PRECODING FOR SECRET KEY GENERATION IN MULTIPLE ANTENNA CHANNELS WITH STATISTICAL CHANNEL STATE INFORMATION

Sabrina Engelmann, Anne Wolf, and Eduard A. Jorswieck

Communications Theory, Communications Laboratory
Department of Electrical Engineering and Information Technology
Technische Universität Dresden, Germany
Email: {sabrina.engelmann, anne.wolf, eduard.jorswieck}@tu-dresden.de

ABSTRACT

In future wireless communication systems, more and more small low-power mobile devices will communicate without infrastructure and internet access. In order to provide a lightweight yet powerful security mechanism, physical layer parameters can be used to generate secret keys for perfect secrecy. In this paper, we study the optimal operation of a multiple antenna link with statistical channel state information at all nodes for secret key generation. The impact of spatial correlation on the achievable secret key rates is characterized. Furthermore, the optimal pilot precoding during channel estimation is computed. Numerical simulations illustrate the results for selected scenarios.

1. INTRODUCTION

Secret key generation on the physical layer is an interesting and promising approach to solve the problem of key exchange in cryptography. The corresponding theory was first introduced by [1] and [2]. On the physical layer, the secret keys can be generated from a source of common randomness between two legitimate communication partners [3]. If an eavesdropper has no access to a (correlated) realization of the random process, the scenario is called source model [4]. The reconciliation of the generated keys at both partners occurs over a public channel of infinite capacity [5].

One possible source of common randomness is the fading process of the communication channel between the partners. For the single-antenna case with complex Gaussian channel realizations and independent Gaussian noise, the secret key rate was computed in [6]. Recently, the case of secret key agreement in multiple-antenna (MIMO) channels was investigated [7]. In [8], secret key generation in spatially correlated MIMO channels was studied.

In this paper, we investigate the key generation from a reciprocal and spatially correlated channel for the special case where only one partner has multiple antennas and all nodes have only statistical channel state information on the communication link. Contributions of this paper are:

- We present a closed form solution for the optimal pilot precoding during the channel estimation phase.
- We provide results for the impact of spatial correlation of the channel on the achievable secret key rate.

This work was funded by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 16 KIS 0009, Prophylaxe). The authors alone are responsible for the content of the paper.

This work is supported in part by the German Research Foundation (DFG) in the Collaborative Research Center 912 "Highly Adaptive Energy-Efficient Computing".

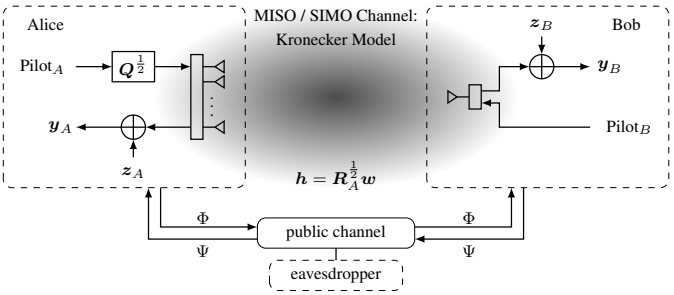

Fig. 1. Key generation from a reciprocal and spatially correlated MISO / SIMO channel.

2. PRELIMINARIES

2.1. System and Channel Model

We investigate the secret key generation in a source model with two legitimate communication partners, Alice and Bob (Figure 1). Their source of common randomness is the block flat-fading channel between them. We assume that Alice has n_T antennas, whereas Bob has only one single antenna. Therefore, we have a MISO channel for the transmission from Alice to Bob and a SIMO channel for the transmission from Bob to Alice. The spatial correlation of the channel is modeled with the Kronecker model. The random channel vector is given by

$$\boldsymbol{h} = \boldsymbol{R}_A^{\frac{1}{2}}\boldsymbol{w},$$

where $\boldsymbol{R}_A \succeq 0$ is an $(n_T \times n_T)$ spatial correlation matrix at Alice and $\boldsymbol{w}$ is an $(n_T \times 1)$ multi-path channel vector with independent and identically distributed (i.i.d.) entries which are circularly symmetric complex Gaussian with zero mean and variance 1. The channel estimation is done in $n_T + 1$ time slots. Alice uses n_T time slots with n_T different precoding vectors, which we write as the columns of the linear precoding matrix $\boldsymbol{Q}$, to allow channel estimation at Bob. Afterwards, Bob sends his pilot in one time slot with power p and Alice estimates the channel. The resulting receive vectors at Bob and Alice are given by

