Secret-key Agreement over Spatially Correlated Fast-Fading Multiple-Antenna Channels with Public Discussion

Marwen Zorgui[1], Zouheir Rezki[1], Basel Alomair[2] and Mohamed-Slim Alouini[1]
[1]Computer, Electrical, and Mathematical Sciences and Engineering (CEMSE) Division
King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia
[2] The National Center for Cybersecurity Technology (C4C)
King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia
{marwen.zorgui,zouheir.rezki,slim.alouini}@kaust.edu.sa, alomair@kacst.edu.sa

***Abstract*—We consider secret-key agreement with public discussion over multiple-input multiple-output (MIMO) Rayleigh fast-fading channels under correlated environment. We assume that transmit, legitimate receiver and eavesdropper antennas are correlated. The legitimate receiver and the eavesdropper are assumed to have perfect channel knowledge while the transmitter has only knowledge of the correlation matrices. First, we derive the expression of the secret-key capacity under the considered setup. Then, we prove that the optimal transmit strategy achieving the secret-key capacity consists in transmitting independent Gaussian signals along the eingenvectors of the transmit correlation matrix. The powers allocated to each channel mode are determined as the solution to a numerical optimization problem that we derive. A necessary and sufficient condition for beamforming (i.e., transmitting along the strongest channel mode) to be capacity-achieving is derived. Finally, we analyze the impact of correlation matrices on the system performance and provide closed-form expressions of the gain/loss due to correlation in the high power regime.**

***Index Terms*—Secret-key agreement, MIMO systems, optimal signaling, correlation, beamforming, high power regime.**

I. Introduction

The premise of information-theoretic security is to exploit the inherent randomness of the physical medium and the difference between a legitimate receiver channel and an eavesdropper channel in order to securely transmit confidential messages. With the availability of a feedback channel, much work has been investigating the idea of distilling a secret-key shared between legitimate parties through the concept of common randomness. In particular, in case of fast-fading multiple-input multiple-output (MIMO) wiretap channels, [1] shows that the transmitter does not require the instantaneous channel state information to achieve a positive secret-key rate. The secret-key capacity is provided and it is also shown that distributing power uniformly across transmit antennas is secret-key capacity-achieving. In [1], it is assumed that the channel matrices have independent and identically distributed (i.i.d.) rows and also i.i.d. columns. Such an assumption may be hard to prove in practice. Indeed, practical systems demonstrate strong correlation due to several impairments, to mention a lack of sufficient local reflectors or insufficient spacing across transmit and/or receive antennas. Taking correlation into consideration, a wide body of work has focused on the effect of spatial correlation on the performance of wireless communication systems, but without secrecy constraint [2]. To the best of our knowledge, the effect of spatial correlation on secrecy has not been addressed before. Analyzing the impact of correlation and identifying optimal signaling strategies under such assumptions is interesting from both information-theoretic and system design perspectives.

Motivated by the importance of wireless physical layer security and the relevance of spatial correlation in practical wireless systems, we analyze the performance of secret-key agreement in a correlated environment. For that, we consider the problem of secret-sharing over a fast-fading MIMO wiretap channel. We assume that transmit, legitimate receiver and eavesdropper antennas are all correlated, and we refer to them as transmit, receive and eavesdropper correlation, respectively. First, we provide the expression of the secret-key capacity under this setup. Next, we identify the optimal signaling strategy achieving the secret-key capacity. Optimal power allocation is shown to be the solution of an optimization problem depending on the system parameters. Next, we develop a necessary and sufficient condition for beamforming to be a secret-key capacity-achieving strategy. We also analyze the impact of each correlation matrix on the system performance and provide numerical results supporting our analysis. Finally, we investigate the system performance in the high power regime and provide closed-form expressions of the asymptotic difference between secret-key capacities with and without spatial correlation.

The organization of this paper is as follows. In Section II, the system model and the corresponding assumptions are described and the secret-key capacity expression is derived. Section III contains the solution to the transmitter optimization problem. In Section IV, we develop a necessary and sufficient condition under which beamforming is optimal. In Section V, we study the impact of correlation matrices on the secret-key capacity. Section VI analyzes the system in the high power regime. Section VII contains a discussion of these results.

