On the Relationship Between the Multi-antenna Secrecy Communications and Cognitive Radio Communications

Lan Zhang, Rui Zhang, Ying-Chang Liang, Yan Xin, and Shuguang Cui

Abstract

This paper studies the capacity of the multi-antenna or multiple-input multiple-output (MIMO) secrecy channels with multiple eavesdroppers having single/multiple antennas. It is known that the MIMO secrecy capacity is achievable with the optimal transmit covariance matrix that maximizes the minimum difference between the channel mutual information of the secrecy user and those of the eavesdroppers. The MIMO secrecy capacity computation can thus be formulated as a non-convex max-min problem, which cannot be solved efficiently by standard convex optimization techniques. To handle this difficulty, we explore a relationship between the MIMO secrecy channel and the recently developed MIMO cognitive radio (CR) channel, in which the multi-antenna secondary user transmits over the same spectrum simultaneously with multiple primary users having single/multiple antennas, subject to the received interference power constraints at the primary users, or the so-called "interference temperature (IT)" constraints. By constructing an auxiliary CR MIMO channel that has the same channel responses as the MIMO secrecy channel, we prove that the optimal transmit covariance matrix to achieve the secrecy capacity is the same as that to achieve the CR spectrum sharing capacity with properly selected IT constraints under certain conditions. Based on this relationship, several algorithms are proposed to solve the non-convex secrecy capacity computation problem by transforming it into a sequence of CR spectrum sharing capacity computation problems that are convex. For the case with single-antenna eavesdroppers, the proposed algorithms obtain the exact capacity of the MIMO secrecy channel, while for the case with multi-antenna eavesdroppers, the proposed algorithms obtain both upper and lower bounds on the MIMO secrecy capacity.

L. Zhang is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 118622 (email: zhanglan@nus.edu.sg).

R. Zhang and Y.-C. Liang are with the Institute for Infocomm Research, A*STAR, Singapore (emails: {rzhang, ycliang}@i2r.a-star.edu.sg).

Y. Xin is with the NEC Laboratories America, Princeton, New Jersey, USA (email: yanxin@nec-labs.com).

S. Cui is with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, Texas, USA (email: cui@ece.tamu.edu).

Index Terms

Cognitive radio, convex optimization, CR spectrum sharing capacity, interference temperature, multi-antenna systems, secrecy capacity.

I. Introduction

In the 1970s, Wyner introduced a secrecy transmission model in his seminal work [1] on information-theoretic secrecy. In this model, the secrecy transmitter sends confidential messages to a legitimate receiver subject to the requirement that the messages cannot be decoded by an eavesdropper. The information-theoretic study of the secrecy transmission problem has been continued and extended to many other channel models, including broadcast channels (BCs) [2], [3], multiple access channels (MACs) [4], [5], and interference channels (ICs) [6], [7]. Very recently, the secrecy capacity of the multi-antenna/multiple-input multiple-output (MIMO) channel has been characterized by Khisti and Wornell [8], and Oggier and Hassibi [9]. In their work, the MIMO secrecy channel with a single eavesdropper having multiple antennas is transformed into a degraded MIMO-BC, whose capacity is an upper bound on the secrecy capacity. It was shown in [8], [9] that this capacity upper bound is indeed tight for the Gaussian noise case, i.e., the exact secrecy capacity. However, this computable secrecy capacity cannot be extended to the general case of multiple eavesdroppers. Moreover, Liu and Shammai [10] also established the MIMO secrecy capacity by using the channel enhancement technique [11]. However, no computable characterization of the secrecy capacity was provided in [10].

On the other hand, cognitive radio is considered as an efficient technology to dramatically improve spectrum utilization, thus having great potential to solve spectrum scarcity problem. In a spectrum-sharing CR system, the CR user or the so-called secondary user (SU) is allowed to simultaneously transmit with the licensed primary user (PU) over the same spectrum, provided that the SU to PU interference level is regulated below a predefined threshold, which is also called the "interference temperature (IT)" constraint. The capacity achieving transmission problems under the IT constraint for the secondary users have been studied in [12], [13], and [14] for the CR MIMO point-to-point channel, the CR MIMO-MAC, and the CR MIMO-BC, respectively. Since the IT constraint is a linear function of the transmit covariance matrix, the capacity characterization problem for the CR MIMO channel can be formulated as a convex optimization problem, and is thus solvable via the standard interior point method [12]. It is worth noting that the system models of the secrecy channel and the CR channel are fairly similar in the sense that the secrecy and SU transmitters need to regulate the resultant signal power level at the eavesdropper and PU, respectively, so as to achieve the goals of confidential transmission and PU protection, respectively.

In this paper, we study the capacity computation problem for the general case of the MIMO secrecy channel with multiple eavesdroppers having single/multiple antennas. Based on the results in [8], [9], the related MIMO secrecy capacity can be obtained via optimizing over the transmit covariance matrix of the secrecy user to maximize the minimum difference between the mutual information of the secrecy channel and those of the channels from the secrecy transmitter to different eavesdroppers. It can thus be shown that the resulting capacity computation problem is a non-convex max-min optimization problem, which cannot be solved efficiently with standard convex optimization techniques. To handle this difficulty, we consider an auxiliary CR MIMO channel with multiple PUs having single/multiple antennas and the same channel responses as those in the MIMO secrecy problem. We next establish a relationship between this auxiliary CR MIMO channel and the MIMO secrecy channel by proving that the optimal transmit covariance matrix for the secrecy channel is the same as that for the CR channel with properly selected IT constraints for the PUs under certain conditions. Based on such a relationship, we transform the non-convex MIMO secrecy capacity computation problem into a sequence of CR capacity computation problems, which are convex and thus can be efficiently solved. For the case of single-antenna eavesdroppers, the proposed algorithms obtain the exact capacity of the associated MIMO secrecy channel, while for the case of multi-antenna eavesdroppers, the proposed algorithms obtain both the upper and lower bounds on the MIMO secrecy capacity.

The rest of this paper is organized as follows. Section II presents the system models and problem formulations for the CR MIMO transmission and the secrecy MIMO transmission. Section III describes the main theoretical results of this paper on the relationship between the secrecy capacity and the CR spectrum sharing capacity. Section IV studies the case of single-antenna eavesdroppers, and develops several algorithms to compute the MIMO secrecy capacity. Section V extends the results to the case of multi-antenna eavesdroppers to obtain the upper and lower bounds on the MIMO secrecy capacity. Section VI presents some numerical examples. Finally, Section VII concludes the paper.

Notation: Uppercase boldface and lowercase boldface letters are used to denote matrices and vectors, respectively. $(\boldsymbol{S})^H$, $\mathrm{tr}(\boldsymbol{S})$, and $|\boldsymbol{S}|$ denote the conjugate transpose, the trace, and the determinant of a matrix $\boldsymbol{S}$, respectively. $\mathcal{R}^K$ denotes the vector space of $K \times 1$ real vectors, and $\mathcal{R}$ denotes the field of real numbers. $\boldsymbol{I}$ denotes an identity matrix. $\mathbb{E}[\cdot]$ denotes statistical expectation. $|\cdot|$ denotes the absolute value of a complex number.

II. System Model and Problem Formulation

In this section, we present system models and problem formulations for the CR MIMO transmission and the secrecy MIMO transmission in the following two subsections, respectively.

A. CR MIMO Transmission

As shown in Fig. 1(a), we consider a CR MIMO channel, where the SU transmitter (SU-Tx) is equipped with N transmit antennas, and the SU receiver (SU-Rx) is equipped with M receive antennas. The SU-Tx to SU-Rx channel is denoted by a $N \times M$ matrix $\boldsymbol{H}_s$. Moreover, there are K single-antenna PU receivers denoted by PU$_i$, $i = 1, \cdots, K$, and the channel from SU-Tx to PU$_i$ is denoted by the $N \times 1$ vector $\boldsymbol{h}_i$. The received signal $\boldsymbol{y}$ at SU-Rx is expressed as

$$\boldsymbol{y} = \boldsymbol{H}_s^H \boldsymbol{x} + \boldsymbol{z} \tag{1}$$

where $\boldsymbol{x}$ is the transmit signal vector at SU-Tx, and $\boldsymbol{z}$ denotes the noise vector at SU-Rx. The entries of the noise vector are independent circularly symmetric complex Gaussian (CSCG) random variables of zero mean and covariance matrix $\boldsymbol{I}$. Since the SU shares the same spectrum with the PUs, there are K IT constraints imposed to the SU transmission, expressed as $\mathbb{E}[|\boldsymbol{h}_i^H \boldsymbol{x}|^2] \le \Gamma_i, i = 1, \cdots, K$, where Γ_i denotes the tolerable IT limit for PU$_i$.

Consider the CR MIMO transmission problem, in which we determine the optimal transmit covariance matrix for SU-Tx to maximize the data rate subject to the transmit power constraint and the IT constraints for the K PUs. Mathematically, this problem can be formulated as [12]

$$\begin{aligned} (\mathbf{PA}): \quad & \max_{\boldsymbol{S}} \ \log |\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S} \boldsymbol{H}_s| \\ & \text{subject to: } \operatorname{tr}(\boldsymbol{S}) \le P \\ & \qquad \boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i \le \Gamma_i, \ i = 1, \cdots, K \end{aligned}$$

where $\boldsymbol{S} = \mathbb{E}[\boldsymbol{x}\boldsymbol{x}^H]$ denotes the transmit covariance matrix at SU-Tx, and P denotes the transmit power constraint. Note that $\boldsymbol{S}$ is a positive semi-definite matrix such that $(\mathbf{PA})$ is a convex problem and can be solved efficiently by the standard interior point method [15].