$$\boldsymbol{y}_B = \boldsymbol{Q}^{\frac{1}{2}}\boldsymbol{h} + \boldsymbol{z}_B \quad \text{and} \quad \boldsymbol{y}_A = \sqrt{p}\boldsymbol{h} + \boldsymbol{z}_A, \tag{1}$$

respectively, where $\boldsymbol{z}_A$ and $\boldsymbol{z}_B$ are complex $(n_T \times 1)$ noise vectors with i.i.d. circularly symmetric complex Gaussian entries with zero mean and variance σ_n^2, $n \in \{A, B\}$. The random variables $\boldsymbol{w}$,

$\boldsymbol{z}_A$, and $\boldsymbol{z}_B$ are modeled statistically independent. $\boldsymbol{Q}$ is a positive semi-definite $(n_T \times n_T)$ matrix. Furthermore, we have the power constraints $\mathrm{tr}\,(\boldsymbol{Q}) \leq P_A$ at Alice and $p \leq P_B$ at Bob. Alice and Bob have only statistical information about the channel state, i.e., the correlation matrix $\boldsymbol{R}_A$ is known to them. We assume that the eavesdropper has no access to the (correlated) channel realizations.

2.2. Secret Key Generation for the Source Model

Alice and Bob generate the keys K and L, which are from the set $\mathcal{K}$. The reconciliation of the keys occurs over a public channel of infinite capacity, where the public message from Alice to Bob is denoted by Φ and the public messages from Bob to Alice by Ψ.

Definition 1 (Definition 1 in [5])**.** *A secret key rate R_{SK} is achievable if for every $\epsilon > 0$ and sufficiently large block length n, there exists a public communication strategy such that*

$$\begin{aligned} Pr\left[K \neq L\right] &< \epsilon, \\ \tfrac{1}{n}\mathrm{I}\left(\Phi, \Psi; K\right) &< \epsilon, \\ \tfrac{1}{n}\mathrm{H}\left(K\right) &< R_{SK} - \epsilon, \quad \textit{and} \\ \tfrac{1}{n}\log_2\left|\mathcal{K}\right| &< \tfrac{1}{n}\mathrm{H}\left(K\right) + \epsilon. \end{aligned}$$

The secret key capacity in the source model with unlimited public discussion is defined as the supremum over all achievable secret key rates and is given by [3, Corollary 4.1]

$$C_{SK} = \mathrm{I}\left(\boldsymbol{y}_A; \boldsymbol{y}_B\right). \tag{2}$$

3. OPTIMAL PRECODING FOR KEY GENERATION

With the receive vectors in (1), we can compute the covariance and cross covariance matrices

$$\begin{aligned} K_{\boldsymbol{y}_B} &= \mathbb{E}\left[\boldsymbol{y}_B \boldsymbol{y}_B^H\right] = \boldsymbol{Q}^{\frac{1}{2}} \boldsymbol{R}_A \boldsymbol{Q}^{\frac{1}{2}} + \sigma_B^2 \boldsymbol{I}, \\ K_{\boldsymbol{y}_A} &= \mathbb{E}\left[\boldsymbol{y}_A \boldsymbol{y}_A^H\right] = p\boldsymbol{R}_A + \sigma_A^2 \boldsymbol{I}, \quad \text{and} \\ K_{\boldsymbol{y}_B \boldsymbol{y}_A^H} &= \mathbb{E}\left[\boldsymbol{y}_B \boldsymbol{y}_A^H\right] = \boldsymbol{Q}^{\frac{1}{2}} \boldsymbol{R}_A \sqrt{p}. \end{aligned}$$