II. System Model and Preliminaries

Notations: Throughout this paper, the symbol † indicates the conjugate transpose operator. $\mathbf{I}_n$ denotes the $n \times n$ identity matrix and $\text{diag}\left[\lambda_1, \ldots, \lambda_n\right]$ denotes the $n \times n$ diagonal matrix whose entries are $\lambda_1, \ldots, \lambda_n$. Vectors are denoted with

This work has been supported by King Abdulaziz City of Science and Technology (KACST), Riyadh, Saudi Arabia.

small bold letters while matrices are denoted with capital bold letters. The capital letter $\mathbb{E}$ denotes the expectation of a random quantity. We use the symbol $\mathbb{I}(\cdot;\cdot)$ to denote the mutual information between two random variables. $\mathbf{H}_{i\bullet}$ and $\mathbf{H}_{\bullet j}$ represent, respectively, the ith row and the jth column of a matrix $\mathbf{H}$. The symbol $|\cdot|$ is used to denote the determinant of a matrix and $\mathrm{Tr}(\cdot)$ denotes the trace operator. We use the notation $\mathbf{A} \succeq 0$ to denote that A is a positive semi-definite matrix. $\mathbf{A}^{\frac{1}{2}}$ denotes a square-root of a matrix. The notation $\mathbf{x} \sim \mathcal{CN}\{0, \mathbf{\Sigma}\}$ denotes that the random vector $\mathbf{x}$ is complex Gaussian with zero mean and covariance matrix $\mathbf{\Sigma}$.

We consider the problem of secret-key agreement between a transmitter and a legitimate receiver in the presence of an eavesdropper who overhears transmissions broadcasted over the wireless medium [1]. The transmitter, destination and eavesdropper have m_S, m_D and m_E antennas, respectively. For each channel use, the channel is represented as follows

$$\begin{aligned} \mathbf{y}_D(i) &= \mathbf{H}_D(i)\mathbf{x}(i) + \mathbf{n}_D(i) \\ \mathbf{y}_E(i) &= \mathbf{H}_E(i)\mathbf{x}(i) + \mathbf{n}_E(i), \end{aligned} \tag{1}$$

where index $i, i = 1, \ldots, b$, designates time instant i, and

- $\mathbf{x}(i)$ is the $m_S \times 1$ complex-valued transmitted symbol vector,
- $\mathbf{y}_D(i)$ (resp. $\mathbf{y}_E(i)$) is the $m_D \times 1$ (resp. $m_E \times 1$) complex-valued received symbol vector at the destination (resp. at the eavesdropper),
- $\mathbf{n}_D(i)$ (resp. $\mathbf{n}_E(i)$) is the $m_D \times 1$ (resp. $m_E \times m_S$) noise vector with i.i.d circular-symmetric complex Gaussian entries $\sim \mathcal{CN}(0, \sigma_D^2)$ (resp. $\sim \mathcal{CN}(0, \sigma_E^2)$),
- $\mathbf{H}_D(i)$ (resp. $\mathbf{H}_E(i)$) is the $m_D \times m_S$ (resp. $m_E \times m_S$) channel matrix from the source to the destination (resp. the eavesdropper).

For ease of notation we drop the index hereafter. The transmitter is constrained in its total power, that is equivalent to a trace constraint on the input covariance matrix $\mathbf{Q} = \mathbb{E}[\mathbf{x}\mathbf{x}^\dagger]$

$$\mathrm{Tr}(\mathbf{Q}) \leq P. \tag{2}$$

The channel matrices for the case where there is spatial correlation at all terminals, are modeled as in [2]:

$$\begin{aligned} \mathbf{H}_D &= \mathbf{R}_D^{1/2}\mathbf{W}_D\mathbf{R}_T^{1/2} \\ \mathbf{H}_E &= \mathbf{R}_E^{1/2}\mathbf{W}_E\mathbf{R}_T^{1/2}, \end{aligned} \tag{3}$$

where $\mathbf{W}_D$ (resp. $\mathbf{W}_E$) is $m_D \times m_S$ (resp. $m_E \times m_S$) matrix with i.i.d entries $\sim \mathcal{CN}(0,1)$. $\mathbf{R}_T$ is the $m_S \times m_S$ transmit correlation matrix, $\mathbf{R}_D$ is the $m_D \times m_D$ destination correlation matrix and $\mathbf{R}_E$ is the $m_E \times m_E$ eavesdropper correlation matrix. All correlation matrices are normalized such that all diagonal entries are unity. The destination and the eavesdropper have perfect CSI about their incoming channels while the transmitter has only covariance feedback, i.e., the transmitter knows the correlation matrices.

Let $\mathbf{y} = \begin{bmatrix}\mathbf{y}_D & \mathbf{H}_D\end{bmatrix}$ be the observation of the legitimate receiver for each channel use, and $\mathbf{z} = \begin{bmatrix}\mathbf{y}_E & \mathbf{H}_E\end{bmatrix}$ be the observation of the eavesdropper for each channel use. The wireless channel modeled in (1) is used n times. The n uses of the channel are assumed independent and identically distributed, resulting in the memoryless property of the channel $(\mathbf{x}, \mathbf{y}, \mathbf{z})$. Since the transmitter does not have knowledge of the current channels realizations, we have that $\mathbf{x}$ is independent of $\mathbf{H}_D$, $\mathbf{H}_E$, $\mathbf{n}_D$ and $\mathbf{n}_E$. The signals satisfy the Markov chain $\mathbf{y} \to \mathbf{x} \to \mathbf{z}$. Henceforth, using [1, Theorem 1], the secret-key capacity is obtained as

$$C = \max_{\mathrm{Tr}(\mathbf{Q}) \leq P, \mathbf{Q} \succeq 0} \left[\mathbb{I}(\mathbf{x};\mathbf{y}) - \mathbb{I}(\mathbf{y};\mathbf{z})\right]. \tag{4}$$