B. Secrecy MIMO Transmission

As shown in Fig. 1(b), we consider a MIMO secrecy channel, where the secrecy transmitter (SC-Tx) is equipped with N transmit antennas, and the secrecy receiver (SC-Rx) is equipped with M receive antennas. Moreover, there are K single-antenna eavesdroppers. In accordance with the earlier introduced

CR MIMO channel, the channel response from SC-Tx to SC-Rx is denoted by $\boldsymbol{H}_s$, and the channel response from SC-Tx to the ith eavesdropper (EA$_i$) is denoted by $\boldsymbol{h}_i, i = 1, \cdots, K$. According to the secrecy requirement, the transmitted message W from SC-Tx should not be decoded by any of the eavesdroppers, i.e., $H(W|y_i) \geq r, \forall i$, with y_i denoting the received signal at EA$_i$, and r denoting the secrecy transmit rate. According to the results in [8], [9], the secrecy capacity can be obtained by solving the following optimization problem

$$(\mathbf{PB}): \quad \max_{\boldsymbol{S}} \ \min_{i} \ \log|\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S} \boldsymbol{H}_s| - \log\left(1 + \frac{\boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i}{\sigma_i^2}\right)$$

$$\text{subject to: } \mathrm{tr}(\boldsymbol{S}) \leq P$$

where $\boldsymbol{S}$ denotes the transmit covariance matrix of SC-Tx, similar to that of SU-Tx in the CR case, and σ_i^2 denotes the variance of the zero-mean CSCG noise at EA$_i$.

We see that $(\mathbf{PB})$ is a non-convex optimization problem since its objective function is the difference between two concave functions of $\boldsymbol{S}$ and thus not necessarily concave. Existing methods in the literature [8], [9], [16], [17] for the MIMO secrecy capacity computation is only applicable to the case of a single eavesdropper. However, these methods cannot solve the case with multiple eavesdroppers $(\mathbf{PB})$ even for the case where each eavesdropper has a single antenna[1].

Remark 1: According to Fig. 1, it is easy to observe that the system models of the CR transmission and the secrecy transmission bear the similarity that they both need to control the received signal power levels at both PUs and eavesdroppers. However, note that $(\mathbf{PA})$ guarantees that the interference power at each PU receiver is below the required threshold without considering the PU noise power, while for $(\mathbf{PB})$, through the second term in the objective function, the confidential level at each eavesdropper is not only related to the received signal power from SC-Tx, but also related to the noise power at eavesdroppers. Therefore, one immediate question is whether there exists a relationship between these two systems such that we can solve the non-convex problem $(\mathbf{PB})$ by transforming it into some form of $(\mathbf{PA})$ that is convex and thus efficiently solvable. With this motivation, we first study the relationship between these two problems, and then propose corresponding algorithms to solve $(\mathbf{PB})$.

III. Relationship Between Secrecy Capacity and CR Spectrum Sharing Capacity

In this section, we present main theoretical results of the paper on the relationship between the secrecy capacity computation problem $(\mathbf{PB})$ and the CR spectrum sharing capacity computation problem $(\mathbf{PA})$.

[1]Problem $(\mathbf{PB})$ in the case of multi-antenna eavesdroppers will be studied later in Section V.

While the developed relationship applies to both single-antenna and multi-antenna CR/secrecy channels, we are particularly interested in the multi-antenna case since it provides a general guidance for solving $(\mathbf{PB})$.

Proposition 1: For a given $(\mathbf{PB})$, there exists a set of IT constraint values, Γ_i, $i = 1, \cdots, K$, such that the resulting $(\mathbf{PA})$ has the same solution as that of $(\mathbf{PB})$.

Proof: Please refer to Appendix A. ■

Proposition 1 establishes the relationship between $(\mathbf{PA})$ and $(\mathbf{PB})$. To further investigate this relationship, we define an auxiliary function of Γ_is as

$$\begin{aligned} g(\Gamma_1, \cdots, \Gamma_K) := \max_{\boldsymbol{S}} \ & |\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S} \boldsymbol{H}_s| \\ \text{subject to: } & \text{tr}(\boldsymbol{S}) \leq P \\ & \boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i \leq \Gamma_i, i = 1, \cdots, K. \end{aligned} \tag{2}$$

Note that the only difference between Problem (2) and $(\mathbf{PA})$ is that the objective function in Problem (2) does not involve a logarithmic function of matrix determinant while that in (PA) does. As a result, Problem (2) is non-convex since its objective function is not concave in $\boldsymbol{S}$. Also note that Problem (2) is equivalent to $(\mathbf{PA})$ since they have the same optimal solution for $\boldsymbol{S}$. Therefore, although Problem (2) is non-convex, its optimal solution can be obtained via solving the convex counterpart $(\mathbf{PA})$.

Proposition 2: $(\mathbf{PB})$ is equivalent to the following optimization problem:

$$\max_{\Gamma_1, \cdots, \Gamma_K} \min_i \ F_i(\Gamma_1, \cdots, \Gamma_K) := \frac{g(\Gamma_1, \cdots, \Gamma_K)}{1 + \Gamma_i / \sigma_i^2}. \tag{3}$$

Proof: Please refer to Appendix B. ■

Proposition 2 establishes the relationship between $(\mathbf{PB})$ and the auxiliary function $g(\Gamma_1, \cdots, \Gamma_K)$ that is related to $(\mathbf{PA})$. The equivalence between Problem (3) and $(\mathbf{PB})$ means that by solving the optimal Γ_is in Problem (3), we could solve an optimal $\boldsymbol{S}$ given $g(\Gamma_1, \cdots, \Gamma_K)$ is an embedded optimization problem over $\boldsymbol{S}$ inside Problem (3). Such an optimal $\boldsymbol{S}$ is also the solution for $(\mathbf{PB})$, for which the explanation is given in Appendix B.

Problem (3) can be solved by utilizing an important property of $g(\Gamma_1, \cdots, \Gamma_K)$ described as follows:

Proposition 3: The function $g(\Gamma_1, \cdots, \Gamma_K)$ is a concave function with respect to $\Gamma_1, \cdots, \Gamma_K$, and

$$\gamma_i(\Gamma_1, \cdots, \Gamma_K) := \frac{\partial g(\Gamma_1, \cdots, \Gamma_K)}{\partial \Gamma_i} = \mu_i^{(1)} |\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S}^{(1)} \boldsymbol{H}_s|, \ i = 1, \cdots, K \tag{4}$$

where $\boldsymbol{S}^{(1)}$ and $\mu_i^{(1)}$ are the optimal solution of $(\mathbf{PA})$ and the corresponding Lagrange multiplier (the dual solution) with respect to the ith IT constraint, respectively.

Proof: Please refer to Appendix C. ■

Note that from Proposition 3, it follows that the gradient of $g(\Gamma_1, \cdots, \Gamma_K)$ in (3) can be obtained by solving $(\mathbf{PA})$ via the Lagrange duality method, which completes the equivalence between $(\mathbf{PA})$ and $(\mathbf{PB})$ via the intermediate problem (3). At last, we have

Proposition 4: Problem (3) is a quasi-concave maximization problem.

Proof: Please refer to Appendix D. ■

Proposition 4 suggests that Problem (3) can be solved by utilizing convex optimization techniques, for which the details are given in the next section.

IV. Algorithms

In this section, we present the algorithms to compute the MIMO secrecy capacity by exploiting the relationship between the secrecy transmission and the CR transmission developed in Section III. The algorithm for the general case of the MIMO secrecy channel with multiple eavesdroppers is presented first. Two reduced-complexity algorithms are next presented, one for the special case with one single eavesdropper, and the other for the special case with a single-antenna secrecy receiver, i.e., the multiple-input single-output (MISO) secrecy channel.

A. General Case

In this subsection, we present the algorithm for $(\mathbf{PB})$ in the general case of MIMO secrecy channels with multiple eavesdroppers. According to Propositions 2 and 4, $(\mathbf{PB})$ is equivalent to the quasi-concave maximization problem (3). Thus, we instead study Problem (3) since it is easier to handle than $(\mathbf{PB})$.

According to [15], a quasi-concave maximization problem can be reduced to solving a sequence of convex feasibility problems. Thus, Problem (3) can be further transformed as

$$\begin{aligned} &\max_{t, \Gamma_1, \cdots, \Gamma_K} \; t \\ &\text{subject to} : g(\Gamma_1, \cdots, \Gamma_K) \geq t(1 + \Gamma_i/\sigma_i^2), i = 1, \cdots, K. \end{aligned} \tag{5}$$

Let t^* be the optimal solution of Problem (5). Clearly, t^* is also the optimal value of Problem (3). If the feasibility problem

$$\begin{aligned} &\max_{\Gamma_1, \cdots, \Gamma_K} \; 0 \\ &\text{subject to} : g(\Gamma_1, \cdots, \Gamma_K) \geq t(1 + \Gamma_i/\sigma_i^2), i = 1, \cdots, K \end{aligned} \tag{6}$$

for a given t is feasible, then it follows that $t^* \geq t$. Conversely, if Problem (6) is infeasible, then $t^* < t$. Therefore, by assuming an interval $[\ 0,\ \bar{t}\ ]$ known to contain the optimal t^*, the optimal solution of

Problem (5) can be found easily via a bisection search. Note that a suitable value for $\bar{t}$ can be chosen as $g(\infty, \cdots, \infty)$ from (2).

We next solve the feasibility problem (6) by a similar method discussed in [18]. It is worth noting that the feasibility problem (6) can be viewed as an optimization problem. The Lagrangian of Problem (6) can be written as

$$L_0(\{\nu_i\}, \Gamma_1, \cdots, \Gamma_K) = \sum_{i=1}^{K} \nu_i \Big(g(\Gamma_1, \cdots, \Gamma_K) - t(1 + \Gamma_i/\sigma_i^2) \Big) \tag{7}$$

where ν_i is the non-negative dual variable for the ith constraint, and $\{\nu_i\}$ denotes $\nu_1, \cdots, \nu_K$. The corresponding dual function is then defined as

$$f_0(\{\nu_i\}) = \max_{\Gamma_1, \cdots, \Gamma_K} \sum_{i=1}^{K} \nu_i \Big(g(\Gamma_1, \cdots, \Gamma_K) - t(1 + \Gamma_i/\sigma_i^2) \Big). \tag{8}$$

Due to its convexity, Problem (6) can be transformed into its equivalent dual problem as

$$\min_{\{\nu_i\}} \; f_0(\{\nu_i\}) \tag{9}$$

and the duality gap between the optimal values of Problem (6) and Problem (9) is zero if Problem (6) is feasible.

