Secret Key Generation from Reciprocal Spatially Correlated MIMO Channels

(Invited Paper)

Eduard A. Jorswieck, Anne Wolf, and Sabrina Engelmann
Communications Laboratory, Department of Electrical Engineering and Information Technology
Technische Universität Dresden, Germany
Email: {eduard.jorswieck, anne.wolf, sabrina.engelmann}@tu-dresden.de

***Abstract*—Secret key generation from reciprocal multi-antenna channels is an interesting alternative to cryptographic key management in wireless systems without infrastructure access. In this work, we study the secret key rate for the basic source model with a MIMO channel. First, we derive an expression for the secret key rate under spatial correlation modelled by the Kronecker model and with spatial precoding at both communication nodes. Next, we analyze the result for uncorrelated antennas to understand the optimal precoding for this special case, which is equal power allocation. Then, the impact of correlation is characterized using Majorization theory. Surprisingly for small SNR, spatial correlation increases the secret key rate. For high SNR, the maximum secret key rate is achieved for uncorrelated antennas. The results indicate that a solid system design for reciprocal MIMO key generation is required to establish the secret key rate gains.**

I. Introduction

Physical layer security recently gained increased attention because it can provide different levels of security without the need for complicated infrastructure or complex cryptographic algorithms [1]. Physical layer security has its roots in information theory. The strongest security measure is perfect information theoretic security already introduced in [2].

Information theoretic security against wire-tapping requires an advantage of the legitimate communication nodes over the eavesdropper. Such an advantage could be to have (or to create) a better effective channel and to apply a wiretap code to confuse the eavesdropper about the remaining information leakage [3]. Recently, a number of results on the characterization of achievable secrecy rates in multi-antenna and multi-carrier scenarios with point-to-point communication as well as achievable secrecy rate regions in multi-user scenarios were derived [4]. Alternatively, this advantage could be that the two legitimate communication nodes possess a source of common randomness [5] that the eavesdropper has not or only partially. The problem of secret key generation from correlated information was first studied in [6] and [7].

Secret keys can be generated from a source of common randomness between the two communication nodes (cf. Figure 1). This could be either a natural source like the communication channel, i.e., its underlying random fading process, or an artificial source like a random sequence transmitted. Having collected the (usually noisy and different) realizations of the common randomness, a public discussion channel is used by the two legitimate nodes to decide on a common secret key [8]. In [9], the case with limited public discussion rates is investigated. Recently, multiple antenna links and the corresponding secrecy and secret key rates are studied [10], [11].

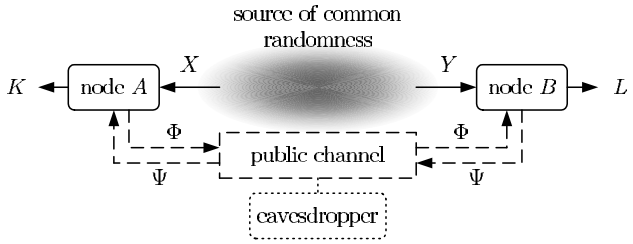


Figure 1. Secret key generation from a source of common randomness.

For the basic source model, where two single-antenna nodes observe channel realizations independently from the eavesdropper from a complex Gaussian distribution in addition to independent white Gaussian noise, the secret key rate is given in [12]. Based on this, practical implementations of channel-based secret key generation schemes were reported, e.g., in [13] for ultrawideband channels and in [14] for MIMO fading channels. In [14], the key generation method is called *Reciprocal Channel Key Generation* (RCKG) because it relies on the reciprocity of the effective channel between the transmitter and the receiver and vice versa. The advantages of using RCKG are listed in [14].

We are interested in the source model with a MIMO channel for secret key generation and the impact of spatial correlation and precoding. For a practical implementation of the RCKG, design guidelines are required, i.e., how to place the antennas, how to precode the signals, and in general which parameters of the propagation environment influence the secret key generation.