Following along similar lines as [1], it can be seen that the optimal input distribution is a circular-symmetric complex Gaussian $\sim \mathcal{CN}(0, \mathbf{Q})$. Taking into account the additional correlation matrices, the secret-key capacity can be expressed as

$$C = \max_{\mathrm{Tr}(\mathbf{Q}) \leq P, \mathbf{Q} \succeq 0} \left\{ \mathbb{E}\left[\log|\mathbf{K}_{\mathbf{y}_D} - \mathbf{K}_{\mathbf{y}_D\mathbf{y}_E}\mathbf{K}_{\mathbf{y}_E}^{-1}\mathbf{K}_{\mathbf{y}_E\mathbf{y}_D}|\right] - m_D \log(\sigma_D^2) \right\}, \tag{5}$$

where the expectation is taken over the realizations of $(\mathbf{H}_D, \mathbf{H}_E)$. $\mathbf{K}_{\mathbf{y}_D}$, $\mathbf{K}_{\mathbf{y}_E}$, $\mathbf{K}_{\mathbf{y}_D\mathbf{y}_E}$ and $\mathbf{K}_{\mathbf{y}_E\mathbf{y}_D}$ are the conditional covariances and cross-covariances. After some algebraic manipulations as in [3, Lemma 1], the secret-key capacity can be expressed as

$$C = \max_{\mathrm{Tr}(\mathbf{Q}) \leq P, \mathbf{Q} \succeq 0} \mathbb{E}\left[\log \frac{\left|\mathbf{I}_{m_D+m_E} + \mathbf{H}\mathbf{Q}\mathbf{H}^\dagger\right|}{\left|\mathbf{I}_{m_E} + \frac{1}{\sigma_E^2}\mathbf{H}_E\mathbf{Q}\mathbf{H}_E^\dagger\right|}\right], \tag{6}$$

where $\mathbf{H} = \begin{bmatrix}\frac{1}{\sigma_D}\mathbf{H}_D \\ \frac{1}{\sigma_E}\mathbf{H}_E\end{bmatrix}$. In the following section, we identify the optimal transmission scheme achieving capacity.

III. Optimal signaling strategy

Let the eigenvalue decomposition of the correlation matrix $\mathbf{R}_l$ be as $\mathbf{R}_l = \mathbf{U}_l\mathbf{\Lambda}_l\mathbf{U}_l^\dagger$, for $l \in \{T, D, E\}$, where $\mathbf{U}_l$ is unitary and $\mathbf{\Lambda}_l$ is a diagonal matrix containing the corresponding eigenvalues. We further assume, without loss in generality, that the eigenvalues of the transmit correlation matrix $\left\{\lambda_i^T, i = 1, \ldots, m_S\right\}$ are arranged in decreasing order, i.e., $\lambda_1^T \geq \lambda_2^T \geq \ldots \geq \lambda_{m_S}^T$. The following theorem characterizes the optimal transmission scheme.

Theorem 1. Let $\mathbf{H}_D = \mathbf{R}_D^{1/2}\mathbf{W}_D\mathbf{R}_T^{1/2}$, $\mathbf{H}_E = \mathbf{R}_E^{1/2}\mathbf{W}_E\mathbf{R}_T^{1/2}$ with $\mathbf{W}_D \sim \mathcal{CN}(0, \mathbf{I}_{m_D})$, $\mathbf{W}_E \sim \mathcal{CN}(0, \mathbf{I}_{m_E})$ and assume that $\mathbf{R}_T$ is of full rank, then the optimal input covariance matrix can be expressed as $\mathbf{Q} = \mathbf{U}_T\mathbf{\Lambda}_Q\mathbf{U}_T^\dagger$, where $\mathbf{\Lambda}_Q = \mathrm{diag}[\lambda_1^Q, \ldots, \lambda_{m_S}^Q]$.

That is, the optimal signaling strategy is to transmit independent complex circular Gaussian inputs along the eigenvectors of $\mathbf{R}_T$. The optimal power allocation is obtained by solving a numerical optimization problem subject to a trace constraint.

