Optimal Signal Design for Coherent Detection of Binary Signals in Gaussian Noise under Power and Secrecy Constraints

Berkan Dulek[a], Sinan Gezici[b,*]

[a]*Department of Electrical and Electronics Engineering, Hacettepe University, Beytepe Campus, Ankara, 06800, Turkey*
[b]*Department of Electrical and Electronics Engineering, Bilkent University, Ankara, 06800, Turkey*

Abstract

The problem of optimal signal design for coherent detection of binary signals in Gaussian noise is revisited under power and secrecy constraints. In particular, the aim is to select the binary transmitted signals in an optimal manner so that the probability of error is minimized at an intended receiver while the probability of error at an eavesdropper is maintained above a threshold value and the signal powers are limited. It is shown that an optimal solution exists in the form of antipodal signaling along the eigenvector corresponding to the solution of a maximum (possibly generalized) eigenvalue problem, which is specified explicitly based on the channel coefficient matrices and the noise covariance matrices at the intended receiver and the eavesdropper. Furthermore, optimal signal design can be performed in an efficient manner by solving a semidefinite programming (SDP) relaxation followed by a matrix rank-one decomposition. Numerical examples are provided to illustrate

*Corresponding author.
Email addresses: berkan@ee.hacettepe.edu.tr (Berkan Dulek), gezici@ee.bilkent.edu.tr (Sinan Gezici)

optimal solutions for three different but exhaustive cases.

Keywords: secrecy, signal design, hypothesis testing, probability of error

---

1. Introduction

It is well-known that the performance of optimum coherent detection of binary signals in Gaussian noise is improved by selecting antipodal signals along the eigenvector of the noise covariance matrix corresponding to the minimum eigenvalue [1, Remark III.B.3]. Under identical power constraints on the transmitted binary signals, this signal selection strategy minimizes the average probability of error at the receiver. However, the detection performance at the receiver may not be the sole performance criterion as is the case with numerous applications where the physical layer secrecy is important and the data needs to be transmitted secretly to an intended receiver in the presence of eavesdropping [2, 3]. Although physical layer secrecy is investigated extensively in the literature based on information theoretic metrics such as secrecy capacity [4], estimation theoretic metrics such as Fisher information and mean-squared error (MSE) [5, 6], and secrecy constrained distributed detection under Neyman-Pearson and Bayesian frameworks [7], effects of signal design have been considered only in a limited number of studies [8, 9], which are based on modifying given signal constellations. To the best of our knowledge, a theoretical analysis of the optimal signal design problem under both power and secrecy constraints in the spirit of [1, Remark III.B.3] is neglected. In this paper, we focus on the optimal signal design problem for a coherent binary communications system and characterize optimal signal vectors under secrecy and power constraints. The technical contributions and novelty of our work can be summarized as follows: (i) A novel optimal signal design problem is proposed for binary communications with the aim

of minimizing the probability of error at an intended receiver under constraints on the probability of error at an eavesdropper and on the power levels of the signals. (ii) It is shown that an optimal solution in the form of antipodal signaling exists and can be obtained as the solution of a nonconvex homogeneous quadratic optimization problem, which admits no duality gap. (iii) Using results from quadratic optimization literature, it is shown that antipodal signaling is performed along the eigenvector corresponding to the solution of a maximum (possibly generalized) eigenvalue problem. (iv) An efficient numerical solution is provided via a semidefinite programming (SDP) relaxation followed by a matrix rank-one decomposition. It should be noted that the term 'secrecy' is employed in a broader sense in our work than that commonly understood in an information theoretic sense. In the latter, the aim is to ensure that the capacity of the channel to the eavesdropper is lower than the chosen communication rate so that the error probability at the eavesdropper goes to one exponentially fast with the block length. In addition to being of interest from a decision theoretic viewpoint, the framework proposed in this paper is applicable in cases when such an information theoretic goal cannot be met. Although the eavesdropper is not completely blanked out and it may decode some of the transmitted symbols correctly, the message can still be rendered unintelligible by forcing the eavesdropper to frequent errors.