Thus, an achievable secret key rate for the system model in Section 2.1 can be calculated evaluating (2) as

$$\begin{aligned} R_{SK}(p, \boldsymbol{Q}) &= \log_2 \det\left(\boldsymbol{Q}^{\frac{1}{2}} \boldsymbol{R}_A \boldsymbol{Q}^{\frac{1}{2}} + \sigma_B^2 \boldsymbol{I}\right) \\ &- \log_2 \det\left(\boldsymbol{Q}^{\frac{1}{2}} \boldsymbol{R}_A^{\frac{1}{2}} \left[\boldsymbol{I} + \tfrac{p}{\sigma_A^2}\boldsymbol{R}_A\right]^{-1} \boldsymbol{R}_A^{\frac{1}{2}} \boldsymbol{Q}^{\frac{1}{2}} + \sigma_B^2 \boldsymbol{I}\right). \end{aligned} \tag{3}$$

We consider the optimization problem

$$R_{SK}^{\text{opt}} = \max_{\substack{\boldsymbol{Q} \succeq 0,\ \mathrm{tr}(\boldsymbol{Q}) \leq P_A, \\ 0 \leq p \leq P_B}} R_{SK}(p, \boldsymbol{Q}).$$

Obviously, the optimal power allocation at Bob has to minimize the second term in (3) and is given by $p = P_B$, i.e., we choose the power as high as possible, and the optimization problem reduces to

$$R_{SK}^{\text{opt}} = \max_{\boldsymbol{Q} \succeq 0,\ \mathrm{tr}(\boldsymbol{Q}) \leq P_A} R_{SK}(P_B, \boldsymbol{Q}). \tag{4}$$

Lemma 2. *The optimization problem in* (4) *is a convex problem with respect to the precoding matrix $\boldsymbol{Q}$.*

The constraints in (4) describe a convex set. Additionally, we rewrite (3) in (4) as

$$\begin{aligned} R_{SK}(P_B, \boldsymbol{Q}) = &\log_2 \det\left(\boldsymbol{I} + \tfrac{1}{\sigma_B^2}\boldsymbol{R}_A^{\frac{1}{2}} \boldsymbol{Q} \boldsymbol{R}_A^{\frac{1}{2}}\right) \\ &- \log_2 \det\left(\boldsymbol{I} + \tfrac{1}{\sigma_B^2}\boldsymbol{R}_B^{\frac{1}{2}} \boldsymbol{Q} \boldsymbol{R}_B^{\frac{1}{2}}\right) \end{aligned}$$

with $\boldsymbol{R}_B = \boldsymbol{R}_A^{\frac{1}{2}} \left[\boldsymbol{I} + \frac{P_B}{\sigma_A^2}\boldsymbol{R}_A\right]^{-1} \boldsymbol{R}_A^{\frac{1}{2}}$.

We introduce the representation $\boldsymbol{R}_B^{\frac{1}{2}} = \boldsymbol{D}\boldsymbol{R}_A^{\frac{1}{2}}$. The matrix $\boldsymbol{I} - \boldsymbol{D}\boldsymbol{D}^H$ is positive semi-definite, since it has only non-negative eigenvalues of the form $1 - \frac{1}{1+(P_B/\sigma_A^2)\lambda_k}$, where λ_k is the k-th eigenvalue of $\boldsymbol{R}_A$. Therefore, we can apply [9, Lemma C.1] and conclude that R_{SK} is concave in $\boldsymbol{Q}$. Consequently, the optimization problem in (4) is a convex problem.

Remark. *The calculation of the MIMO secrecy capacity under an average power constraint leads to a similar objective function and optimization problem. This was independently solved in [10], [11].*

3.1. Optimal Precoding for Known Correlation

Theorem 3. *Let the spatial correlation of the antennas $\boldsymbol{R}_A$ be known by Alice. The eigenvectors of the optimal precoding matrix $\boldsymbol{Q}$ for the optimization problem in* (4) *diagonalize the spatial correlation matrix $\boldsymbol{R}_A$, i.e.,*