Proof: Starting from the expressions of $\mathbf{H}_D$ and $\mathbf{H}_E$, $\mathbf{H}$ can be expressed as

$$\begin{aligned} \mathbf{H} &= \begin{bmatrix}\frac{1}{\sigma_D}\mathbf{R}_D^{1/2}\mathbf{W}_D\mathbf{R}_T^{1/2} \\ \frac{1}{\sigma_E}\mathbf{R}_E^{1/2}\mathbf{W}_E\mathbf{R}_T^{1/2}\end{bmatrix} = \underbrace{\begin{bmatrix}\mathbf{R}_D^{1/2} & 0 \\ 0 & \mathbf{R}_E^{1/2}\end{bmatrix}}_{\mathbf{R}_{DE}^{1/2}} \underbrace{\begin{bmatrix}\frac{1}{\sigma_D}\mathbf{W}_D \\ \frac{1}{\sigma_E}\mathbf{W}_E\end{bmatrix}}_{\mathbf{W}} \mathbf{R}_T^{1/2} \\ &= \mathbf{R}_{DE}^{1/2}\mathbf{W}\mathbf{R}_T^{1/2}. \end{aligned} \tag{7}$$

Based on that and using the techniques of [4], one can obtain the desired result. ∎

Based on Theorem 1, the optimization problem becomes

$$C = \max_{\mathrm{Tr}(\mathbf{\Lambda}_Q) \leq P, \mathbf{\Lambda}_Q \succeq 0} \mathbb{E}\left[\log \frac{\left|\mathbf{I}_{m_D+m_E} + \mathbf{\Lambda}_{DE}^{1/2}\mathbf{W}\mathbf{\Lambda}_T\mathbf{\Lambda}_Q\mathbf{W}^\dagger\mathbf{\Lambda}_{DE}^{1/2}\right|}{\left|\mathbf{I}_{m_E} + \frac{1}{\sigma_E^2}\mathbf{\Lambda}_E^{1/2}\mathbf{W}_E\mathbf{\Lambda}_T\mathbf{\Lambda}_Q\mathbf{W}_E^\dagger\mathbf{\Lambda}_E^{1/2}\right|}\right]$$

$$= \max_{\mathrm{Tr}(\mathbf{\Lambda}_Q)\leq P, \mathbf{\Lambda}_Q \succeq 0} C(\mathbf{\Lambda}_Q), \tag{8}$$

Remark 1. We note that the power constraint should be satisfied with equality. Indeed, since the function $C(\mathbf{\Lambda}_Q)$, defined in (8), is strictly increasing on the set of positive definite matrices [5], we can simply allocate the rest of the available power to the strongest mode to achieve a higher secret-key rate. The optimal eigenvalues have to be computed by solving the optimization problem

$$\mathbf{\Lambda}_Q^{opt} = \arg \max_{\mathbf{\Lambda}_Q \succeq 0: \sum_{i=1}^{m_S} \lambda_i^Q = P} \mathbb{E}\left[\log \frac{\left|\mathbf{I}_{m_D+m_E} + \sum_{i=1}^{m_S} \lambda_i^T \lambda_i^Q \tilde{\mathbf{W}}_{\bullet i} \tilde{\mathbf{W}}_{\bullet i}^\dagger\right|}{\left|\mathbf{I}_{m_E} + \frac{1}{\sigma_E^2} \sum_{i=1}^{m_S} \lambda_i^T \lambda_i^Q \tilde{\mathbf{W}}_{E\bullet i} \tilde{\mathbf{W}}_{E\bullet i}^\dagger\right|}\right], \tag{9}$$

where

$$\tilde{\mathbf{W}}_{\bullet i} = \mathbf{\Lambda}_{RE}^{1/2} \mathbf{W}_{\bullet i} = \begin{pmatrix} \frac{1}{\sigma_D} \mathbf{\Lambda}_D^{1/2} \mathbf{W}_{D\bullet i} \\ \frac{1}{\sigma_E} \mathbf{\Lambda}_E^{1/2} \mathbf{W}_{E\bullet i} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sigma_D} \tilde{\mathbf{W}}_{D\bullet i} \\ \frac{1}{\sigma_E} \tilde{\mathbf{W}}_{E\bullet i} \end{pmatrix} \tag{10}$$

$$\tilde{\mathbf{W}}_{E\bullet i} = \mathbf{\Lambda}_E^{1/2} \mathbf{W}_{E\bullet i}, \ \tilde{\mathbf{W}}_{D\bullet i} = \mathbf{\Lambda}_D^{1/2} \mathbf{W}_{D\bullet i}. \tag{11}$$

Remark 2. The optimal choice of eigenvectors depends only on the transmit antenna correlation matrix $\mathbf{R}_T$ and is independent of the receive correlation matrix $\mathbf{R}_D$ and of the eavesdropper correlation matrix $\mathbf{R}_E$. Nonetheless, the optimal power allocation scheme depends on all the three correlation matrices. This will highlighted by the necessary and sufficient condition of optimality of beamforming, derived in the sequel.

In the next section, we study the optimality of beamforming. Beamforming corresponds to transmitting along the strongest eigenvector. In this case, the input covariance matrix has rank one. We provide a necessary and sufficient condition under which beamforming is secret-key capacity-achieving.