The paper is organized as follows: First, we provide some preliminary definitions and results on the secret key rate for the source model. The system model and the channel

The work is partially funded by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 16 KIS 0009, 'Prophylaxe') and by the German Research Foundation (DFG) in the Collaborative Research Center 912 'Highly Adaptive Energy-Efficient Computing.'

model based on the Kronecker correlation model are described. Next, we derive an expression for the secret key rate with precoding under spatial correlation and derive the special cases without precoding and without correlation. Then, we make the following key observations for the system design:

1) Without spatial correlation, the secret key rate is maximized by equal power allocation. Technically speaking this means that the secret key rate is a Schur-concave function of the power allocation vectors.
2) Without precoding, the impact of spatial correlation on the secret key rate depends on the SNR operating point. For small SNR, spatial correlation *increases* the secret key rate. For high SNR, spatial correlation decreases the rate. For intermediate SNR, the behaviour cannot be clearly described.

II. System Model and Preliminaries

A. Secret Key Rates for the Source Model

After the definition of an achievable secret key rate, we review the result on the secret key capacity for the source model from [6], [7]. The noisy versions of the common randomness observed at node A and B are denoted by X and Y, respectively. We use K and L to denote the random key generated by node A and B, respectively. The messages transmitted over the public channel from A to B are denoted by Φ and from B to A by Ψ (see Figure 1).

Definition 1 (Definition 1 in [8])**.** *A secret key rate R_S is achievable if for every $\epsilon > 0$ and sufficiently large n_b, there exists a public communication strategy such that*[1]

$$Pr\{K \neq L\} < \epsilon \tag{1}$$

$$\tfrac{1}{n_b} I(\Phi, \Psi; K) < \epsilon \tag{2}$$

$$\tfrac{1}{n_b} H(K) > R_S - \epsilon \tag{3}$$

$$\tfrac{1}{n_b} \log |\mathcal{K}| < \tfrac{1}{n_b} H(K) + \epsilon. \tag{4}$$

The secret key capacity is then defined as the supremum over all achievable secret key rates.

Theorem 2. *The secret key capacity with unlimited public discussion is*

$$C_S = I(X;Y). \tag{5}$$

Note that in the source model it is assumed that the eavesdropper does not have access to the (correlated) realization of the common random process.

Figure 2 shows a basic source model where two single-antenna nodes observe channel realizations independently from the eavesdropper in addition to independent white Gaussian noise. Assuming a circularly symmetric complex Gaussian distribution with expectation zero and variance P for the channel realizations and circularly symmetric complex Gaussian distributions with expectation zero and variances N_A and N_B for the noise at node A and B, respectively, the secret key rate is given by this simple expression [12, Equation (2)]:

$$I(Y_A; Y_B) = \log\left(1 + \frac{P}{N_A + N_B + \frac{N_A N_B}{P}}\right). \tag{6}$$

[1] All logarithms log are with respect to base two.

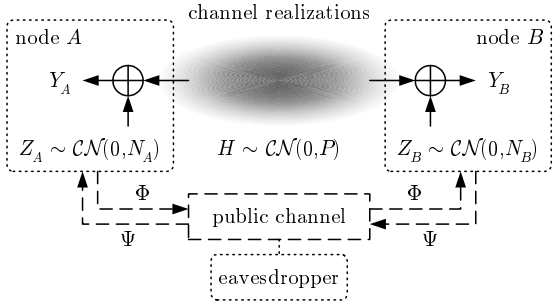


Figure 2. Basic source model with two single-antenna nodes observing channel realizations independently from the eavesdropper.

B. System and Channel Model

We consider the flat-fading MIMO channel model illustrated in Figure 3. Both nodes access the MIMO channel in a time division fashion to probe and estimate its channel state matrix $\boldsymbol{H}$. The random channel matrix[2] is modelled according to the Kronecker model [15], [16], i.e.,

$$\boldsymbol{H} = \boldsymbol{R}_B^{1/2} \boldsymbol{W} \boldsymbol{R}_A^{1/2},$$

where $\boldsymbol{R}_B \succeq 0$ is the spatial correlation matrix at node B, $\boldsymbol{R}_A \succeq 0$ is the spatial correlation matrix at node A, and $\boldsymbol{W}$ is the random multi-path channel matrix with independent and identically circularly symmetric complex Gaussian distributed entries with expectation zero and and variance one. We allow both nodes to apply linear precoding with $\boldsymbol{Q}_A^{1/2}$ at node A and $\boldsymbol{Q}_B^{1/2}$ at node B.