$$\boldsymbol{U}_{\boldsymbol{Q}} = \boldsymbol{U}_{\boldsymbol{R}_A}$$

with the eigenvalue decompositions $\boldsymbol{Q} = \boldsymbol{U}_{\boldsymbol{Q}}^H \boldsymbol{\Lambda}_{\boldsymbol{Q}} \boldsymbol{U}_{\boldsymbol{Q}}$ and $\boldsymbol{R}_A = \boldsymbol{U}_{\boldsymbol{R}_A}^H \boldsymbol{\Lambda}_{\boldsymbol{R}_A} \boldsymbol{U}_{\boldsymbol{R}_A}$. The eigenvalue matrix $\boldsymbol{\Lambda}_{\boldsymbol{Q}} = \mathrm{diag}\left(q_1, \ldots, q_{n_T}\right)$ of the optimal precoding matrix $\boldsymbol{Q}$ is given by the power allocation

$$\begin{aligned} q_k(\mu) = \Bigg[&- \tfrac{\sigma_A^2 \sigma_B^2 + \lambda_k\left(\sigma_B^2 P_B + \sigma_A^2\right)}{2\lambda_k\left(\sigma_A^2 + \lambda_k \sigma_B^2\right)} \\ &+ \sqrt{\tfrac{P_B^2 \sigma_B^4}{4\sigma_A^4}\left(1 + \tfrac{P_B \lambda_k}{\sigma_A^2}\right) + \tfrac{P_B \sigma_B^2}{\mu \log 2 \sigma_A^2}} \Bigg]^+, \end{aligned}$$

where λ_k, $k \in \{1, \ldots, n_T\}$, are the eigenvalues of the spatial correlation matrix $\boldsymbol{R}_A$. The waterfilling level $\mu > 0$ is chosen such that

$$\sum_{k=1}^{n_T} q_k(\mu) = P_A.$$

We use the notation $\boldsymbol{q}$ and $\boldsymbol{\lambda}$ for the vectors of the eigenvalues q_k und λ_k, $k \in \{1, \ldots, n_T\}$, of the precoding matrix $\boldsymbol{Q}$ and the spatial correlation matrix $\boldsymbol{R}_A$, respectively.

Proof. The proof is given in two steps. First, we show that the optimal $\boldsymbol{Q}$ has the same eigenvectors as $\boldsymbol{R}_A$. Then we give the optimal power allocation derived with the necessary Karush-Kuhn-Tucker (KKT) conditions.

First step: Due to the concavity of the secret key rate R_{SK} (Lemma 2) and the fact that the matrices $\boldsymbol{R}_A$ and $\boldsymbol{R}_B$ commute, i.e., both matrices have the same eigenvectors, we can apply the same transformation approach as used in the proof of [12, Theorem 5] to obtain

$$R_{SK}^{\text{opt}} = \max_{\substack{q_k \geq 0 \\ \sum_{k=1}^{n_T} q_k \leq P_A}} R_{SK}(\boldsymbol{q}) \quad \text{with} \tag{5}$$

$$R_{SK}(\boldsymbol{q}) = \sum_{k=1}^{n_T} \left(\log_2 \left(1 + \frac{1}{\sigma_B^2} \lambda_k q_k \right) - \log_2 \left(1 + \frac{1}{\sigma_B^2} \frac{\lambda_k}{1 + \frac{P_B}{\sigma_A^2} \lambda_k} q_k \right) \right).$$

Second step: We rewrite the secret key rate in (5) to get

$$R_{SK}(\boldsymbol{q}) = \sum_{k=1}^{n_T} \left(\log_2 \left(1 + \frac{P_B \lambda_k}{\sigma_A^2} + \left(\frac{\lambda_k}{\sigma_B^2} + \frac{P_B \lambda_k^2}{\sigma_A^2 \sigma_B^2} \right) q_k \right) - \log_2 \left(1 + \frac{P_B \lambda_k}{\sigma_A^2} + \frac{\lambda_k}{\sigma_B^2} q_k \right) \right).$$

For convenience, we set

$$\sigma_k^2 = 1 + \frac{P_B \lambda_k}{\sigma_A^2}, \quad \alpha_k = \frac{\lambda_k}{\sigma_B^2} + \frac{P_B \lambda_k^2}{\sigma_A^2 \sigma_B^2}, \quad \text{and} \quad \beta_k = \frac{\lambda_k}{\sigma_B^2}.$$

