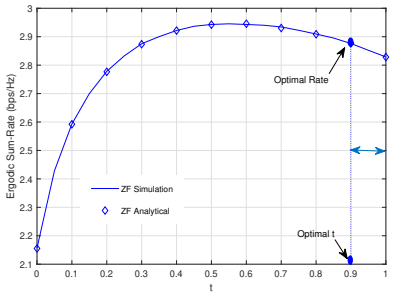


(b) Ergodic secrecy-rate of RS versus transmit SNR.

Figure 2: Ergodic sum-rate and secrecy rates of RS versus transmit SNR when $\beta = 0.1$ and $\alpha = 0.5$.



(a) Ergodic secrecy-rate versus t.



(b) Ergodic sum-rate versus t.

Figure 3: Ergodic sum-rate and secrecy rates of RS versus t when SNR=5 dB, $N = K = 3$, $\beta = 0.7$ and $\alpha = 0$.

In Fig. 2 we plot the ergodic sum-rate and secrecy rate versus the SNR for the RS transmission scheme when $N = K = 4$, $N = 8, K = 4$ and t is optimized using the golden section technique, Fig. 2a presents the sum-rate and Fig. 2b shows the secrecy-rate. The good agreement between the analytical and simulated results confirms the validity of the analysis introduced in this paper. Looking closer at the results in this figure, it is clear that increasing the SNR and the number of antennas N always enhances the ergodic sum-rate and secrecy rate. In addition, the ZF precoding technique can provide secure RS transmission.

In Fig. 3 we plot the ergodic sum-rate and secrecy rate versus t for the target secrecy rate $r_s = 0.56\ (bps/Hz)$. The tradeoff between the secrecy rate and the sum rate can be observed clearly from the results in this figure, where $t = 1$ is the best option for the secrecy rate, but $t = 0.6$ is the best for the sum-rate. However, in our case the value of t that achieves the secrecy constraint is $t_s = 0.9$ as shown in Fig.3a. Thus the optimal value of t is in the range $[0.9, 1]$. By using golden section algorithm, the optimal value of t is $t^* = 0.9$ as in Fig.3b. Therefore, the BS should allocate most of the power to the private messages. On the other hand, the optimal value of t without secrecy constraint is about 0.6. That means that without secrecy constraint the BS should allocate more power to the common part to achieve the optimal performance, and this explains clearly the impact of the secrecy constraint on the optimal value of t.

VI. Conclusions

In this paper the secrecy performance of RS scheme in MU-MISO systems was considered. New analytical expressions for the ergodic sum-rate and secrecy rate were derived and a power allocation strategy that maximizes the sum-rate subject to a target secrecy rate was proposed. The results in this work demonstrated the inherent tradeoff between sum rate benefits and secrecy rates for RS, and provided a low complexity methodology for optimizing the split between common and private signaling.

Appendix A

The SINR of the common part at the k^{th} user in (6) can be written as

$$\gamma_k^c = \frac{P_c\, x + P_c \sigma^2_{\tilde{\mathbf{h}}_k}}{P_p y + P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2} \tag{19}$$

where $x = \left| \frac{\hat{\mathbf{h}}_k \sum_{i=1}^{K} \hat{\mathbf{h}}_i^H}{\left\| \sum_{i=1}^{K} \hat{\mathbf{h}}_i^H \right\|} \right|^2$ and $y = \frac{1}{\left[\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)^{-1}\right]_{k,k}}$. Thus, the ergodic rate for the common part is $\mathbb{E}\left[R_k^c\right] = \mathbb{E}\left[\log_2\left(1+\gamma_k^c\right)\right]$. It is found in [9] that for any random variables $x, y > 0$

$$\mathbb{E}\left[\ln\left(1+\frac{x}{y}\right)\right] = \int_0^\infty \frac{1}{z}\left(\mathcal{M}_y\left(z\right) - \mathcal{M}_{y,x}\left(z\right)\right) dz \tag{20}$$

where $\mathcal{M}_x\left(z\right) = \mathbb{E}\left[e^{-zx}\right]$ denotes the moment generating function (MGF) of x and $\mathcal{M}_{v,u}\left(z\right) = \mathbb{E}\left[e^{-z(v+u)}\right]$. Accordingly, (19) can be expressed as $\gamma_k^c = \frac{u}{v+\beta}$ where $u = P_c\, x + P_c \sigma^2_{\tilde{\mathbf{h}}_k}$, $v = P_p y$, and $\beta = K P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2$. Now, from (20) the ergodic rate of the common part at user k can be calculated by

$$R_k^c = \frac{1}{\ln\left(2\right)} \int_0^\infty \frac{1}{z}\left(1 - \mathcal{M}_u\left(z\right) e^{-zP_c\sigma^2_{\tilde{\mathbf{h}}_k}}\right) \mathcal{M}_v\left(z\right) e^{-z\beta}\, dz \tag{21}$$