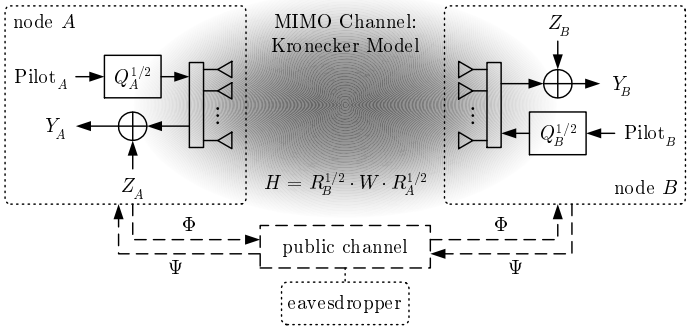


Figure 3. Reciprocal channel key generation in spatially correlated MIMO channels interpreted by the Kronecker model.

The estimated channel matrices at nodes A and B are modelled by

$$\boldsymbol{Y}_B = \boldsymbol{H}\boldsymbol{Q}_A^{1/2} + \boldsymbol{Z}_B \tag{7}$$

$$\boldsymbol{Y}_A = \boldsymbol{Q}_B^{1/2}\boldsymbol{H} + \boldsymbol{Z}_A \tag{8}$$

with the i.i.d. circularly symmetric complex Gaussian noise $\boldsymbol{Z}_A$ and $\boldsymbol{Z}_B$ with expectation zero and variance σ^2. Node B directly estimates $\boldsymbol{Y}_B$, whereas node A observes $\boldsymbol{H}^T\boldsymbol{Q}_B^{1/2} + \boldsymbol{Z}_A$ and computes the transpose to obtain (8).

[2] For simplicity we assume that the number of transmit and receive antennas is equal to n. The generalization to different numbers is possible.

III. Secret Key Rate Results

First, we derive a general expression for the secret key rate for the system model described in Section II-B. Then, we analyze the scenarios without spatial correlation and without precoding.

A. Secret Key Rate Expression

Theorem 3. *The secret key rate for the source model with observations (7) and (8) is given by*

$$\begin{aligned} C_S &= \log\det(\boldsymbol{M}) - \log\det\left(\boldsymbol{M} - \boldsymbol{F}\,\boldsymbol{N}^{-1}\,\boldsymbol{F}\right) \quad \textit{with} \\ \boldsymbol{M} &= \left(\sigma^2\boldsymbol{I} + \boldsymbol{Q}_B^{1/2}\boldsymbol{R}_B\boldsymbol{Q}_B^{1/2} \otimes \boldsymbol{R}_A\right), \\ \boldsymbol{N} &= \left(\sigma^2\boldsymbol{I} + \boldsymbol{R}_B \otimes \boldsymbol{Q}_A^{1/2}\boldsymbol{R}_A\boldsymbol{Q}_A^{1/2}\right), \\ \boldsymbol{F} &= \left(\boldsymbol{R}_B\boldsymbol{Q}_B^{1/2} \otimes \boldsymbol{Q}_A^{1/2}\boldsymbol{R}_A\right). \end{aligned} \tag{9}$$

Proof: First, vectorize the received matrices $\boldsymbol{Y}_A$ and $\boldsymbol{Y_B}$:

$$\boldsymbol{x} = \mathrm{vec}\,(\boldsymbol{Y}_A), \qquad \boldsymbol{y} = \mathrm{vec}\,(\boldsymbol{Y}_B). \tag{10}$$

Note the following second order moments for $\boldsymbol{x}$ and $\boldsymbol{y}$, respectively:

$$\boldsymbol{K}_x = \mathbb{E}\left[\boldsymbol{x}\boldsymbol{x}^H\right] = \left(\boldsymbol{Q}_A^{1/2}\boldsymbol{R}_A\boldsymbol{Q}_A^{1/2} \otimes \boldsymbol{R}_B\right) + \sigma^2\boldsymbol{I} \tag{11}$$

$$\boldsymbol{K}_y = \mathbb{E}\left[\boldsymbol{y}\boldsymbol{y}^H\right] = \left(\boldsymbol{R}_A \otimes \boldsymbol{Q}_B^{1/2}\boldsymbol{R}_B\boldsymbol{Q}_B^{1/2}\right) + \sigma^2\boldsymbol{I}. \tag{12}$$