IV. Optimality of beamforming

The form of the optimization problem (9) does not lend itself to a simple closed-form solution. Knowing the eigenvalues of the correlation matrices $\mathbf{R}_T$, $\mathbf{R}_D$ and $\mathbf{R}_E$, the optimal power allocation is difficult to compute. For that, we study the condition under which allocating all the power to the strongest eigenvector is optimal. The following theorem formalizes our result.

Theorem 2. For the problem of secret-key agreement over fast-fading MIMO wiretap channel with known transmit correlation matrix $\mathbf{R}_T$, known receive correlation matrix $\mathbf{R}_D$, and known eavesdropper correlation matrix $\mathbf{R}_E$, with $\mathcal{A}$ defined as in (13), we have the following properties:

- if $\mathcal{A} \leq 0$, then beamforming is always optimal,
- else: beamforming is optimal if and only if

$$\lambda_2^T \mathcal{A} + \frac{1}{P}\left\{\mathbb{E}\left[\frac{1}{1+P\lambda_1^T\left(\frac{\|\tilde{\mathbf{W}}_{D\bullet 1}\|^2}{\sigma_D^2} + \frac{\|\tilde{\mathbf{W}}_{E\bullet 1}\|^2}{\sigma_E^2}\right)}\right] - \mathbb{E}\left[\frac{1}{1+\frac{P\lambda_1^T}{\sigma_E^2}\|\tilde{\mathbf{W}}_{E\bullet 1}\|^2}\right]\right\} \leq 0 \tag{12}$$

$$\mathcal{A} = \frac{m_D}{\sigma_D^2} - \mathbb{E}\left[\frac{P\lambda_1^T\left[\frac{\|\mathbf{\Lambda}_D^{1/2}\tilde{\mathbf{W}}_{D\bullet 1}\|^2}{\sigma_D^4} + \frac{\|\mathbf{\Lambda}_E^{1/2}\tilde{\mathbf{W}}_{E\bullet 1}\|^2}{\sigma_E^4}\right]}{1+P\lambda_1^T\left(\frac{\|\tilde{\mathbf{W}}_{D\bullet 1}\|^2}{\sigma_D^2} + \frac{\|\tilde{\mathbf{W}}_{E\bullet 1}\|^2}{\sigma_E^2}\right)}\right] + \frac{1}{\sigma_E^2}\mathbb{E}\left[\frac{\frac{P\lambda_1^T}{\sigma_E^2}\|\Lambda_E^{1/2}\tilde{\mathbf{W}}_{E\bullet 1}\|^2}{1+\frac{P\lambda_1^T}{\sigma_E^2}\|\tilde{\mathbf{W}}_{E\bullet 1}\|^2}\right]. \tag{13}$$

Proof: We give a sketch of the proof. Suppose we allocate power $P-p$ to the dominant eigenvalue of $\mathbf{R}_T$ and distribute the rest of the power budget among the remaining eigenvalues so that $\lambda_i^Q = \alpha_i p, i \in \{2,3,\ldots,m_S\}$. The coefficients α_i are all non-negative and sum to one. we denote the secret-key rate achievable in this case $C(p)$. If beamforming is optimal, then we should have $\left.\frac{\partial C(p)}{\partial p}\right|_{p=0} \leq 0$. Maximizing over α_i would give us a necessary condition. Then, showing that $C(p)$ is concave in p implies that the necessary condition is also sufficient. ∎

We illustrate the result of Theorem 2 through the example below.

Example 1. We consider uncorrelated receive and eavesdropper antennas, and assume $\sigma_D^2 = \sigma_E^2 = \sigma^2$. Simplification of the expression of $\mathcal{A}$ yields

$$\mathcal{A} = \frac{1}{\sigma^2}\left(m_D + \alpha - \beta\right), \tag{14}$$

where $\alpha = \mathbb{E}\left[\frac{1}{1+\frac{P\lambda_1^T}{\sigma^2}(\|\mathbf{W}_{D\bullet 1}\|^2+\|\mathbf{W}_{E\bullet 1}\|^2)}\right]$, and $\beta = \mathbb{E}\left[\frac{1}{1+\frac{P\lambda_1^T}{\sigma^2}\|\mathbf{W}_{E\bullet 1}\|^2}\right]$. Clearly, $\mathcal{A} > 0$. Thus, the necessary and sufficient condition for optimality of beamforming becomes

$$\frac{\lambda_2^T}{\sigma^2}\left(m_D + \alpha - \beta\right) - \frac{1}{P}\left(\beta - \alpha\right) \leq 0. \tag{15}$$

Since α involves a chi-squared random variable with $2(m_D+m_E)$ degrees of freedom, we can evaluate α in closed form as

$$\alpha = \left(\frac{\sigma^2}{P\lambda_1^T}\right)^{m_D+m_E} e^{\frac{\sigma^2}{P\lambda_1^T}} \Gamma\left(1-m_D-m_E, \frac{\sigma^2}{P\lambda_1^T}\right), \tag{16}$$

where $\Gamma(a,x) = \int_x^\infty t^{a-1}e^{-t}dt$ is the upper incomplete Gamma function. Similarly, β can be expressed as

$$\beta = \left(\frac{\sigma^2}{P\lambda_1^T}\right)^{m_E} e^{\frac{\sigma^2}{P\lambda_1^T}} \Gamma\left(1-m_E, \frac{\sigma^2}{P\lambda_1^T}\right). \tag{17}$$

In Fig. 1, the region under which beamforming is optimal is shown for $m_D = 4$ and $m_E = 1$. It corresponds to all the points located below the curve. Depending on the particular configuration of the two dominant eigenvalues of the transmit correlation matrix, the transmitter can determine whether beamforming would be optimal or not.