Since it is known from Proposition 3 that function $g(\Gamma_1, \cdots, \Gamma_K)$ is concave with respect to $\{\Gamma_1, \cdots, \Gamma_K\}$, Problem (8) can be solved via a gradient-based algorithm. According to Proposition 3, the gradient of function $g(\Gamma_1, \cdots, \Gamma_K)$ can be obtained by solving $(\mathbf{PA})$. Furthermore, since function $f_0(\{\nu_i\})$ is convex with respect to $\{\nu_i\}$, Problem (9) can be solved by a subgradient-based algorithm, such as the ellipsoid method [15]. Similar to Lemma 3.5 in [18], Problem (6) is infeasible if and only if there exist $\{\nu_i\}$ such that $f_0(\{\nu_i\}) < 0$. Using this fact along with the subgradient-based search over $\{\nu_i\}$, the feasibility problem (6) can be solved. In summary, the algorithm for Problem (3) with a target accuracy parameter ϵ is listed as follows:

Algorithm 1:

- Initialization: $t^{\min} = 0, t^{\max} = \bar{t}$.
- Repeat
  - $t \leftarrow \frac{1}{2}(t^{\min} + t^{\max})$.
  - Solve the feasibility problem (6). If Problem (6) is feasible, $t^{\min} \leftarrow t$; otherwise, $t^{\max} \leftarrow t$.
  - Stop, when $t^{\max} - t^{\min} \leq \epsilon$.
- The optimal value of Problem (3) is taken as $t^{\min}$.

B. Single-Eavesdropper Case

We now consider a special case of $(\mathbf{PB})$, where there is only one single eavesdropper in the secrecy channel, and propose a simplified algorithm over Algorithm 1 for the corresponding $(\mathbf{PB})$.

Consider first the counterpart CR transmission problem $(\mathbf{PA})$. For the single-PU case, $(\mathbf{PA})$ can be rewritten as

$$(\mathbf{PC}): \quad \max_{\boldsymbol{S}} \ \log|\boldsymbol{I}+\boldsymbol{H}_s^H\boldsymbol{S}\boldsymbol{H}_s|$$
$$\text{subject to: } \mathrm{tr}(\boldsymbol{S}) \leq P$$
$$\boldsymbol{h}^H\boldsymbol{S}\boldsymbol{h} \leq \Gamma$$

where $\boldsymbol{h}$ denotes the channel from SU-Tx to the single PU, and Γ is the corresponding IT limit for the PU. On the other hand, for the single-eavesdropper case, the secrecy transmission problem $(\mathbf{PB})$ can be rewritten as

$$(\mathbf{PD}): \quad \max_{\boldsymbol{S}} \ \log|\boldsymbol{I}+\boldsymbol{H}_s^H\boldsymbol{S}\boldsymbol{H}_s| - \log\left(1+\frac{\boldsymbol{h}^H\boldsymbol{S}\boldsymbol{h}}{\sigma^2}\right)$$
$$\text{subject to: } \mathrm{tr}(\boldsymbol{S}) \leq P$$

where $\boldsymbol{h}$ denotes the channel from SC-Tx to the single eavesdropper, and σ^2 denotes the variance of the noise at the eavesdropper. Following Proposition 2, $(\mathbf{PD})$ is equivalent to the optimization problem

$$\max_{\Gamma} \ F(\Gamma) := \frac{g(\Gamma)}{1+\Gamma/\sigma^2} \tag{10}$$

where the function $g(\Gamma)$ is the single-PU counterpart of that in (2). Moreover, it is evident from Proposition 4 that function $F(\Gamma)$ is quasi-concave and the optimization problem (10) is a quasi-concave maximization problem.

Lemma 1: The sufficient and necessary condition for Γ^* to be the optimal solution of Problem (10) is

$$\gamma(\Gamma^*)(1+\Gamma^*/\sigma^2) = \frac{1}{\sigma^2}g(\Gamma^*) \tag{11}$$

where $\gamma(\Gamma) := \frac{\partial g(\Gamma)}{\partial \Gamma}$.

Proof: Please refer to Appendix E. ■

Based on Lemma 1, $(\mathbf{PD})$ can be solved via the equivalent problem (10) by the bisection method summarized as follows:

Algorithm 2:

- Initialization: $\Gamma^{\min} = 0, \Gamma^{\max} = \bar{\Gamma}$.

- Repeat
  - $\Gamma \leftarrow \frac{1}{2}(\Gamma^{\min} + \Gamma^{\max})$.
  - Solve Problem (2) for the single-PU case, and compute $\gamma(\Gamma)$. If $\gamma(\Gamma)(1 + \Gamma/\sigma^2) > \frac{1}{\sigma^2} g(\Gamma)$, $\Gamma^{\min} \leftarrow \Gamma$; otherwise, $\Gamma^{\max} \leftarrow \Gamma$.
  - Stop, when $\Gamma^{\max} - \Gamma^{\min} \leq \epsilon$.
- The optimal solution of $(\mathbf{PD})$ equals that of $(\mathbf{PC})$ with the converged Γ.

Note that in the above algorithm, $\bar{\Gamma} = \boldsymbol{h}^H \boldsymbol{S}_o \boldsymbol{h}$ and $\boldsymbol{S}_o$ is the optimal solution of $(\mathbf{PC})$ without the interference power constraint[2].

Algorithm 2 searches the optimal Γ according to its gradient direction, and thus avoids solving the sequence of feasibility problems in Algorithm 1. Therefore, Algorithm 2 is much simpler than Algorithm 1. However, since the general case of $(\mathbf{PB})$ has multiple variables Γ_is, this gradient-based algorithm cannot be applied to the general case.

Remark 2: Similar to Proposition 1, a dual relationship between the secrecy transmission $(\mathbf{PD})$ and the CR transmission $(\mathbf{PC})$ in the case of a single eavesdropper/PU can be described as follows. For a given $(\mathbf{PC})$, there is a parameter σ, such that $(\mathbf{PD})$ with the noise variance σ^2 at the eavesdropper has the same solution as that of $(\mathbf{PC})$. This property can be proved by combining Lemma 1 and Proposition 2. This proof is thus omitted for brevity.

C. Single-Antenna SC-Rx Case

We now turn our attention to another special case of the secrecy channel where SC-Rx is equipped with a single receive antenna, i.e., the MISO secrecy channel. Same as the MIMO secrecy case, each eavesdropper is still assumed to have a single antenna. For notational convenience, $(\mathbf{PA})$, $(\mathbf{PB})$, $(\mathbf{PC})$, and $(\mathbf{PD})$ in the case of single-antenna SC-Rx are denoted correspondingly by PA-s, PB-s, PC-s, and PD-s.

The problem PC-s has been studied in [12]. In [12], it was shown that the optimal transmit covariance matrix for the CR MISO channel is a rank-one matrix, and a closed-form solution for the optimal transmit beamforming was presented. The problem PD-s has been studied in [6], [16], where it was shown that the optimal transmit covariance matrix for the secrecy MISO channel is also a rank-one matrix, and based on the generalized eigenvalue decomposition, a closed-form solution for the optimal transmit beamforming was provided.

[2]When $\Gamma > \bar{\Gamma}$, the value of $g(\Gamma)$ is constant regardless of Γ. Thus, the optimal solution of Problem (10) satisfies $\Gamma^* \leq \bar{\Gamma}$.

Consider PA-s, in which there are multiple PUs each having a single receive antenna. To the authors' best knowledge, no closed-form solution exists for such a case. Nevertheless, due to its convexity, this problem can be solved via a standard interior point algorithm. By using a similar method to that in [12], it can be shown that the optimal transmit covariance matrix for PC-s is also a rank-one matrix. In contrast, for PB-s, due to its non-convexity, there is no existing method in the literature to solve this problem. However, since PB-s is a special case of $(\mathbf{PB})$, we can apply Algorithm 1 to efficiently solve this problem .

Next, by exploiting the special structure of PB-s, we provide a simplified algorithm over Algorithm 1. First, we rewrite PB-s as

$$\text{(PB-s)}: \quad \max_{\boldsymbol{S}} \min_{i} \; \hat{F}_i(\boldsymbol{S}) := \frac{1+\boldsymbol{h}_s^H \boldsymbol{S} \boldsymbol{h}_s}{1+(\boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i)/\sigma_i^2} \qquad \text{subject to: } \mathrm{tr}(\boldsymbol{S}) \leq P \tag{12}$$

where the $N \times 1$ vector $\boldsymbol{h}_s$ denotes the channel from SC-Tx to the single antenna SC-Rx. Unlike the general case of $(\mathbf{PB})$ where only its transformed problem in (3) is a quasi-concave problem with respect to Γ_is, PB-s itself is a quasi-concave problem with respect to $\boldsymbol{S}$ due to the following proposition.

Proposition 5: $\hat{F}_i(\boldsymbol{S})$ is a quasi-concave function for $i = 1, \ldots, K$.

Proof: Please refer to Appendix F. ■

Thus, PB-s can be transformed into the following equivalent problem

$$\begin{aligned} &\max_{\boldsymbol{S},t} \; t \\ &\text{subject to: } \mathrm{tr}(\boldsymbol{S}) \leq P \\ &1+\boldsymbol{h}_s^H \boldsymbol{S} \boldsymbol{h}_s \geq t\Big(1+\frac{\boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i}{\sigma_i^2}\Big), i = 1, \cdots, K \end{aligned} \tag{13}$$

where t is a positive variable. For the fixed t, all the constraints in the above problem are linear matrix inequalities over $\boldsymbol{S}$, and thus the corresponding feasibility problem (similarly defined as (6)) can be viewed as a semi-definite programming (SDP) feasibility problem. Correspondingly, the optimal value of t can be obtained by a bisection search algorithm.