Also important are the cross-covariance between $\boldsymbol{x}$ and $\boldsymbol{y}$ given by

$$\boldsymbol{K}_{xy} = \mathbb{E}\left[\boldsymbol{x}\boldsymbol{y}^H\right] = \left(\boldsymbol{Q}_A^{1/2}\boldsymbol{R}_A \otimes \boldsymbol{R}_B\boldsymbol{Q}_B^{1/2}\right) \tag{13}$$

and the cross-covariance $\boldsymbol{K}_{yx}$, which can be calculated analogously. Next, we evaluate the mutual information from (5) as follows:

$$I(\boldsymbol{x};\boldsymbol{y}) = h(\boldsymbol{x}) - h(\boldsymbol{x}|\boldsymbol{y}).$$

The first entropy can be easily evaluated. In order to evaluate the second conditional entropy, we apply the following Lemma.

Lemma 4 (see Lemma 1 in [17])**.** *Let $\boldsymbol{U}$ and $\boldsymbol{V}$ be two circularly symmetric Gaussian jointly distributed complex random vectors of dimension n. Let $\boldsymbol{K}_U$, $\boldsymbol{K}_V$, and $\boldsymbol{K}_{UV}$ be the covariance of $\boldsymbol{U}$, covariance of $\boldsymbol{V}$, and cross-covariance of $\boldsymbol{U}$ and $\boldsymbol{V}$, respectively. If $\boldsymbol{K}_V$ is invertible then*

$$h(\boldsymbol{U}|\boldsymbol{V}) = \log\det\left(\boldsymbol{K}_U - \boldsymbol{K}_{UV}\boldsymbol{K}_V^{-1}\boldsymbol{K}_{VU}\right) + n\log(\pi e). \tag{14}$$

We identify $\boldsymbol{U}$ with $\boldsymbol{x}$ and $\boldsymbol{V}$ with $\boldsymbol{y}$ and insert the covariance matrices and the cross-covariance from (11), (12), and (13) into (14) to obtain (9). □

B. Special Case: Uncorrelated Channels

We assume that the channel is spatially uncorrelated, i.e., $\boldsymbol{R}_A = \boldsymbol{R}_B = \boldsymbol{I}$. From the system model in subsection II-B, we observe that the eigenvectors of $\boldsymbol{Q}_A$ and $\boldsymbol{Q}_B$ do not matter since $\boldsymbol{H} = \boldsymbol{W}$ is isotropically distributed. Therefore, we assume $\boldsymbol{Q}_A = \boldsymbol{\Lambda}_A = \mathrm{diag}(\alpha_1, \alpha_2, ..., \alpha_n)$ and $\boldsymbol{Q}_B = \boldsymbol{\Lambda}_B = \mathrm{diag}(\beta_1, \beta_2, ..., \beta_n)$. We write these eigenvalues as vectors $\boldsymbol{\alpha} = [\alpha_1, \alpha_2, ..., \alpha_n]$ and $\boldsymbol{\beta} = [\beta_1, \beta_2, ..., \beta_n]$. W.l.o.g.[3] we set $\sigma^2 = 1$.

Corollary 5. For spatially uncorrelated channels, the secret key rate is given by

$$C_S(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{k=1}^{n}\sum_{l=1}^{n}\log\left(1 + \frac{\alpha_k\beta_l}{1 + \alpha_k + \beta_l}\right). \tag{15}$$

Proof: We evaluate (9) with $\boldsymbol{R}_A = \boldsymbol{R}_B = \boldsymbol{I}$ and obtain

$$C_S = \log\det\left(\tilde{\boldsymbol{M}}\right) - \log\det\left(\tilde{\boldsymbol{M}} - \tilde{\boldsymbol{F}}\,\tilde{\boldsymbol{N}}^{-1}\,\tilde{\boldsymbol{F}}\right) \quad \text{with}$$

$$\begin{aligned} \tilde{\boldsymbol{M}} &= (\boldsymbol{I} + \boldsymbol{Q}_B \otimes \boldsymbol{I}), \\ \tilde{\boldsymbol{N}} &= (\boldsymbol{I} + \boldsymbol{I} \otimes \boldsymbol{Q}_A), \\ \tilde{\boldsymbol{F}} &= \left(\boldsymbol{Q}_A^{1/2} \otimes \boldsymbol{Q}_B^{1/2}\right), \end{aligned}$$

which can be transformed into

$$\begin{aligned} C_S(\boldsymbol{Q}_A, \boldsymbol{Q}_B) = &\log\det(\boldsymbol{I} + \boldsymbol{Q}_B \otimes \boldsymbol{I}) \\ &- \log\det\left(\boldsymbol{I} + \boldsymbol{Q}_B \otimes (\boldsymbol{I} - [\boldsymbol{I} + \boldsymbol{Q}_A^{-1}]^{-1})\right). \end{aligned}$$