The above secret key rate has the form

$$R_{SK}(\boldsymbol{q}) = \sum_{k=1}^{n_T} \log_2 \left(\frac{\sigma_k^2 + \alpha_k q_k}{\sigma_k^2 + \beta_k q_k} \right). \tag{6}$$

The secret key rate R_{SK} in (6) is concave in $\boldsymbol{q}$, since the Hessian matrix with respect to $\boldsymbol{q}$ is diagonal with only non-positive diagonal entries

$$\frac{\partial^2 R_{SK}(\boldsymbol{q})}{\partial q_k^2} = \sum_{k=1}^{n_T} \frac{\sigma_k^4 \left(\beta_k^2 - \alpha_k^2 \right) + 2\alpha_k \beta_k \sigma_k^2 q_k \left(\beta_k - \alpha_k \right)}{\left(\alpha_k q_k + \sigma_k^2 \right)^2 \left(\beta_k q_k + \sigma_k^2 \right)^2 \log 2}$$

and, consequently, negative semi-definite. Note, that with $\alpha_k = \beta_k + \frac{P_B \lambda_k^2}{\sigma_A^2 \sigma_B^2}$ we have $\alpha_k \geq \beta_k$. Hence, the KKT conditions are necessary and sufficient. We solve the optimization problem using the Lagrangian function

$$L\left(\boldsymbol{q}, \mu, \boldsymbol{\nu}\right) = C_{SK}(\boldsymbol{q}) + \sum_{k=1}^{n_T} q_k \nu_k + \mu \left(P_A - \sum_{k=1}^{n_T} q_k \right).$$

Taking the first derivative of the Langrangian function with respect to q_k, the power allocation satisfies

$$\frac{\sigma_k^2 \left(\alpha_k - \beta_k \right)}{\log 2 \left(\sigma_k^2 + \alpha_k q_k \right) \left(\sigma_k^2 + \beta_k q_k \right)} = \mu - \nu_k \tag{7}$$

with $\nu_k q_k = 0$ and $\mu > 0$. The left-hand-side of the equation is always positive, as $\alpha_k \geq \beta_k$, and therefore we have $q_k > 0$ always fulfilled, i.e., $\nu_k = 0$. If we resubstitute α_k, β_k and σ_k^2 into (7), and solve the equation for q_k, we obtain the result in Theorem 3.

The secret key rate R_{SK} in (6) is monotonically increasing in each q_k, which follows from the non-negativity of the first derivative of R_{SK} with respect to q_k. Thus, the power constraint at Alice has to be fulfilled with equality. □

3.2. Special Case: No Spatial Correlation

For the case, where we have no spatial correlation between the channels, i.e., $\boldsymbol{R}_A = \boldsymbol{I}$, the secret key rate is given by

$$R_{SK}\left(\boldsymbol{q}\right) = \sum_{k=1}^{n_T} \log_2 \left(1 + \frac{P_B \sigma_B^2 q_k}{\sigma_B^2 \left(\sigma_B^2 \sigma_A^2 + P_B \sigma_B^2 + q_k \sigma_A^2 \right)} \right).$$

The secret key rate R_{SK} is symmetric and concave in $\boldsymbol{q}$ and therefore, R_{SK} is Schur-concave [13, Proposition 2.8] and the maximum is achieved for equal power allocation $\boldsymbol{q} = \frac{P_A}{n_T} \mathbb{1} \preceq \boldsymbol{q}$ for any $\boldsymbol{q}$, where $\mathbb{1}$ is an $(n_T \times 1)$ vector with all elements being 1. Without loss of generality, we can set $\sigma_A^2 = \sigma_B^2 = 1$ and obtain the maximum secret key rate

$$R_{SK}\left(\tfrac{P_A}{n_T} \mathbb{1} \right) = n_T \log_2 \left(1 + \frac{P_B \frac{P_A}{n_T}}{1 + P_B + \frac{P_A}{n_T}} \right). \tag{8}$$

Corollary 4. *For a growing number of antennas, the secret key rate* R_{SK} *in* (8) *approaches*

$$\lim_{n_T \to \infty} R_{SK}\left(\tfrac{P_A}{n_T} \mathbb{1} \right) = \frac{P_A P_B}{(P_B + 1) \log 2}.$$