Compared with Algorithm 1, the algorithm for Problem (13) is much simpler, since the SDP feasibility problem can be solved via high-efficiency interior point methods, while the feasibility problem (6) in Algorithm 1 can only be solved through a general gradient-based algorithm. Moreover, according to Proposition 1, we can find a set of parameters Γ_is such that the corresponding PA-s has the same solution of PB-s. Since the optimal solution of PA-s is known to be a rank-one matrix [12], so is the optimal solution for PB-s.

V. Multi-antenna Eavesdropper Receiver

In this section, we extend our results to the case with multi-antenna eavesdroppers. We assume that each eavesdropper is equipped with N_e receive antennas, and the channel from SC-Tx to the ith eavesdropper receiver is denoted by $\boldsymbol{H}_i$ of size $N \times N_e$. Similar to $(\mathbf{PB})$, the MIMO secrecy capacity in the multi-antenna eavesdropper case can be obtained from the following optimization problem [9]

$$(\mathbf{PE}): \quad \max_{\boldsymbol{S}} \min_{i} \ \log|\boldsymbol{I}+\boldsymbol{H}_s^H\boldsymbol{S}\boldsymbol{H}_s| - \log|\boldsymbol{I}+\boldsymbol{H}_i^H\boldsymbol{S}\boldsymbol{H}_i| \tag{14}$$

$$\text{subject to: } \mathrm{tr}(\boldsymbol{S}) \le P. \tag{15}$$

To the best knowledge of the authors, there is no existing solution in the literature for the above problem. In the following, we derive the upper and lower bounds on the MIMO secrecy capacity in the multi-antenna eavesdropper case based on the relationship between the secrecy transmission and the CR transmission.

A. Capacity Lower Bound

First, we have the following lemma:

Lemma 2: If for any $i, i \in \{1, \cdots .K\}$, $\mathrm{tr}(\boldsymbol{H}_i^H\boldsymbol{S}\boldsymbol{H}_i) \le \Gamma_i$, we have $|\boldsymbol{I}+\boldsymbol{H}_i^H\boldsymbol{S}\boldsymbol{H}_i| \le (1+\frac{\Gamma_i}{L})^L$, where $L = \min(N_e, N)$.

Proof: Please refer to Appendix G. ■

Similar to Proposition 2, from Lemma 2, the following proposition holds:

Proposition 6: The optimal value of $(\mathbf{PE})$ is lower-bounded by that of the following optimization problem

$$\max_{\Gamma_1,\cdots,\Gamma_K} \ \min_{i} \ \tilde{F}_i(\Gamma_1,\cdots,\Gamma_K) := \frac{\tilde{g}(\Gamma_1,\cdots,\Gamma_K)}{\left(1+\frac{\Gamma_i}{L}\right)^L} \tag{16}$$

where the function $\tilde{g}(\Gamma_1,\cdots,\Gamma_K)$ is defined as

$$\begin{aligned} \tilde{g}(\Gamma_1,\cdots,\Gamma_K) := \max_{\boldsymbol{S}} & |\boldsymbol{I}+\boldsymbol{H}_s^H\boldsymbol{S}\boldsymbol{H}_s| \\ \text{subject to: } & \mathrm{tr}(\boldsymbol{S}) \le P \\ & \mathrm{tr}(\boldsymbol{H}_i^H\boldsymbol{S}\boldsymbol{H}_i) \le \Gamma_i, \ i=1,\cdots,K. \end{aligned} \tag{17}$$

Problem (16) can be solved by the gradient-based method similar to Algorithm 1. Accordingly, the lower bound on the MIMO secrecy capacity is obtained. Note that this capacity lower bound is tight when $N_e = 1$ and thus $L = 1$.

B. Capacity Upper Bound

In the multi-antenna eavesdropper case, the signals received at different antennas of each eavesdropper are jointly processed to decode the contained secrecy message. Therefore, a straightforward upper bound on the secrecy capacity in this case is obtained by assuming that the signals at different antennas of each eavesdropper are decoded independently. Suppose that $\boldsymbol{h}_{i,j}$ is the jth column of the matrix $\boldsymbol{H}_i, j = 1, \cdots, N_e$, then the upper bound on the secrecy capacity can be obtained as

$$\begin{aligned} &\max_{\boldsymbol{S}} \ \min_{\{i,j\}} \ \log|\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S} \boldsymbol{H}_s| - \log\left(1 + \frac{\boldsymbol{h}_{i,j}^H \boldsymbol{S} \boldsymbol{h}_{i,j}}{\sigma_{i,j}^2}\right) \\ &\text{subject to: } \operatorname{tr}(\boldsymbol{S}) \leq P. \end{aligned} \tag{18}$$

The above problem is the same as $(\mathbf{PB})$ with the number of single-antenna eavesdroppers equal to $N_e K$, and thus can be solved by Algorithm 1.

VI. Numerical Examples

In this section, we provide several numerical examples to illustrate the effectiveness of the proposed algorithms in computing the secrecy channel capacity under different system settings. For all examples, we consider a MIMO secrecy channel with $M = N = 4$. The elements of the matrix $\boldsymbol{H}_s$ and the vectors $\boldsymbol{h}_i$s (or the matrices $\boldsymbol{H}_i$s in the multi-antenna eavesdropper case) are assumed to be independent CSCG random variables of zero mean and unit variance. Moreover, the noise power at each eavesdropper antenna is chosen to be one, and the transmit power of the secrecy transmitter, P, is defined in dB relative to the noise power.

A. MIMO Secrecy Capacity with Two Single-Antenna Eavesdroppers

In this example, we consider a MIMO secrecy channel with $K = 2$ single-antenna eavesdroppers. Fig. 2 plots the secrecy capacity of this channel obtained by Algorithm 1, where the transmit power ranges from 0 dB to 10 dB. Moreover, a reference achievable secrecy rate of this channel is obtained by the Projected-Channel SVD (P-SVD) algorithm in [12]. In this algorithm, the channel $\boldsymbol{H}_s$ is projected into a space, which is orthogonal to $\boldsymbol{h}_1$ and $\boldsymbol{h}_2$, and thus the secrecy signals cannot be received by the eavesdroppers. It is easy to observe from Fig. 2 that the secrecy rate obtained by P-SVD is less than the secrecy capacity obtained by Algorithm 1. Moreover, from Proposition 4, it is known that the function $F_i(\Gamma_1, \Gamma_2)$ is a quasi-concave function, and thus the function $\min_{i=1,2} \ F_i(\Gamma_1, \Gamma_2)$ is also a quasi-concave function. In Fig. 3, we plot the value of this function for $P = 5$ dB. It is observed that this function is indeed quasi-concave.

B. MIMO Secrecy Capacity with One Single-Antenna Eavesdropper

In this example, we apply Algorithm 2 to compute the secrecy capacity of a MIMO channel with one single-antenna eavesdropper. As shown in Fig. 4, the secrecy capacity obtained by Algorithm 2 is larger than the achievable secrecy rate obtained by the P-SVD algorithm. Moreover, it is verified that function $F(\Gamma)$ defined in (10) is indeed quasi-concave in Fig. 5 for $P = 5$ dB.

C. MIMO Secrecy Capacity with One Multi-antenna Eavesdropper

In this example, by applying the methods discussed in Section V, we show in Fig. 6 the lower and upper bounds on the MIMO channel secrecy capacity with a single eavesdropper using $N_e = 2$ receive antennas. From the capacity lower bound, we obtain a feasible transmit covariance matrix and thus a corresponding achievable secrecy rate, shown in Fig. 6 and named as "Achievable Secrecy Rate". Moreover, the achievable secrecy rate by the P-SVD algorithm is also shown for comparison.

VII. Conclusion

In this paper, we have disclosed the relationship between the multi-antenna CR transmission problem and the multi-antenna secrecy transmission problem. By exploiting this relationship, we have transformed the non-convex secrecy capacity computation problem into a quasi-convex optimization problem, and developed various algorithms to obtain the optimal solution for different cases of secrecy channels. Although the proposed method cannot obtain the exact secrecy capacity for the more complicated multi-antenna eavesdropper case, it can be applied to compute the upper and lower capacity bounds.

Appendix

A. Proof of Proposition 1: Proposition 1 can be proved by contradiction. For the fixed σ_is, suppose that the optimal solution of $(\mathbf{PB})$ is $\boldsymbol{S}_o$. Define $\bar{\Gamma}_i = \boldsymbol{h}_i^H \boldsymbol{S}_o \boldsymbol{h}_i, i = 1, \ldots, K$. If the optimal solution of $(\mathbf{PA})$ with $\Gamma_i = \bar{\Gamma}_i$, $\forall i$, denoted by $\bar{\boldsymbol{S}}_o$, satisfies $\log|\boldsymbol{I} + \boldsymbol{H}_s^H \bar{\boldsymbol{S}}_o \boldsymbol{H}_s| > \log|\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S}_o \boldsymbol{H}_s|$, then $\bar{\boldsymbol{S}}_o$ is a better solution for $(\mathbf{PB})$ than $\boldsymbol{S}_o$, which contradicts the preassumption that $\boldsymbol{S}_o$ is the optimal solution of $(\mathbf{PB})$. Then there must be $\log|\boldsymbol{I} + \boldsymbol{H}_s^H \bar{\boldsymbol{S}}_o \boldsymbol{H}_s| \leq \log|\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S}_o \boldsymbol{H}_s|$, which means that $\boldsymbol{S}_o$ is also the optimal solution of $(\mathbf{PA})$, with $\Gamma_i = \boldsymbol{h}_i^H \boldsymbol{S}_o \boldsymbol{h}_i, i = 1, \ldots, K$. Proposition 1 thus follows.