V. Correlation impact on secret-key capacity

In this section, we analyze the impact correlation induces on the secret-key capacity.

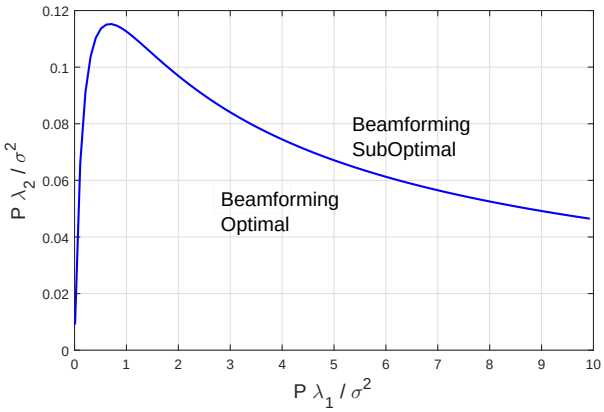

Fig. 1. Necessary and sufficient condition for optimality of beamforming. The destination has 4 antennas and the eavesdropper has a single antenna. Points on this curve satisfy $\frac{P\lambda_1^T}{\sigma^2} \geq \frac{P\lambda_2^T}{\sigma^2}$ and $\lambda_1^T + \lambda_2^T \leq m_S$.

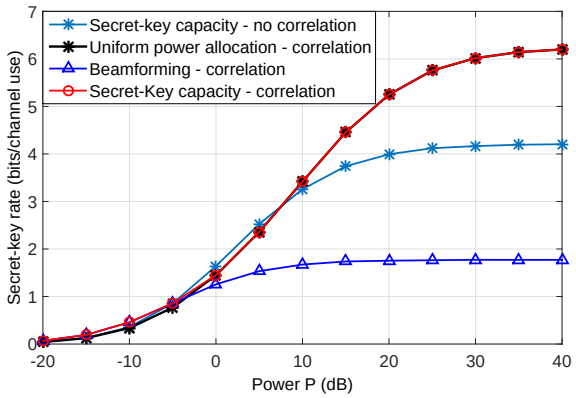

Fig. 2. Impact of combined correlation on secret-key rates. The transmitter, the destination and the eavesdropper are equipped with 2, 3 and 2 antennas, respectively.

A. Impact of transmit correlation

The impact of transmit correlation depends on the operating regime. Indeed, simulations suggest that transmit correlation helps increase the secret-key capacity in the low power regime. However, as the power increases, the beneficial impact of transmit correlation reduces and eventually transmit correlation becomes detrimental. Indeed, in the high power regime, we show later in Proposition 4, that in case of uncorrelated eavesdropper antennas, transmit correlation induces secret-key capacity loss for all configurations of antennas. In [6], it has been shown that for a MISO system without secrecy constraint and with covariance feedback, spatial correlation improves the capacity for any power. As we show in the next section and in Proposition 4, this fact does not hold in presence of a single-antenna eavesdropper.

B. Impact of receive correlation

Receive correlation decreases the secret-key capacity. This is formalized in the following proposition.

Proposition 1. The secret-key capacity of a MIMO system in a correlated environment is largest for uncorrelated receive antennas.

Proof: For fixed $\mathbf{\Lambda}_T$, $\mathbf{\Lambda}_E$ and $\mathbf{\Lambda}_Q$, the secret-key rate function can be shown to be Schur-concave in the eigenvalues of receive correlation matrix. Thus, the largest secret-key rate is achieved with uncorrelated receive antennas. ■

C. Impact of eavesdropper correlation

Unlike receive correlation that is shown to decrease secret-key capacity, we show that eavesdropper correlation increases secret-key capacity. Intuitively, correlation reduces the degrees of freedom gained by the use of multiple antenna by creating a dependency between the observations, henceforth it is plausible that eavesdropper correlation would increase the secret-key capacity. The following proposition establishes the relevance of such intuition.

Proposition 2. The secret-key capacity of a MIMO system with covariance knowledge is the lowest for uncorrelated eavesdropper antennas.