3.3. Special Case: Without Precoding

We can analyze the influence of the spatial correlation at Alice, if we omit the precoding and set $\boldsymbol{Q} = \frac{P_A}{n_T} \boldsymbol{I}$. With equal power allocation, the secret key rate is given by

$$R_{SK}(\boldsymbol{\lambda}) = \sum_{k=1}^{n_T} \log_2 \left(1 + \frac{\lambda_k^2}{\frac{\sigma_A^2}{P_B} \frac{\sigma_B^2 n_T}{P_A} + \frac{\sigma_B^2 n_T}{P_A} \lambda_k + \frac{\sigma_A^2}{P_B} \lambda_k} \right).$$

If we choose P_A and P_B such that the inverted SNR at Alice and Bob is equalized, i.e., $\frac{\sigma_B^2 n_T}{P_A} = \frac{\sigma_A^2}{P_B} =: \rho$, we obtain the secret key rate

$$R_{SK}(\boldsymbol{\lambda}) = \sum_{k=1}^{n_T} \log_2 \left(1 + \frac{\lambda_k^2}{\rho \left(\rho + 2\lambda_k \right)} \right).$$

We can observe the same behavior as in [8]: For all SNR $\rho^{-1} \leq \sqrt{1/2} \approx 1.5$ dB, the secret key rate $R_{SK}(\boldsymbol{\lambda})$ is Schur-convex and the maximum secret key rate is achieved for $\boldsymbol{\lambda} = [n_T, 0, ..., 0]$. This means, that for small SNR, the secret key rate is higher if the channel is completely correlated. For high SNR, the secret key rate decreases with increasing correlation, even though we cannot prove the formal statement of Schur-concavity.

4. NUMERICAL RESULTS

In this section, we illustrate the performance of the optimal power allocation (OPA) given in Theorem 3 compared to an equal power allocation (EPA) scheme. For all simulations, we set $\sigma_A^2 = \sigma_B^2 = 1$ and the power at Bob is fixed to $P_B = 10$. The spatial correlation matrix $\boldsymbol{R}_A$ is a Toeplitz matrix with elements $\xi^{|i-j|}$, i.e., it has the form

$$\boldsymbol{R}_A = \begin{pmatrix} 1 & \xi & \cdots & \xi^{n_T-2} & \xi^{n_T-1} \\ \xi & 1 & \xi & \cdots & \xi^{n_T-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \xi^{n_T-2} & \cdots & \xi & 1 & \xi \\ \xi^{n_T-1} & \xi^{n_T-2} & \cdots & \xi & 1 \end{pmatrix}$$

with $0 \leq \xi \leq 1$ being the level of spatial correlation between the antennas, where $\xi = 0$ represents no correlation and $\xi = 1$ the complete correlation.

In Figure 2, the two-antenna case is presented.We compare the secret key rates R_{SK} over the SNR for the cases of almost complete correlation, i.e., $\xi = 0.9$, and no correlation, i.e., $\xi = 0$. For the case of no correlation (solid curve with triangles), the power is allocated

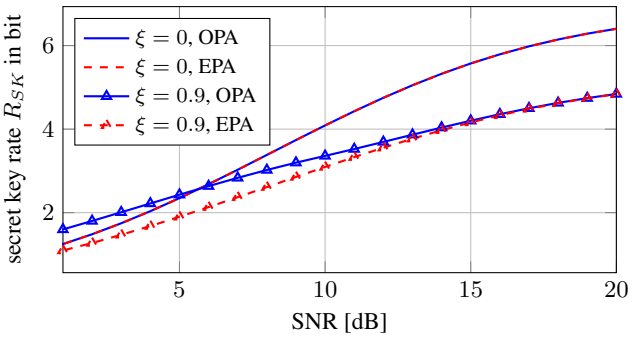

Fig. 2. Secret key rate over SNR for $n_T = 2$ transmit antennas at Alice with different levels of correlation and fixed power $P_B = 10$ at Bob.