B. Proof of Proposition 2: It is easy to observe that $(\mathbf{PB})$ can be re-expressed as

$$\begin{aligned} &\max_{\boldsymbol{S}} \ \min_{i} \ \frac{|\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S} \boldsymbol{H}_s|}{1 + \boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i / \sigma_i^2} \\ &\text{subject to: } \mathrm{tr}(\boldsymbol{S}) \leq P. \end{aligned} \tag{19}$$

Suppose that $\boldsymbol{S}_o$ is the optimal solution of Problem (19) and $(\mathbf{PB})$. Define $T_o := |\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S}_o \boldsymbol{H}_s|$ and $\bar{\Gamma}_i := \boldsymbol{h}_i^H \boldsymbol{S}_o \boldsymbol{h}_i, i = 1, \cdots, K$, then the optimal objective value of Problem (19) is $\bar{F} = \min\Big(T_o/(1 + \bar{\Gamma}_1), \cdots, T_o/(1 + \bar{\Gamma}_K)\Big)$.

Suppose that the optimal solution $\bar{\boldsymbol{S}}_o$ of Problem (2) with $\Gamma_i = \bar{\Gamma}_i, \forall i$, satisfies $|\boldsymbol{I} + \boldsymbol{H}_s^H \bar{\boldsymbol{S}}_o \boldsymbol{H}_s| > T_o$, then $\bar{\boldsymbol{S}}_o$ is a better solution for Problem (19) than $\boldsymbol{S}_o$, which contradicts the preassumption that $\boldsymbol{S}_o$ is the optimal solution of Problem (19). Therefore, we have $T_o = g(\bar{\Gamma}_1, \cdots, \bar{\Gamma}_K)$. Thus, $\bar{F}$ is achievable for Problem (3) with the particular choice of $\Gamma_i = \bar{\Gamma}_i, \forall i$.

Furthermore, suppose that $\tilde{\Gamma}_i$s are the optimal solutions of Problem (3), and the corresponding optimal objective value is $\tilde{F}$. For Problem (2) with $\Gamma_i = \tilde{\Gamma}_i$, suppose that the optimal solution is $\tilde{\boldsymbol{S}}$. We can prove that $\tilde{F} \leq \bar{F}$ by contradiction: If $\tilde{F} > \bar{F}$, $\tilde{\boldsymbol{S}}$ is a better solution for Problem (19) than $\boldsymbol{S}_o$, which contradicts the preassumption that $\boldsymbol{S}_o$ is the optimal solution of Problem (19). As such, we see that $\bar{F}$ is not only achievable for Problem (3), but also the optimal value of Problem (3) with the optimal solutions given as $\tilde{\boldsymbol{S}} = \boldsymbol{S}_o$ and $\tilde{\Gamma}_i = \boldsymbol{h}_i^H \boldsymbol{S}_o \boldsymbol{h}_i$, $\forall i$ (Note that $\boldsymbol{S}$ is a hidden design variable for Problem (3).). Proposition 2 thus follows.

C. Proof of Proposition 3: We first study several important properties of Problem (2) that is known to be an equivalent problem of $(\mathbf{PA})$. Considering $(\mathbf{PA})$ first, its Lagrangian function can be written as

$$L_1(\boldsymbol{S}, \lambda, \{\mu_i\}) = \log|\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S} \boldsymbol{H}_s| - \lambda(\text{tr}(\boldsymbol{S}) - P) - \sum_{i=1}^{K} \mu_i(\boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i - \Gamma_i) \tag{20}$$

where λ and μ_i are the non-negative Lagrange multipliers/dual variables with respect to the transmit power constraint and the interference power constraint at PU$_i$, respectively. Since $(\mathbf{PA})$ is a convex optimization problem, the Karush-Kuhn-Tucker (KKT) conditions [15] are both sufficient and necessary for a solution to be optimal, and solving $(\mathbf{PA})$ is equivalent to solving its dual problem

$$\min_{\lambda, \{\mu_i\}} \max_{\boldsymbol{S}} L_1(\boldsymbol{S}, \lambda, \{\mu_i\}). \tag{21}$$

On the other hand, the auxiliary problem (2) is non-convex due to the fact that its objective function is not concave. In general, the KKT conditions may not be sufficient for a feasible solution to be optimal when we have a non-convex optimization problem. However, we prove in the following lemma that this is not the case for Problem (2).

Lemma 3: With Problem (2), the KKT conditions are both sufficient and necessary for a solution to be optimal.

Proof: The necessary part of Lemma 3 is obvious even for a non-convex optimization problem [15]. The sufficient part of Lemma 3 can be proved via contradiction as follows. The Lagrangian of Problem (2) can be written as

$$L_2(\boldsymbol{S}, \delta, \{\gamma_i\}) = |\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S} \boldsymbol{H}_s| - \delta(\mathrm{tr}(\boldsymbol{S}) - P) - \sum_{i=1}^{K} \gamma_i (\boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i - \Gamma_i) \tag{22}$$

where δ and γ_i are the non-negative dual variables with respect to the transmit power constraint and the interference power constraint at PU$_i$, respectively. We first list the KKT conditions of Problem (2) as follows:

$$|\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S} \boldsymbol{H}_s| \boldsymbol{H}_s (\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S} \boldsymbol{H}_s)^{-1} \boldsymbol{H}_s^H = \delta \boldsymbol{I} + \sum_{i=1}^{K} \gamma_i \boldsymbol{h}_i \boldsymbol{h}_i^H \tag{23}$$

$$\delta(\mathrm{tr}(\boldsymbol{S}) - P) = 0 \tag{24}$$

$$\gamma_i (\boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i - \Gamma_i) = 0, \ i = 1, \cdots, K. \tag{25}$$

Suppose that $\boldsymbol{S}^{(0)}$, $\delta^{(0)}$, and $\gamma_i^{(0)}$ are a set of primal and dual variables that satisfy the above KKT conditions, and the corresponding optimal value of Problem (2) is $C^{(0)}$.

The KKT conditions of $(\mathbf{PA})$ are expressed as

$$\boldsymbol{H}_s (\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S} \boldsymbol{H}_s)^{-1} \boldsymbol{H}_s^H = \lambda \boldsymbol{I} + \sum_{i=1}^{K} \mu_i \boldsymbol{h}_i \boldsymbol{h}_i^H \tag{26}$$

$$\lambda(\mathrm{tr}(\boldsymbol{S}) - P) = 0 \tag{27}$$

$$\mu_i (\boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i - \Gamma_i) = 0, \ i = 1, \cdots, K. \tag{28}$$

Suppose that $\boldsymbol{S}^{(1)}$, $\lambda^{(1)}$, and $\mu_i^{(1)}$ are the optimal primal and dual variables that satisfy the above KKT conditions, and the corresponding optimal value of $(\mathbf{PA})$ is $C^{(1)}$. Note that since $(\mathbf{PA})$ is convex, the KKT conditions are both necessary and sufficient.

If (23)-(25) are not sufficient such that $\log(C^{(0)}) \neq C^{(1)}$, i.e., $\boldsymbol{S}^{(0)} \neq \boldsymbol{S}^{(1)}$, we can choose

$$\boldsymbol{S} = \boldsymbol{S}^{(0)} \tag{29}$$

$$\lambda = \delta^{(0)} / |\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S}^{(0)} \boldsymbol{H}_s| \tag{30}$$

$$\mu_i = \gamma_i^{(0)} / |\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S}^{(0)} \boldsymbol{H}_s|, \ i = 1, \cdots, K \tag{31}$$

for $(\mathbf{PA})$, which clearly also satisfy the KKT conditions of $(\mathbf{PA})$. Given the sufficiency of the KKT conditions for $(\mathbf{PA})$, $\boldsymbol{S}^{(0)}$ is also optimal for $(\mathbf{PA})$ based on (29) such that $\log(C^{(0)}) = C^{(1)}$, which contradicts our assumption that $\log(C^{(0)}) \neq C^{(1)}$. Lemma 3 thus follows. ■

Essentially, it is due to the equivalence between the non-convex Problem (2) and the convex $(\mathbf{PA})$ that Lemma 3 holds. From Lemma 3, it follows that the duality gap between Problem (2) and its dual problem, defined as

$$D = \min_{\delta,\{\gamma_i\}} \max_{\boldsymbol{S}} \ L_2(\boldsymbol{S}, \delta, \{\gamma_i\}), \tag{32}$$

is zero, i.e., $g(\Gamma_1, \cdots, \Gamma_K) = \min_{\delta,\{\gamma_i\}} \max_{\boldsymbol{S}} \ L_2(\boldsymbol{S}, \delta, \{\gamma_i\})$. As such, from (22) we have

$$\frac{\partial g(\Gamma_1, \cdots, \Gamma_K)}{\partial \Gamma_i} = \frac{\partial D}{\partial \Gamma_i} = \gamma_i^{(0)}, i = 1, \cdots, K. \tag{33}$$

Combining (31) and (33), the latter part of Proposition 3 thus follows.

Now we prove the concavity of $g(\Gamma_1, \cdots, \Gamma_K)$. For the function $g(\boldsymbol{q})$, where $\boldsymbol{q} := [\Gamma_1, \cdots, \Gamma_K]^T \in \mathcal{R}_+^K$, its concavity can be verified by considering an arbitrary line given by $\boldsymbol{q} = \boldsymbol{x} + t\boldsymbol{v}$, where $\boldsymbol{x} \in \mathcal{R}_+^K$, $\boldsymbol{v} \in \mathcal{R}^K$, $t \in \mathcal{R}_+$, and $\boldsymbol{x} + t\boldsymbol{v} \in \mathcal{R}_+^K$ [15]. In the sequel, we just need to prove that the function $g(\boldsymbol{x} + t\boldsymbol{v})$ is concave with respect to t. Moreover, if the ith IT constraint is not active for Problem (2), we have $\gamma_i = 0$ from the KKT condition such that the concavity holds. To exclude the above trivial case, we assume that all K IT constraints are active for Problem (2) in the following.