Notation: Throughout this paper, vectors (in column form) and matrices are denoted by boldface lower and upper case letters, such as $\mathbf{x}$ and $\mathbf{A}$, respectively. $(\cdot)^T$ and $\mathrm{tr}(\cdot)$ denote transpose and trace operators, respectively. For symmetric matrices $\mathbf{A}$ and $\mathbf{B}$, we write $\mathbf{A} \succeq \mathbf{B}$ if $\mathbf{A} - \mathbf{B}$ is positive semidefinite, and likewise, $\mathbf{A} \succ \mathbf{B}$ if $\mathbf{A} - \mathbf{B}$ is positive definite. The identity matrix is denoted by $\mathbf{I}$. $\|\mathbf{x}\|$ denotes the ℓ^2-norm of $\mathbf{x}$, i.e., $\|\mathbf{x}\| = \sqrt{\mathbf{x}^T\mathbf{x}}$.

The set of real numbers is denoted by $\mathbb{R}$, the set of real vectors with dimension k is denoted by $\mathbb{R}^k$, the set of $n \times k$ real matrices is denoted by $\mathbb{R}^{n\times k}$, and the set of $k \times k$ real symmetric matrices is denoted by $\mathbb{S}^{k\times k}$. The multivariate real Gaussian distribution with mean vector $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$ is denoted by $\mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$. Optimal values of optimization variables are shown with an asterisk as in $\mathbf{x}^*$. The generalized eigenvector problem with $k \times k$ matrices $\mathbf{A}_r$ and $\mathbf{A}_e$, denoted by the ordered pair $(\mathbf{A}_r, \mathbf{A}_e)$, is defined as a solution of $\mathbf{A}_r\mathbf{w}_i = \lambda_i\mathbf{A}_e\mathbf{w}_i$ for all $i \in \{1, \ldots, k\}$, where $\mathbf{w}_i$ denotes the i-th generalized eigenvector with the corresponding generalized eigenvalue λ_i.

2. Problem Formulation

We consider a binary hypothesis testing problem in the Bayesian framework with *a priori* probabilities of the hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ denoted by π_0 and $\pi_1 = 1 - \pi_0$, respectively. Under hypothesis $\mathcal{H}_i$, the transmitter sends the signal $\mathbf{s}_i \in \mathbb{R}^k$, which passes through a linear channel and is corrupted by Gaussian noise. Accordingly, the observation at the intended receiver, denoted by $\mathbf{y}_r \in \mathbb{R}^n$, is expressed as

$$\mathcal{H}_i \;:\; \mathbf{y}_r = \mathbf{F}_r\mathbf{s}_i + \mathbf{n}_r\,, \quad i \in \{0, 1\} \tag{1}$$

where $\mathbf{F}_r \in \mathbb{R}^{n\times k}$ is the channel matrix having full column rank with $n \geq k$, and $\mathbf{n}_r \in \mathbb{R}^n$ is Gaussian with zero mean and covariance matrix $\boldsymbol{\Sigma}_r \succ 0$; that is, $\mathbf{n}_r \sim \mathcal{N}(\mathbf{0}, \boldsymbol{\Sigma}_r)$. In addition to the intended receiver, an eavesdropper in the environment makes the following observation under $\mathcal{H}_i$:

$$\mathcal{H}_i \;:\; \mathbf{y}_e = \mathbf{F}_e\mathbf{s}_i + \mathbf{n}_e\,, \quad i \in \{0, 1\} \tag{2}$$

where $\mathbf{y}_e \in \mathbb{R}^m$, $\mathbf{F}_e \in \mathbb{R}^{m\times k}$, and $\mathbf{n}_e \in \mathbb{R}^m$ represent the observation, the full-rank channel matrix with $m \geq k$, and the noise vector distributed as

$\mathbf{n}_e \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_e)$ with $\mathbf{\Sigma}_e \succ 0$ at the eavesdropper, respectively.[1] Similarly to [6] and [10], the eavesdropper is assumed to be smart in the sense that it can learn or has perfect knowledge of the binary transmitted signals $\mathbf{s}_0$ and $\mathbf{s}_1$, the corresponding *a priori* probabilities π_0 and π_1, the channel matrix $\mathbf{F}_e$, and the noise covariance matrix $\mathbf{\Sigma}_e$.