Then we insert the diagonal $\boldsymbol{Q}_A = \boldsymbol{\Lambda}_A$ and $\boldsymbol{Q}_B = \boldsymbol{\Lambda}_B$ and observe that the eigenvalues of the Kronecker product $\boldsymbol{\Lambda}_A \otimes \boldsymbol{\Lambda}_B$ are $\alpha_1\beta_1, ..., \alpha_1\beta_n, \alpha_2\beta_1, ..., \alpha_2\beta_n, ...\alpha_n\beta_n$ [18, Theorem 13.12]. We obtain

$$\begin{aligned} C_S(\boldsymbol{\alpha}, \boldsymbol{\beta}) &= \sum_{k=1}^{n}\sum_{l=1}^{n}\log\left(\frac{1 + \beta_k}{1 + \beta_k - \frac{\beta_k}{1 + \frac{1}{\alpha_l}}}\right) \\ &= \sum_{k=1}^{n}\sum_{l=1}^{n}\log\left(1 + \frac{\alpha_k\beta_l}{1 + \alpha_k + \beta_l}\right). \end{aligned}$$

□

The function $C_S(\boldsymbol{\alpha}, \boldsymbol{\beta})$ can be further analyzed using Majorization theory [16]. We need the following definition to proceed.

Definition 6 (Definition 2.1 in [16])**.** *For two vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$ with descending ordered components $x_1 \geq x_2 \geq ... \geq x_n \geq 0$ and $y_1 \geq y_2 \geq ... \geq y_n \geq 0$, one says that the vector $\boldsymbol{x}$ majorizes the vector $\boldsymbol{y}$ and writes*

$$\begin{aligned} \boldsymbol{x} \succeq \boldsymbol{y} \quad \textit{if} \quad &\sum_{k=1}^{m} x_k \geq \sum_{k=1}^{m} y_k, \quad m = 1, ..., n-1 \\ \textit{and} \quad &\sum_{k=1}^{n} x_k = \sum_{k=1}^{n} y_k. \end{aligned} \tag{16}$$

An order preserving function on the majorization order is called Schur-convex or Schur-concave function.

Definition 7 (Definition 2.6 in [16])**.** *A real-valued function ϕ defined on $\mathbb{R}^n$ is said to be Schur-convex if for all*

$$\boldsymbol{x} \succeq \boldsymbol{y} \quad \Rightarrow \quad \phi(\boldsymbol{x}) \geq \phi(\boldsymbol{y}). \tag{17}$$

Similarly, ϕ is called Schur-concave if $-\phi$ is Schur-convex.

Corollary 8. For spatially uncorrelated fading, the secret key rate C_S as a function of the linear precoding coefficients $\boldsymbol{\alpha}$ and

[3] The noise variance σ^2 can be transformed in the linear precoding matrices $\boldsymbol{Q}_A^{1/2}$ and $\boldsymbol{Q}_B^{1/2}$.

$\boldsymbol{\beta}$ is Schur-concave. The maximum secret key rate is achieved for equal power allocation at both nodes A and B.

Proof: The proof relies on a basic result on Schur-convex functions:

Lemma 9 (3.C.1 in [19])**.** *If $g : \mathbb{R} \to \mathbb{R}$ is convex and twice differentiable, then*

$$\phi(\boldsymbol{x}) = \sum_{k=1}^{n} g(x_k)$$

is Schur-convex.

The statement in Corollary 8 follows then by the second derivative of $C_S(\boldsymbol{\alpha}, \boldsymbol{\beta})$ with respect to α_k or β_l. □

Remark. For the practical system design, this implies that equal power allocation $\boldsymbol{Q}_A = \frac{P}{n}\boldsymbol{I} = \boldsymbol{Q}_B$ maximizes the secret key rate for a spatially uncorrelated Rayleigh fading MIMO channel.