Define

$$f_2(\delta, \gamma_1, \cdots, \gamma_K) := \max_{\boldsymbol{S}} L_2(\boldsymbol{S}, \delta, \gamma_1, \cdots, \gamma_K) \tag{34}$$

as the dual function of Problem (2). Let $\boldsymbol{s}$ be the subgradient of $f_2(\delta, \gamma_1, \cdots, \gamma_K)$. According to the definition of subgradient, the subgradient at the point $[\tilde{\delta}, \tilde{\gamma}_1, \cdots, \tilde{\gamma}_K]$ satisfies

$$f_2(\bar{\delta}, \bar{\gamma}_1, \cdots, \bar{\gamma}_K) \geq f_2(\tilde{\delta}, \tilde{\gamma}_1, \cdots, \tilde{\gamma}_K) + ([\bar{\delta}, \bar{\gamma}_1, \cdots, \bar{\gamma}_K] - [\tilde{\delta}, \tilde{\gamma}_1, \cdots, \tilde{\gamma}_K]) \cdot \boldsymbol{s}, \tag{35}$$

where $[\bar{\delta}, \bar{\gamma}_1, \cdots, \bar{\gamma}_K]$ is another arbitrary feasible point.

Lemma 4: The subgradient $\boldsymbol{s}$ of function $f_2(\delta, \gamma_1, \cdots, \gamma_K)$ at point $[\tilde{\delta}, \tilde{\gamma}_1, \cdots, \tilde{\gamma}_K]$ is $[P - \text{tr}(\tilde{\boldsymbol{S}}), \Gamma_1 - \boldsymbol{h}_1^H \tilde{\boldsymbol{S}} \boldsymbol{h}_1, \cdots, \Gamma_K - \boldsymbol{h}_K^H \tilde{\boldsymbol{S}} \boldsymbol{h}_K]$, where $\tilde{\boldsymbol{S}}$ is the optimal solution of Problem (34) at this point.

Proof: Let $\bar{\boldsymbol{S}}$ be the optimal solution of Problem (34) with $\delta = \bar{\delta}$ and $\gamma_i = \bar{\gamma}_i, i = 1, \cdots, K$. Thus, we have

$$f_2(\bar{\delta}, \bar{\gamma}_1, \cdots, \bar{\gamma}_K) = \bar{r} - \bar{\delta}(\text{tr}(\bar{\boldsymbol{S}}) - P) - \sum_{i=1}^{K} \bar{\gamma}_i(\boldsymbol{h}_i^H \bar{\boldsymbol{S}} \boldsymbol{h}_i - \Gamma_i) \tag{36}$$

$$\geq \tilde{r} - \bar{\delta}(\text{tr}(\tilde{\boldsymbol{S}}) - P) - \sum_{i=1}^{K} \bar{\gamma}_i(\boldsymbol{h}_i^H \tilde{\boldsymbol{S}} \boldsymbol{h}_i - \Gamma_i) \tag{37}$$

$$= \tilde{r} - \tilde{\delta}(\mathrm{tr}(\tilde{\boldsymbol{S}}) - P) - \sum_{i=1}^{K} \tilde{\gamma}_i(\boldsymbol{h}_i^H \tilde{\boldsymbol{S}} \boldsymbol{h}_i - \Gamma_i) + \tilde{\delta}(\mathrm{tr}(\tilde{\boldsymbol{S}}) - P) + \sum_{i=1}^{K} \tilde{\gamma}_i(\boldsymbol{h}_i^H \tilde{\boldsymbol{S}} \boldsymbol{h}_i - \Gamma_i)$$

$$- \bar{\delta}(\mathrm{tr}(\tilde{\boldsymbol{S}}) - P) - \sum_{i=1}^{K} \bar{\gamma}_i(\boldsymbol{h}_i^H \tilde{\boldsymbol{S}} \boldsymbol{h}_i - \Gamma_i) \tag{38}$$

$$= f_2(\bar{\delta}, \bar{\gamma}_1, \cdots, \bar{\gamma}_K) + (\mathrm{tr}(\tilde{\boldsymbol{S}}) - P)(\tilde{\delta} - \bar{\delta}) + \sum_{i=1}^{K} (\boldsymbol{h}_i^H \tilde{\boldsymbol{S}} \boldsymbol{h}_i - \Gamma_i)(\tilde{\gamma}_i - \bar{\gamma}_i) \tag{39}$$

where $\bar{r} = |\boldsymbol{I} + \boldsymbol{H}_s^H \bar{\boldsymbol{S}} \boldsymbol{H}_s|$ and $\tilde{r} = |\boldsymbol{I} + \boldsymbol{H}_s^H \tilde{\boldsymbol{S}} \boldsymbol{H}_s|$. According to (39), we have Lemma 4. ■

According to Lemma 3, Problem (2) is equivalent to its dual problem

$$\min_{\delta, \gamma_1, \cdots, \gamma_K} \quad f_2(\delta, \gamma_1, \cdots, \gamma_K) \tag{40}$$

where $f_2(\delta, \gamma_1, \cdots, \gamma_K)$ is convex. We next consider Problem (2) with parameters $P, \Gamma_1, \cdots, \Gamma_K$, denoted as Problem I. Assume that $\boldsymbol{S}^{(1)}$, $\delta^{(1)}, \gamma_1^{(1)}, \cdots, \gamma_K^{(1)}$ are its primal and dual optimal solutions. Moreover, we have another form of Problem (2) with parameters $P, \Gamma_1 + tv_1, \cdots, \Gamma_K + tv_K$, denoted as Problem II, where t is a positive constant and v_i is a real constant. Assume that $\boldsymbol{S}^{(2)}$, $\delta^{(2)}, \gamma_1^{(2)}, \cdots, \gamma_K^{(2)}$ are the primal and dual optimal solutions of Problem II. According to (34), we can write the dual function of Problem II as

$$f_2^{\mathrm{II}}(\delta, \gamma_1, \cdots, \gamma_K) := \max_{\boldsymbol{S}} \; |\boldsymbol{I} + \boldsymbol{H}_s^H \boldsymbol{S} \boldsymbol{H}_s| - \delta\big(\mathrm{tr}(\boldsymbol{S}) - P\big) - \sum_{i=1}^{K} \gamma_i(\boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i - \Gamma_i - tv_i) \tag{41}$$

To solve Problem II, we apply the subgradient-based algorithm to search the minimum of its dual function $f_2^{\mathrm{II}}(\delta, \gamma_1, \cdots, \gamma_K)$ along the subgradient direction. Suppose that we start from the point $[\delta^{(1)}, \gamma_1^{(1)}, \cdots, \gamma_K^{(1)}]$. Based on Lemma 4, one valid subgradient of $f_2(\delta, \gamma_1, \cdots, \gamma_K)$ at this point is

$$[0, \Gamma_1 + tv_1 - \boldsymbol{h}_1^H \boldsymbol{S}^{(1)} \boldsymbol{h}_1, \cdots, \Gamma_K + tv_K - \boldsymbol{h}_K^H \boldsymbol{S}^{(1)} \boldsymbol{h}_K] = [0, tv_1, \cdots, tv_K], \tag{42}$$

where (42) is due to the KKT condition of Problem I: $\Gamma_i^{(1)} - \boldsymbol{h}_i^H \boldsymbol{S}^{(1)} \boldsymbol{h}_i = 0$ given $\gamma_i^{(1)} > 0, \forall i$. Moreover, according to (35), we have

$$f_2^{\mathrm{II}}(\delta^{(2)}, \gamma_1^{(2)}, \cdots, \gamma_K^{(2)}) \geq f_2^{\mathrm{II}}(\delta^{(1)}, \gamma_1^{(1)}, \cdots, \gamma_K^{(1)}) + ([\delta^{(2)}, \gamma_1^{(2)}, \cdots, \gamma_K^{(2)}] - [\delta^{(1)}, \gamma_1^{(1)}, \cdots, \gamma_K^{(1)}]) \cdot \boldsymbol{s}^{(1)}, \tag{43}$$

where $\boldsymbol{s}^{(1)}$ is the subgradient at the point $[\delta^{(1)}, \gamma_1^{(1)}, \cdots, \gamma_K^{(1)}]$. Since $\delta^{(2)}, \gamma_1^{(2)}, \cdots, \gamma_K^{(2)}$ are the dual optimal solutions of Problem II, we have $f_2^{\mathrm{II}}(\delta^{(2)}, \gamma_1^{(2)}, \cdots, \gamma_K^{(2)}) \leq f_2^{\mathrm{II}}(\delta^{(1)}, \gamma_1^{(1)}, \cdots, \gamma_K^{(1)})$. Combining this with (42) and (43), we have

$$\sum_{i=1}^{K} \gamma_i^{(2)} tv_i \leq \sum_{i=1}^{K} \gamma_i^{(1)} tv_i. \tag{44}$$

Thus,

$$\sum_{i=1}^{K}\gamma_i^{(2)}v_i \le \sum_{i=1}^{K}\gamma_i^{(1)}v_i, \text{ given } t>0. \tag{45}$$

Moreover, according to Lemma 3 and (22), we have

$$\frac{\partial g(\boldsymbol{x}+t\boldsymbol{v})}{\partial t}=\sum_{i=1}^{K}\gamma_i v_i. \tag{46}$$

Note that γ_i is the Lagrange multiplier of Problem (2) with respect to the ith IT constraint. With a different IT threshold, i.e., a different value of t, γ_is are not necessarily the same, and thus γ_is can be viewed as implicit functions of t. Combining (45) with (46), it is easy to observe $\frac{\partial g(\boldsymbol{x}+t\boldsymbol{v})}{\partial t}$ decreases with the increase of t since the derivative change over t is given as $\sum_{i=1}^{K}\gamma_i^{(2)}v_i-\sum_{i=1}^{K}\gamma_i^{(1)}v_i\le 0$, i.e., the second order derivative of function $g(\boldsymbol{x}+t\boldsymbol{v})$ over t is negative on an arbitrary line $\boldsymbol{x}+t\boldsymbol{v}$ in the feasible region. Therefore, $g(\boldsymbol{q})$ is concave. Proposition 3 thus follows.