Proof: For fixed $\mathbf{\Lambda}_T$, $\mathbf{\Lambda}_D$ and $\mathbf{\Lambda}_Q$, the secret-key rate function can be shown to be Schur-convexe in the eigenvalues of the eavesdropper correlation matrix. Thus, the minimum secret-key rate is achieved with uncorrelated eavesdropper antennas. ■

Remark 3. Unlike transmit correlation which is beneficial in the low power regime, eavesdropper correlation is helpful regardless of the operating power regime.

Remark 4. We note that the vector $\lambda_E^{max} = \{m_E, 0, \ldots, 0\}$ majorizes every vector in $\Omega_{m_E} = \{\lambda_i \geq 0 \text{ and } \sum_{i=1}^{m_E} \lambda_i = m_E\}$. Hence, it follows from the Schur-convexity property proved in Proposition 2, that the secret-key capacity is highest for fully correlated eavesdropper antennas, i.e., for $\lambda_E = \lambda_E^{max}$. Any permutation of λ_E^{max} achieves likewise the same secret-key rate as the secret-key rate function is symmetric in λ_E.

We now provide numerical simulations illustrating our results.

Example 2. In Fig. 2, we study the combined impact of all correlation matrices. We consider $m_S = 2, m_D = 3$ and $m_E = 2$. The correlation matrices are $\mathbf{\Lambda}_T = \text{diag}[1.7, 0.3], \mathbf{\Lambda}_D = \text{diag}[1.8, 0.9, 0.3]$ and $\mathbf{\Lambda}_E = \text{diag}[1.9, 0.1]$. In the low power regime, we experience a slight gain in secret-key capacity and beamforming is optimal. In the high power, due to eavesdropper correlation, we experience a substantial gain in capacity, that is asymptotically equal to 2 bits per channel use. This gain highlights the beneficial effect of eavesdropper correlation. In general, depending on the eigenvalues' distribution of correlation matrices, one can experience either a gain, or loss or no impact on secret-key capacity in the high-power regime. In the next section, we evaluate analytically this impact on secret-key capacity in the high power regime in terms of system parameters.

VI. High Power Analysis

In this section, we study the impact of correlation matrices on secret-key capacity in the high power regime. For this purpose, we argue that a uniform power allocation strategy is approximately capacity-achieving in the high power regime. The justification of this choice is twofold. First, in case $m_E \geq m_S$, assuming the optimal covariance matrix is of full rank in the high power regime (otherwise one cannot achieve the maximum secret-key multiplexing gain), we show in Proposition 3 that any non-singular covariance matrix achieves the secret-key capacity. In particular, a uniform power allocation strategy is asymptotically optimal. Second, in case $m_E < m_S$, the secret-key capacity scales with P. Determining the optimal input covariance matrix is not straightforward. Based on our simulation results, we observe that uniform power allocation performs comparatively very close to the optimal solution in most configurations. Henceforth, we assume that uniform power allocation is secret-key capacity-achieving in the high power regime.

Proposition 3. If $m_E \geq m_S$, assuming $\mathbf{R}_T$ and $\mathbf{R}_E$ are invertible, the secret-key capacity in the high power regime is given by

$$\lim_{P\to\infty} C(P) = \mathbb{E}\left\{ \frac{\left|W_E^\dagger \mathbf{\Lambda}_E \mathbf{W}_E + \frac{\sigma_E^2}{\sigma_D^2}\mathbf{W}_D^\dagger \mathbf{\Lambda}_D \mathbf{W}_D\right|}{\left|\mathbf{W}_E^\dagger \mathbf{\Lambda}_E \mathbf{W}_E\right|} \right\}. \quad (18)$$

Moreover, it is achieved by any non-singular input covariance matrix.

Proof: $\mathbf{W}_E^\dagger \mathbf{W}_E$ is invertible in this case. After some algebraic manipulations and then taking the limit as $P \to \infty$, one can show that

$$\lim_{P\to\infty} C(\mathbf{\Lambda}_Q) = \mathbb{E}\left[\log\left|\mathbf{I}_{m_S} + \left(\mathbf{W}_E^\dagger \mathbf{\Lambda}_E \mathbf{W}_E\right)^{-1} \frac{\sigma_E^2}{\sigma_D^2}\mathbf{W}_D^\dagger \mathbf{\Lambda}_D \mathbf{W}_D\right|\right],$$

which concludes the result. ∎

We note that (18) generalizes [1, Equation 30]. We study now the impact of correlation matrices. To start with, we consider the case of uncorrelated eavesdropper antennas with correlated transmit and receive antennas. Proposition 4 shows that the secret-key capacity in case of correlation cannot exceed the secret-key capacity in case of no correlation.

Proposition 4. In case of no eavesdropper correlation, the secret-key capacity in the high power regime is upper-bounded by the secret-key capacity in case of no correlation.