Since u has gamma distribution, the MGF of u is $\mathcal{M}_u\left(z\right) = \left(1 + P_c\theta_k\, z\right)^{-K}$. Then, the MGF of v can be calculated as $\mathcal{M}_v\left(z\right) = \left(1 + P_p\Psi_k\, z\right)^{-1+K-N}$. Substituting $\mathcal{M}_u\left(z\right)$ and $\mathcal{M}_v\left(z\right)$ into (21) and using Gaussian rules we can get the ergodic rate in Theorem 1.

Appendix B

The SINR of the private part at the k^{th} user in (9) can be expressed as $\gamma_k^p = \frac{P_p y + P_p \sigma^2_{\tilde{\mathbf{h}}_k}}{\sum_{\substack{i=1 \\ i\neq k}}^{K} P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}$. Now, the ergodic private-rate is given by $\mathbb{E}\left[R_k^p\right] = \mathbb{E}\left[\log_2\left(1+\gamma_k^p\right)\right]$ and

$$\mathbb{E}\left[R_k^p\right] = \int_0^\infty \log_2\left(1 + \frac{P_p y + P_p \sigma^2_{\tilde{\mathbf{h}}_k}}{\left(K-1\right) P_p \sigma^2_{\tilde{\mathbf{h}}_k} + \sigma_k^2}\right) f_y\left(y\right) dy$$

where the PDF of y is $f_y\left(y\right) = \frac{y^{(N-K)} (\Psi_k)^{N-K+1} e^{-\Psi_k y}}{\Gamma(N-K+1)}$. By using Gaussian rules we can find the expression in Theorem 2.

Appendix C

The ergodic rate of user k, $\mathbb{E}\left[R_k^p\right]$, is derived in (10), and the ergodic rate at the worst user (eavesdropper), for user k, is calculated by

$$\mathbb{E}\left[\max\left\{R_{i\to k}^p\right\}\right] = \mathbb{E}\left[\max_i \left\{\log_2\left(1+\gamma_{i\to k}^p\right)\right\}\right] \tag{22}$$

Substituting (13) into (22), the ergodic rate at the worst user, for user k, is

$$\mathbb{E}\left[\max R_{i\to k}^p\right] = \max_i \log_2\left(1 + \frac{P_p \sigma^2_{\tilde{\mathbf{h}}_i}}{\left(K-1\right) P_p \sigma^2_{\tilde{\mathbf{h}}_j} + \sigma_i^2}\right) \tag{23}$$

Substituting (10) and (23) into (11), we can obtain the ergodic secrecy rate presented in Theorem 3.

References

[1] C. Hao, Y. Wu, and B. Clerckx, "Rate analysis of two-receiver miso broadcast channel with finite rate feedback: A rate-splitting approach," *IEEE Transactions on Communications*, vol. 63, no. 9, pp. 3232–3246, Sept 2015.

[2] C. Hao and B. Clerckx, "Miso networks with imperfect csit: A topological rate-splitting approach," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 2164–2179, May 2017.

[3] Y. Mao, B. Clerckx, and V. O. Li, "Rate-splitting multiple access for downlink communication systems: bridging, generalizing, and outperforming sdma and noma," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 133, May 2018. [Online]. Available: https://doi.org/10.1186/s13638-018-1104-7

[4] A. Salem, C. Masouros, and B. Clerckx, "Rate splitting with finite constellations: The benefits of interference exploitation vs suppression," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1541–1557, 2021.

[5] P. Li, M. Chen, Y. Mao, Z. Yang, B. Clerckx, and M. Shikh-Bahaei, "Cooperative rate-splitting for secrecy sum-rate enhancement in multi-antenna broadcast channels," in *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, 2020, pp. 1–6.

[6] H. Fu, S. Feng, W. Tang, and D. W. K. Ng, "Robust secure beamforming design for two-user downlink miso rate-splitting systems," *IEEE Transactions on Wireless Communications*, vol. 19, no. 12, pp. 8351–8365, 2020.

[7] H. Joudeh and B. Clerckx, "Sum-rate maximization for linearly precoded downlink multiuser miso systems with partial csit: A rate-splitting approach," *IEEE Transactions on Communications*, vol. 64, no. 11, pp. 4847–4861, Nov 2016.

[8] J. Li and A. P. Petropulu, "On ergodic secrecy rate for gaussian miso wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, April 2011.

[9] K. Hamdi, "A useful lemma for capacity analysis of fading interference channels," *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 411–416, Feb. 2010.