D. Proof of Proposition 4: The quasi-concavity is define as follows [15]:

Definition 1: A function $f:\mathcal{R}^K\rightarrow\mathcal{R}$ is called *quasi-concave* if all its sublevel sets

$$S_\alpha=\{\boldsymbol{x}\in \mathbf{dom}f\,|\,f(\boldsymbol{x})\ge\alpha\} \tag{47}$$

for $\alpha\in\mathcal{R}$, are convex sets.

According to Proposition 3, $g(\Gamma_1,\cdots,\Gamma_K)$ is a concave function of Γ_is. Therefore, the α-sublevel set of $F_i(\Gamma_1,\cdots,\Gamma_K)$

$$S_\alpha=\left\{\boldsymbol{q}\middle|\frac{g(\Gamma_1,\cdots,\Gamma_K)}{1+\Gamma_i/\sigma_i^2}\ge\alpha\right\}=\{\boldsymbol{q}|g(\Gamma_1,\cdots,\Gamma_K)\ge\alpha(1+\Gamma_i/\sigma_i^2)\} \tag{48}$$

is a convex set for any α, and thus the function $F_i(\Gamma_1,\cdots,\Gamma_K)$ is a quasi-concave function. Since the objective function of Problem (3) is the minimum of K quasi-concave functions, $F_i(\Gamma_1,\cdots,\Gamma_K)$, $i=1,\cdots,K$, it is still quasi-concave [15]. Proposition 4 thus follows.

E. Proof of Lemma 1: The optimality condition of Problem (10) is

$$\frac{\partial F(\Gamma)}{\partial\Gamma}=\frac{\gamma(\Gamma)(1+\Gamma/\sigma^2)-\frac{1}{\sigma^2}g(\Gamma)}{\left(1+\Gamma/\sigma^2\right)^2}=0. \tag{49}$$

Since the above optimality condition is a necessary condition for any unconstrained smooth optimization problems regardless of its convexity [15], the necessary part of Lemma 1 follows.

We next prove the sufficient part of this lemma by contradiction. We first present a property of $\gamma(\Gamma)$ as follows.

Lemma 5: $\gamma(\Gamma)$ is a non-increasing function for $\Gamma\ge 0$.

The proof of Lemma 5 is similar to that of Proposition 4, and thus is omitted here. Suppose that there are two solutions $\Gamma^{(1)}$ and $\Gamma^{(2)}$, both of which satisfy the condition in (11). Furthermore, without loss of generality, we assume $\Gamma^{(1)} < \Gamma^{(2)}$. Therefore, we have

$$g(\Gamma^{(1)}) > g(\Gamma^{(2)}). \tag{50}$$

According to (33), we have

$$\frac{g(\Gamma^{(2)}) - g(\Gamma^{(1)})}{\Gamma^{(2)} - \Gamma^{(1)}} \geq \gamma(\Gamma^{(2)}). \tag{51}$$

Thus,

$$g(\Gamma^{(2)}) - \Gamma^{(2)}\gamma(\Gamma^{(2)}) \geq g(\Gamma^{(1)}) - \Gamma^{(1)}\gamma(\Gamma^{(2)}) \geq g(\Gamma^{(1)}) - \Gamma^{(1)}\gamma(\Gamma^{(1)}) \tag{52}$$

where the second inequality is due to the fact that $\gamma(\Gamma^{(1)}) \geq \gamma(\Gamma^{(2)})$ from Lemma 5.

Since both solutions satisfy the necessary condition (11), we have

$$\gamma(\Gamma^{(1)}) = \frac{1}{\sigma^2}\Big(g(\Gamma^{(1)}) - \gamma(\Gamma^{(1)})\Gamma^{(1)}\Big) \tag{53}$$

$$\gamma(\Gamma^{(2)}) = \frac{1}{\sigma^2}\Big(g(\Gamma^{(2)}) - \gamma(\Gamma^{(2)})\Gamma^{(2)}\Big). \tag{54}$$

From (52) and $\gamma(\Gamma^{(1)}) \geq \gamma(\Gamma^{(2)})$, it is easy to observe that (53) and (54) hold simultaneously if and only if $\gamma(\Gamma^{(1)}) = \gamma(\Gamma^{(2)}) = \gamma$. Thus, we have

$$g(\Gamma^{(1)}) = g(\Gamma^{(2)}) - \gamma(\Gamma^{(1)} - \Gamma^{(2)}). \tag{55}$$

Since $\Gamma^{(1)} < \Gamma^{(2)}$ and $g(\Gamma^{(1)}) > g(\Gamma^{(2)})$, we further derive $\gamma < 0$, which contradicts the fact that the Lagrange multiplier $\gamma \geq 0$. As such the solution of (11) is unique, which implies the sufficiency given the already proven necessity part. Lemma 1 thus follows.

F. Proof of Proposition 5: Similar to the proof given in Appendix D, the α-sublevel set of $\hat{F}_i(\boldsymbol{S})$

$$S_\alpha = \{\boldsymbol{S} | \frac{1 + \boldsymbol{h}_s^H \boldsymbol{S} \boldsymbol{h}_s}{1 + (\boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i)/\sigma_i^2} \geq \alpha\} \tag{56}$$

$$= \{\boldsymbol{S} | 1 + \boldsymbol{h}_s^H \boldsymbol{S} \boldsymbol{h}_s \geq \alpha(1 + (\boldsymbol{h}_i^H \boldsymbol{S} \boldsymbol{h}_i)/\sigma_i^2)\}. \tag{57}$$

is a convex set. Thus, $\hat{F}_i(\boldsymbol{S})$ is a quasi-concave function.

G. Proof of Lemma 2: We have

$$|\boldsymbol{I}+\boldsymbol{H}_i^H\boldsymbol{S}\boldsymbol{H}_i| = |\boldsymbol{I}+\boldsymbol{U}_i^H\boldsymbol{\Lambda}_i\boldsymbol{U}_i| = |\boldsymbol{I}+\boldsymbol{\Lambda}_i| \tag{58}$$

where $\boldsymbol{H}_i^H\boldsymbol{S}\boldsymbol{H}_i := \boldsymbol{U}_i^H\boldsymbol{\Lambda}_i\boldsymbol{U}_i$ is the eigenvalue decomposition. Since $\text{tr}(\boldsymbol{H}_i^H\boldsymbol{S}\boldsymbol{H}_i) = \text{tr}(\boldsymbol{\Lambda}_i)$, from $\text{tr}(\boldsymbol{H}_i^H\boldsymbol{S}\boldsymbol{H}_i) \leq \Gamma_i$ it follows that

$$\text{tr}(\boldsymbol{\Lambda}_i) \leq \Gamma_i. \tag{59}$$

Combining (58) and (59) and denoting $L = \min(N_e, N)$, we have

$$|\boldsymbol{I}+\boldsymbol{H}_i^H\boldsymbol{S}\boldsymbol{H}_i| \leq \left|\boldsymbol{I}+\frac{\Gamma_i}{L}\boldsymbol{I}\right| = \left(1+\frac{\Gamma_i}{L}\right)^L \tag{60}$$

where the inequality is obtained by solving the following problem: $\max_{\text{tr}(\boldsymbol{\Lambda}_i)\leq\Gamma_i} |\boldsymbol{I}+\boldsymbol{\Lambda}_i|$. Lemma 2 thus follows.

References

[1] A. Wyner, "The wire-tap chnnel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 5, pp. 339–348, May 1978.

[3] Y. Liang, H. V. Poor, and S. Shamai(Shitz), "Secrecy capacity region of fading broadcast channels," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Nice, France, June 2007.

[4] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 976–1002, 2008.

[5] ——, "Generalized multiple access channels with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, Washington, July 2006.

[6] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2493–2507, June 2008.

[7] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai(Shitz), and S. Verdu, "Cognitive interference channels with confidential messages," in *Proc. of Allerton Conference on Communication, Control, and Computing (Allerton)*, Monticello, IL, 2007.

[8] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The misome wiretap channel," 2007. [Online]. Available: arXiv:0708.4219v1

[9] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," 2007. [Online]. Available: arXiv:0710.1920v1

[10] T. Liu and S. Shamai, "A note on the secrecy capacity of the multi-antenna wiretap channel," 2007. [Online]. Available: arXiv:0710.4105

[11] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 3936–64, Sept. 2006.

[12] R. Zhang and Y.-C. Liang, "Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks," *IEEE J. Select. Topics in Signal Processing*, vol. 2, no. 1, pp. 88–102, Feb. 2008.

[13] L. Zhang, Y.-C. Liang, and Y. Xin, "Joint beamforming and power allocation for multiple access channels in cognitive radio networks," *IEEE J. Select. Areas Commun.*, vol. 26, no. 1, pp. 38–51, Jan. 2008.