Compared to the secret key rate in (6), the advantages of the multiple antennas are illustrated in the following: Using equal power allocation, the secret key rate is[4]

$$C_S(n) = n^2 \log\left(1 + \frac{P^2/n}{n + 2P}\right). \tag{18}$$

If the number of antennas grows, the secret key rate approaches the following limit

$$\lim_{n\to\infty} C_S(n) = \frac{P^2}{\ln(2)}. \tag{19}$$

This scaling behaviour is illustrated in Figure 4.

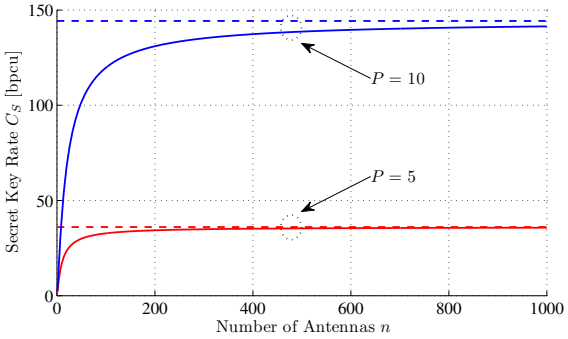


Figure 4. Secret key rate scaling with number of antennas.

C. Special Case: Without Precoding

Here, we consider the special case in which $\boldsymbol{Q}_A = \boldsymbol{Q}_B = \frac{P}{n}\boldsymbol{I}$. We define the overall correlation matrix $\boldsymbol{K} = \boldsymbol{R}_B \otimes \boldsymbol{R}_A$ and the inverse SNR $\rho = \frac{\sigma^2 n}{P}$.

Corollary 10. Without precoding, the secret key rate is given by

$$C_S(\boldsymbol{\lambda}) = \sum_{k=1}^{n^2} \log\left(1 + \frac{\lambda_k^2}{\rho(\rho + 2\lambda_k)}\right), \tag{20}$$

[4]Compared to the representation in (6), (18) can be transformed into

$$C_S(n) = n^2 \log\left(1 + \frac{P/n}{\frac{N_A N_B}{P/n} + N_A + N_B}\right).$$

where $\boldsymbol{\lambda} = [\lambda_1, ..., \lambda_{n^2}]$ is the vector that contains the eigenvalues of the large correlation matrix $\boldsymbol{K}$, i.e., $\boldsymbol{\lambda} = [\alpha_1\beta_1, \alpha_1\beta_2, ..., \alpha_1\beta_n, \alpha_2\beta_1, ..., \alpha_n\beta_n]$.

Proof: We insert the large correlation matrix and equal power allocation into the secret key rate in (9)

$$\begin{aligned} C_S(\boldsymbol{K}) &= \log\det(\rho\,\boldsymbol{I} + \boldsymbol{K}) \\ &\quad - \log\det\left(\rho\,\boldsymbol{I} + \boldsymbol{K} - \boldsymbol{K}[\rho\,\boldsymbol{I} + \boldsymbol{K}]^{-1}\boldsymbol{K}\right) \\ &= \sum_{k=1}^{n^2}\left(\log(\rho + \lambda_k) - \log\left(\frac{(\rho + \lambda_k)^2 - \lambda_k^2}{\rho + \lambda_k}\right)\right) \\ &= \sum_{k=1}^{n^2} \log\left(1 + \frac{\lambda_k^2}{\rho\,(\rho + 2\lambda_k)}\right). \end{aligned} \tag{21}$$

□

Interestingly, there is not a clear behaviour of the secret key rate in (21) with respect to the vector $\boldsymbol{\lambda}$. However, for small SNR, the secret key rate becomes Schur-convex as the following result shows.

Corollary 11. For all SNR $= \frac{P}{\sigma^2 n} \leq \sqrt{1/2} \approx 1.5$ dB, the function $C_S(\boldsymbol{\lambda})$ is Schur-convex and the maximum secret key rate is achieved for $\boldsymbol{\lambda} = [1, 0, ..., 0]$.

Proof: For all $\rho \geq \sqrt{2}$, the second derivative of the term $\log(1 + \frac{x}{\rho(\rho+2x)})$ is non-negative. Therefore, the function in the sum is convex and Lemma 9 can be applied. □

Remark. Note that the impact of the correlation matrices $\boldsymbol{R}_A$ and $\boldsymbol{R}_B$ is different than the impact of the precoding matrices $\boldsymbol{Q}_A$ and $\boldsymbol{Q}_B$ for secret key rate. This is in contrast to the transmission rates for MIMO systems where the transmit correlation matrix $\boldsymbol{R}_A$ has the same impact as the transmit precoding matrix $\boldsymbol{Q}_A$.