Proof: The proof hinges on the fact that for a Hermitian matrix $\mathbf{A}$, the vector of eigenvalues majorizes the vector of diagonal entries. ∎

In the general case, when eavesdropper correlation comes into the picture, its beneficial impact may balance out the detrimental effect of transmit and receive correlation, and we may experience considerable secret-key rate gain as shown in Fig. 2. Assuming non-singular correlation matrices, let $\Delta(P) = C_{\text{uncor}}(P) - C(P)$ denotes the difference between secret-key rate capacities without and with spatial correlation. Using a uniform power allocation strategy to evaluate the secret-key capacity as argued earlier, Theorem 3 characterizes the behavior of $\Delta(P)$ in the high power regime.

Theorem 3. For non-singular correlation matrices, $\mathbf{R}_T, \mathbf{R}_D$ and $\mathbf{R}_E$, we have

$$\lim_{P\to\infty} \Delta(P) = \begin{cases} \mathbb{E}\log\frac{|\mathbf{W}_E^\dagger \mathbf{\Lambda}_E \mathbf{W}_E|}{|\mathbf{W}_E^\dagger \mathbf{W}_E|} - \mathbb{E}\log\frac{|\mathbf{W}^\dagger \mathbf{\Lambda}_{DE} \mathbf{W}|}{|\mathbf{W}^\dagger \mathbf{W}|} \text{ if } m_E \geq m_S \\ -\log|\mathbf{\Lambda}_T| + \log|\mathbf{\Lambda}_E| + \mathbb{E}\log\frac{|\mathbf{W}_E \mathbf{\Lambda}_T \mathbf{W}_E^\dagger|}{|\mathbf{W}_E \mathbf{W}_E^\dagger|} \\ \qquad -\mathbb{E}\log\frac{|\mathbf{W}^\dagger \mathbf{\Lambda}_{DE} \mathbf{W}|}{|\mathbf{W}^\dagger \mathbf{W}|} \text{ if } m_E < m_S \leq m_E + m_D \\ -\log|\mathbf{\Lambda}_D| - \mathbb{E}\log\frac{|\mathbf{W}\mathbf{\Lambda}_T \mathbf{W}^\dagger|}{|\mathbf{W}\mathbf{W}^\dagger|} + \mathbb{E}\log\frac{|\mathbf{W}_E \mathbf{\Lambda}_T \mathbf{W}_E^\dagger|}{|\mathbf{W}_E \mathbf{W}_E^\dagger|} \text{ else.} \end{cases} \quad (19)$$

Proof: As the secret-key capacity can be written as a difference between two rates, one can obtain the difference between secret-key capacities with and without correlation by finding first the corresponding difference of a general MIMO system, then using the result to deduce the secret-key capacities difference. ∎

Theorem 3 quantifies the secret-key rate loss/gain due to correlation in the high power regime.

VII. Conclusions

In this paper, we have studied secret-key agreement of Rayleigh fast-fading MIMO channels in a correlated environment. First, we have derived the expression of the secret-key capacity. Then, we have solved the transmitter optimization problem. In particular, we have shown that transmitting independent Gaussian signals along the eigenvectors of the transmit correlation matrix is optimal. The corresponding power allocated to each channel direction can be determined as the solution to a numerical optimization problem. Next, we have derived a necessary and sufficient condition for beamforming (i.e., transmitting along the strongest channel mode) to be capacity-achieving. In addition, we have analyzed the impact of correlation matrices on secret-key capacity. For instance, we have proved that eavesdropper correlation increases secret-key capacity. Finally, we have investigated the high power regime. We have argued that uniform power allocation is optimal in such regime, and quantified in closed-forms the gain/loss induced by spatial of correlation matrices on the secret-key capacity.

References

[1] T. F. Wong, M. Bloch, and J. M. Shea, "Secret sharing over fast-fading MIMO wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 8, 2009.

[2] E. Jorswieck and H. Boche, "Channel capacity and capacity-range of beamforming in mimo wireless systems under correlated fading with covariance feedback," *IEEE Transactions on Wireless Communications*, vol. 3, no. 5, pp. 1543–1553, Sept 2004.

[3] F. Renna, M. Bloch, and N. Laurenti, "Semi-blind key-agreement over MIMO fading channels," *IEEE Transactions on Communications*, vol. 61, no. 2, pp. 620–627, February 2013.

[4] S. Jafar and A. Goldsmith, "Transmitter optimization and optimality of beamforming for multiple antenna systems," *IEEE Transactions on Wireless Communications*, vol. 3, no. 4, pp. 1165–1175, July 2004.

[5] M. Zorgui, Z. Rezki, B. Alomair, and M.-S. Alouini, "On the diversity-multiplexing tradeoff of secret-key agreement over multiple-antenna channels," in *52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton), 2014*, Sept 2014, pp. 175–182.

[6] E. Jorswieck and H. Boche, "Optimal transmission strategies and impact of correlation in multiantenna systems with different types of channel state information," *IEEE Trans. on Signal Processing*, vol. 52, no. 12, pp. 3440–3453, Dec 2004.