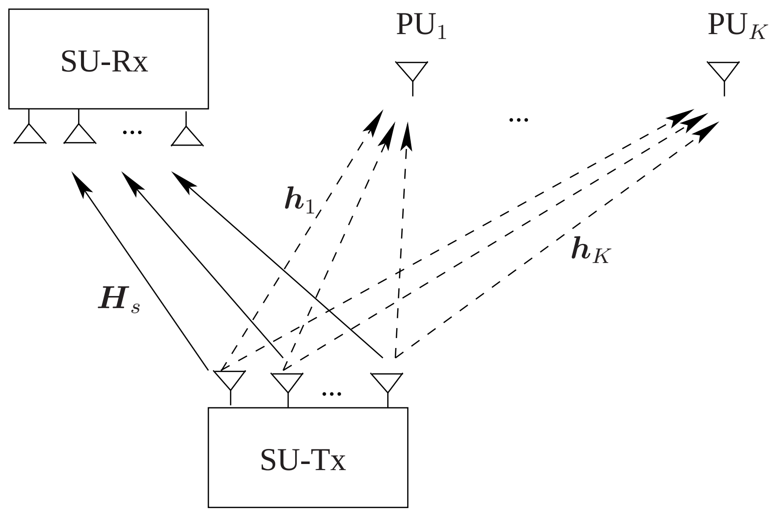
[14] L. Zhang, Y. Xin, and Y.-C. Liang, "Weighted sum rate optimization for cognitive radio MIMO broadcast channels," in *IEEE international conference on communications*, Beijing, China, 19-23, May, 2008, pp. 3679–3683.

[15] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.

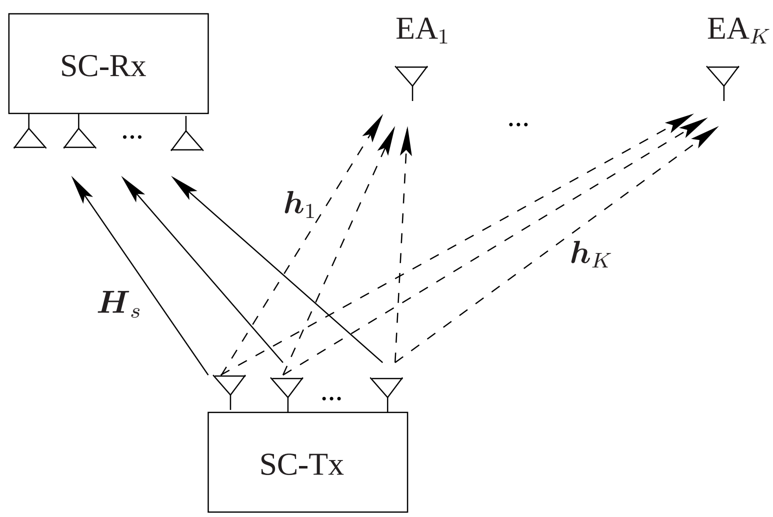
[16] S. Shafiee and S. Ulukus, “Achievable rates in gaussian MISO channels with secrecy constraints,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, June 2007.

[17] R. Liu and H. V. Poor, “Secrecy capacity region of a multi-antenna gaussian boradcast channel with confidential messages,” 2008. [Online]. Available: arXiv:0804.4195v1.

[18] M. Mohseni, R. Zhang, and J. M. Cioffi, “Optimized transmission for fading multiple-access and broadcast channels with multiple antennas,” *IEEE J. Select. Areas Commun.*, vol. 24, no. 8, pp. 1627–1639, Aug. 2006.



(a)



(b)

Fig. 1. The comparison of two system models: (a) the CR MIMO channel with K single-antenna PUs; and (b) the secrecy MIMO channel with K single-antenna eavesdroppers.

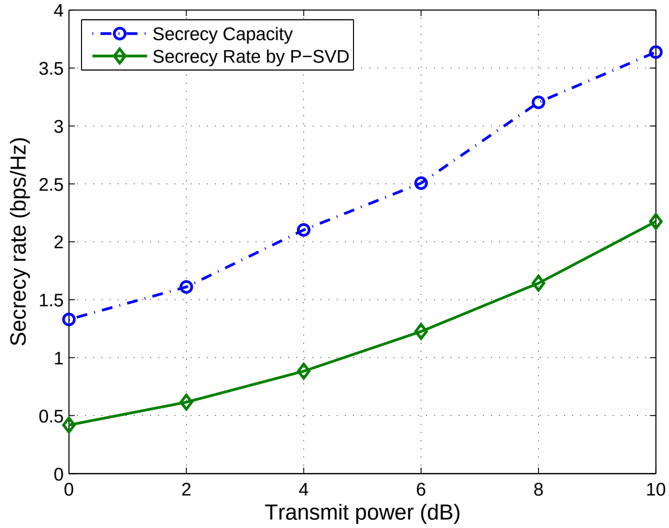


Fig. 2. Comparison of the secrecy capacity by Algorithm 1 and the secrecy rate by the P-SVD algorithm in [12] for $M = N = 4$ and $K = 2$ single-antenna eavesdroppers.

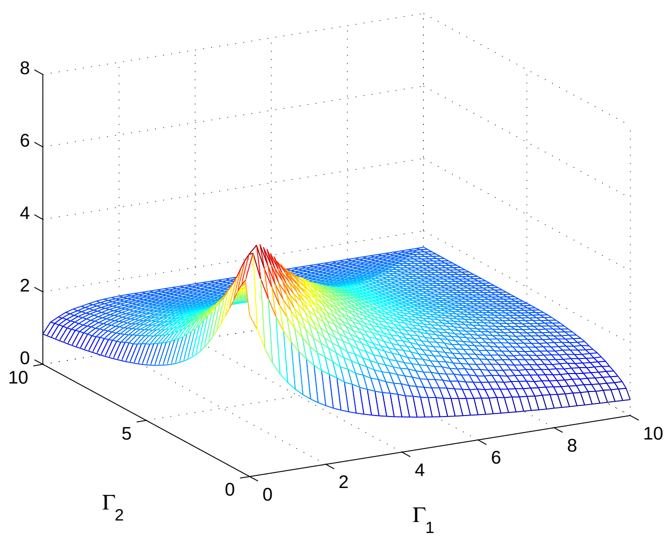


Fig. 3. The value of the function $\min_{i=1,2} \ F_i(\Gamma_1, \Gamma_2)$ for $M = N = 4$, $K = 2$ single-antenna eavesdroppers, and $P = 5$ dB.

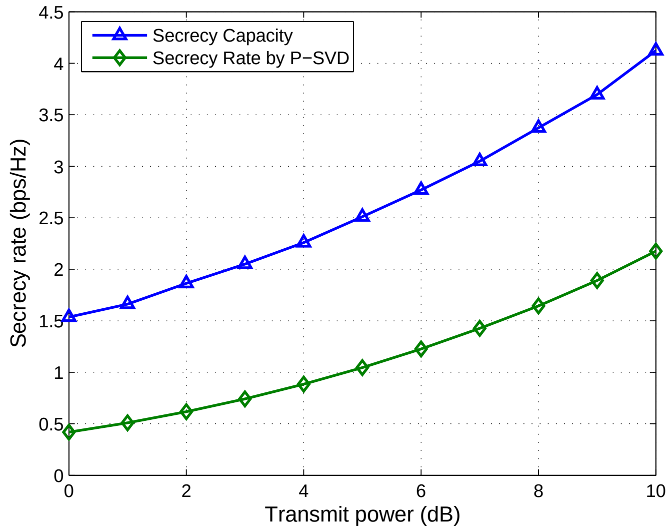


Fig. 4. Comparison of the secrecy capacity by Algorithm 2 and the secrecy rate by the P-SVD algorithm in [12] for $M = N = 4$ and $K = 1$ single-antenna eavesdropper.

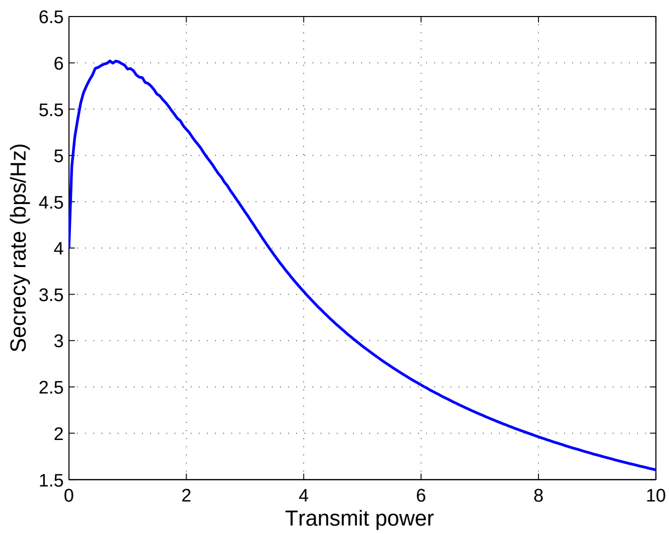


Fig. 5. The value of the function $F(\Gamma)$ for $M = N = 4$, $K = 1$ single-antenna eavesdropper, and $P = 5$ dB.

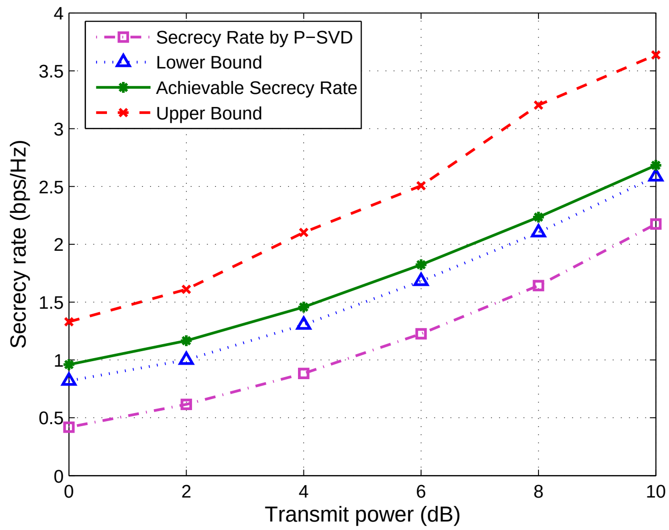


Fig. 6. Comparison of the lower and upper bounds on the secrecy capacity and two achievable secrecy rates for $M = N = 4$, $K = 1$ eavesdropper with $N_e = 2$ receive antennas.