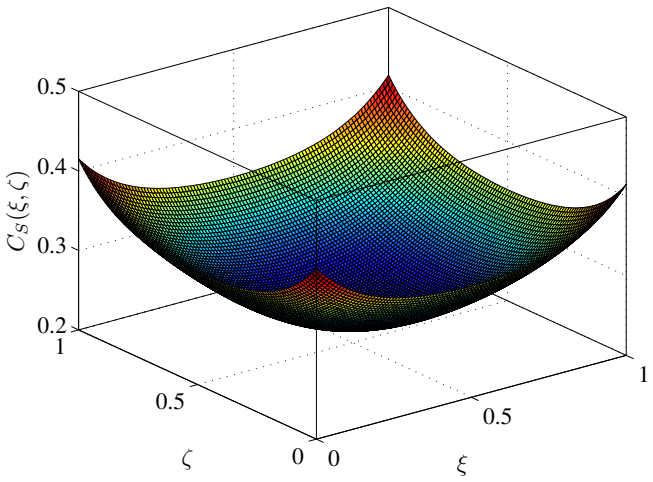
Remark. The important practical design guideline in Corollary 11 is that for small SNR, a completely correlated channel gives higher secret key rates than an uncorrelated channel. This behaviour is different to the rate of a MIMO system without precoding: The average rate is a Schur-concave function for all SNR and spatial correlation always decreases rate [16].

In Figure 5, the case with $n = 2$ transmit and receive antennas is studied. Denote the two eigenvalues of $\boldsymbol{R}_A$ by $(1 - \xi)$ and ξ and the two eigenvalues of $\boldsymbol{R}_B$ by $(1 - \zeta)$ and ζ. Then $\boldsymbol{K}$ has the eigenvalues

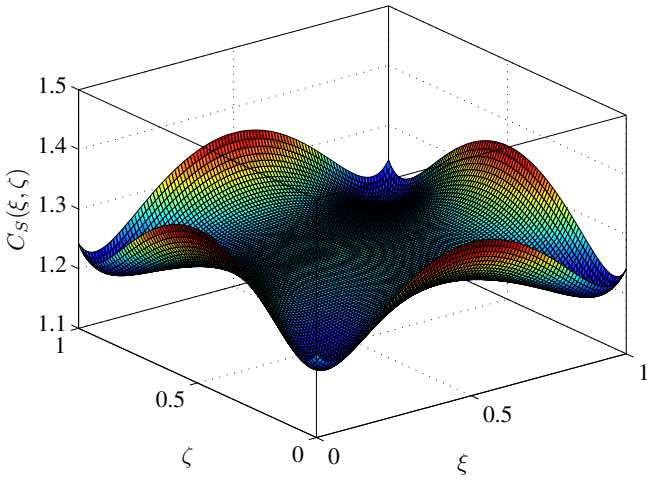
$$\boldsymbol{\lambda} = [(1 - \xi)(1 - \zeta), (1 - \xi)\zeta, \xi(1 - \zeta), \xi\zeta].$$

The function in Figure 5 is plotted over these ξ and ζ from the intervals $[0, 1]$, i.e., the function $C_S(\xi, \zeta)$. The cases $\xi = 1$ and $\xi = 0$ correspond to completely correlated transmit antennas at node A and the case $\xi = 1/2$ corresponds to completely uncorrelated transmit antennas at node A. The same holds analogously for node B.