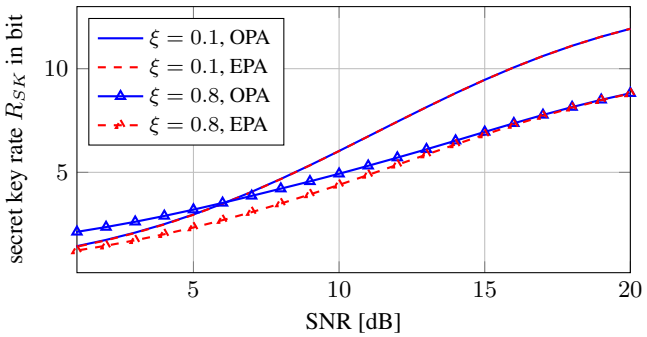

Fig. 3. Secret key rate over SNR for $n_T = 4$ transmit antennas at Alice with different levels of correlation and fixed power $P_B = 10$ at Bob.

equally, as described in Section 3.2. If the antennas are correlated, we need to apply the result from Theorem 3 in order to generate an optimal pilot precoding. For the low SNR regime, the resulting secret key rate with OPA (solid curve) is superior to the rate achieved by EPA (dashed curve) and even better than the rate for uncorrelated antennas. In the high SNR regime, the secret key rate achieved by OPA approaches the rate achieved by EPA, while we gain a much better rate without correlation.

The case with four antennas is presented in Figure 3. We compare the secret key rates for $\xi = 0.1$ and $\xi = 0.8$ achieved by EPA and OPA. We can observe a similar behavior to the one found in the two-antenna case. If the antennas are spatially correlated, the OPA scheme (solid curves) performs better in the low SNR regime than the EPA scheme (dashed curves). If there is almost no correlation, i.e., $\xi = 0.1$, the optimal power allocation tends to the equal power allocation.

This behavior can be seen again in Figure 4 for $n_T = 8$ transmit antennas and small values of ξ, i.e., a low level of spatial correlation.

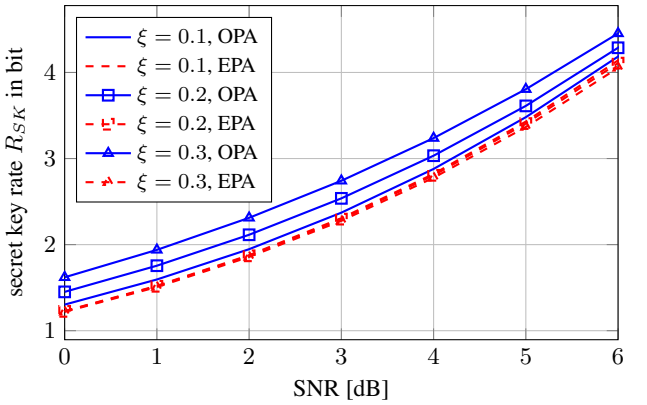

Fig. 4. Secret key rate over SNR for $n_T = 8$ transmit antennas at Alice with different levels of correlation and fixed power $P_B = 10$ at Bob.

5. REFERENCES

[1] 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.

[2] 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.

[3] M. Bloch and J. Barros, *Physical-Layer Security*, First Edit. Cambridge University Press, 2011.

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

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

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

[7] 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.

[8] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret Key Generation from Reciprocal Spatially Correlated MIMO Channels," in *Proc. of IEEE Global Communications Conference (GLOBECOM)*, 2013.

[9] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound Wiretap Channels," *EURASIP Journal on Wireless Communications and Networking*, 2009, Article ID 142374.

[10] S. A. A. Fakoorian and A. L. Swindlehurst, "Full Rank Solutions for the MIMO Gaussian Wiretap Channel With an Average Power Constraint," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2620–2631,

[11] S. Loyka and C. D. Charalambous, "On Optimal Signaling over Secure MIMO Channels," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, 2012, pp. 443–447.

[12] A. Wolf and E. A. Jorswieck, "Maximization of Worst-Case Secret Key Rates in MIMO Systems with Eavesdropper," in *Proc. of IEEE Global Communications Conference (GLOBECOM)*, 2011.

[13] E. A. Jorswieck and H. Boche, "Majorization and Matrix Monotone Functions in Wireless Communications," Foundations and Trends in Communications and Information Theory, vol. 3, no. 6, S. Verdu, Ed., pp. 553–701, 2007.