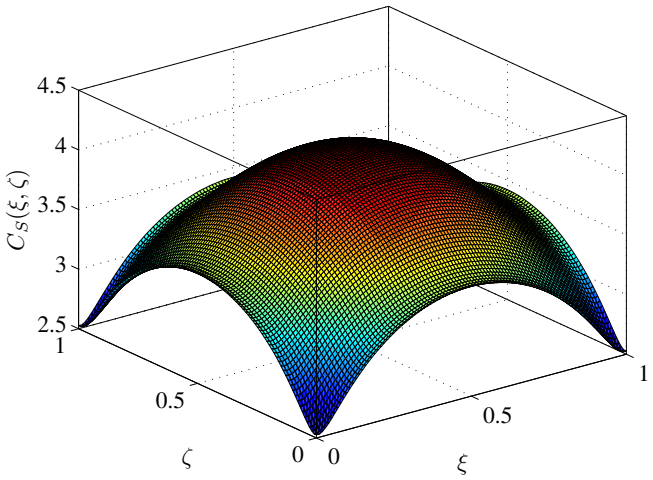
In Figure 5, the changing behaviour of the secret key rate as a function of spatial correlation can be observed. As predicted by Corollary 11 for low SNR (below 1.5 dB) the function is Schur-convex and the maximum secret key rate is achieved for completely correlated channels (e.g., $\xi = 1$, $\zeta = 1$), the minimum secret key rate is achieved for uncorrelated channels, i.e., $\xi = 1/2$, $\zeta = 1/2$. This is illustrated in Figure 5(a). In



(a) SNR $= 0$ dB



(b) SNR $= 5$ dB



(c) SNR $= 10$ dB

Figure 5. Impact of spatial correlation on the secret key rate for $n = 2$ antennas and low, medium, and high SNR.

Figure 5(b), the intermediate SNR scenario is shown. Here, no clear behaviour in terms of Schur-convexity and Schur-concavity can be observed. For higher SNR, Figure 5(c) suggests that the function becomes Schur-concave. However, this is not true in general because for very small correlation values (the points close to the axes) the function is not monotonic. If one is just interested in the maximum secret key rate, the conclusion for high SNR is that it is achieved for uncorrelated antennas at both nodes A and B.

IV. Conclusion

Secret key generation from reciprocal MIMO channels is a promising technique to establish information theoretic confidential data transmission without key management infrastructure support. We show that the fading statistic of the MIMO channel has an important impact on the secret key rate for a simple source model with a MIMO channel. A careful positioning and precoding of the antenna systems at both nodes is required to obtain high secret key generation rates.

For future work, the non-trivial extension to the scenario in which the eavesdropper obtains a correlated observation of the MIMO channel is studied. The results from the current paper will serve as an upper bound to the achievable secret key rates for the MIMO channel model.

References

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[2] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*, ser. Foundations and Trends in Communications and Information Theory. now publishers, vol. 5, no. 4–5, pp. 355–580, 2009.

[5] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, 2000.

[6] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[7] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography—part i: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[8] L. Lai, Y. Liang, H. V. Poor, and W. Du, *Physical Layer Security in Wireless Communications*. CRC Press, Boca Raton, FL, 2013, ch. Key Generation From Wireless Channels.

[9] S. Watanabe and Y. Oohama, "Secret Key Agreement From Vector Gaussian Sources by Rate Limited Public Communication," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 541–550, 2011.

[10] 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, 2013.

[11] E. A. Jorswieck, R. Mochaourab, and K. M. Ho, *Physical Layer Security in Wireless Communications*. CRC Press, Boca Raton, FL, 2013, ch. Game Theory for Physical Layer Security on Multi-Antenna Interference Channels.

[12] C. Ye, A. Reznik, and Y. Shah, "Extracting Secrecy from Jointly Gaussian Random Variables," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Seattle, USA, 2006.

[13] R. Wilson, D. Tse, and R. A. Scholtz, "Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, 2007.

[14] J. W. Wallace and R. K. Sharma, "Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 381–392, 2010.

[15] C.-N. Chuah, D. N. C. Tse, J. M. Kahn, and R. A. Valenzuela, "Capacity scaling in MIMO wireless systems under correlated fading," *IEEE Transactions on Information Theory*, vol. 48, no. 3, pp. 637–650, 2002.

[16] E. A. Jorswieck and H. Boche, *Majorization and Matrix-Monotone Functions in Wireless Communications*, ser. Foundations and Trends in Communications and Information Theory. now publishers, vol. 3, no. 6, pp. 553–701, 2007.

[17] T. F. Wong, M. Bloch, and J. M. Shea, "Secret Sharing over Fast-Fading MIMO Wiretap Channels," *EURASIP Journal on Wireless Communications and Networking*, Article ID 506973, 2009.

[18] A. J. Laub, *Matrix Analysis for Scientists and Engineers*. SIAM, 2004.

[19] A. W. Marshall, I. Olkin, and B. C. Arnold, *Inequalities: Theory of Majorization and its Applications*. Springer Series in Statistics, 2011.