With perfect knowledge of the system parameters at the intended receiver and the eavesdropper, the aim of the transmitter is to design $\mathbf{s}_0$ and $\mathbf{s}_1$ so that the probability of error is minimized at the intended receiver while keeping the probability of error at the eavesdropper above a certain level and satisfying the transmitted signal power constraints. Under this setting, both the intended receiver and the eavesdropper employ maximum *a posteriori* (MAP) decision rules to minimize the probability of error [1]. For the signal models in (1) and (2), the error probabilities of the MAP decision rules at the intended receiver and the eavesdropper are obtained as [1, Sec. III.B]:

$$\mathrm{P}_j^{err} = \pi_0 Q\left(\frac{\ln(\frac{\pi_0}{\pi_1})}{d_j} + \frac{d_j}{2}\right) + \pi_1 Q\left(\frac{d_j}{2} - \frac{\ln(\frac{\pi_0}{\pi_1})}{d_j}\right) \tag{3}$$

for $j \in \{r, e\}$, where r and e refer to the intended receiver and the eavesdropper, respectively, and d_j is defined as

$$d_j \triangleq \sqrt{(\mathbf{s}_1 - \mathbf{s}_0)^T \mathbf{F}_j^T \mathbf{\Sigma}_j^{-1} \mathbf{F}_j (\mathbf{s}_1 - \mathbf{s}_0)}\,, \quad j \in \{r, e\}\,.$$

Since P_j^{err} in (3) is a monotone decreasing function of d_j [1, Remark III.B.3], the transmitter aims to maximize d_r while imposing an upper bound on d_e

[1] The case of complex vectors in the presence of circularly symmetric complex Gaussian noise can be treated in a similar manner.

for secrecy purposes. Hence, the following signal design problem is proposed:

$$\underset{\mathbf{s}_0\in\mathbb{R}^k,\,\mathbf{s}_1\in\mathbb{R}^k}{\text{maximize}} \quad (\mathbf{s}_1-\mathbf{s}_0)^T\mathbf{A}_r(\mathbf{s}_1-\mathbf{s}_0) \tag{P1-a}$$

$$\text{subject to} \quad (\mathbf{s}_1-\mathbf{s}_0)^T\mathbf{A}_e(\mathbf{s}_1-\mathbf{s}_0)\leq\eta\,, \tag{P1-b}$$

$$\|\mathbf{s}_0\|^2\leq P\,,\quad \|\mathbf{s}_1\|^2\leq P\,, \tag{P1-c}$$

where $\mathbf{A}_r \triangleq \mathbf{F}_r^T\boldsymbol{\Sigma}_r^{-1}\mathbf{F}_r$, $\mathbf{A}_e \triangleq \mathbf{F}_e^T\boldsymbol{\Sigma}_e^{-1}\mathbf{F}_e$, $\eta>0$ specifies the secrecy constraint, and $P>0$ is the power limit on the transmitted signals. It is noted that $\mathbf{A}_r$ and $\mathbf{A}_e$ are positive definite matrices since $\boldsymbol{\Sigma}_r$ and $\boldsymbol{\Sigma}_e$ are positive definite, and $\mathbf{F}_r$ and $\mathbf{F}_e$ have full column rank. The problem is feasible for all $\eta>0$ and $P>0$. Another remark is that the quadratic terms in (P1-a) and (P1-b) correspond to the Chernoff information measures between the probability distributions under the two hypotheses at the receiver and the eavesdropper, respectively [11, Example 6.5]. Since the Chernoff information is the highest achievable exponent in the Bayesian probability of error [12, Section 11.9], the significance of the optimization problem (P1) is not limited to MAP decision rules but it is also important for the large sample size regime.

3. Optimal Signal Design

In order to find an optimal solution of (P1), the following lemma is given first which extends the optimality result for antipodal signaling in the absence of a secrecy constraint given in [1, Remark III.B.3].

Lemma: *There exist antipodal signals, i.e.,* $\mathbf{s}_1^*=-\mathbf{s}_0^*$*, that are optimal for the optimization problem (P1).*

Proof: Since the problem (P1) is feasible for any $\eta>0$ and $P>0$, a solution always exists. Suppose that an optimal pair $(\mathbf{s}_0^*,\mathbf{s}_1^*)$ is obtained as a

solution of (P1). Then, a pair of antipodal signals can be defined as

$$\tilde{\mathbf{s}}_1 = -\tilde{\mathbf{s}}_0 \triangleq \frac{\mathbf{s}_1^* - \mathbf{s}_0^*}{2}\,. \tag{5}$$

It is noted that the values of the objective function in (P1-a) and the constraint function in (P1-b) remain same, i.e., $(\tilde{\mathbf{s}}_1 - \tilde{\mathbf{s}}_0)^T\mathbf{A}_r(\tilde{\mathbf{s}}_1 - \tilde{\mathbf{s}}_0) = (\mathbf{s}_1^* - \mathbf{s}_0^*)^T\mathbf{A}_r(\mathbf{s}_1^* - \mathbf{s}_0^*)$ and $(\tilde{\mathbf{s}}_1 - \tilde{\mathbf{s}}_0)^T\mathbf{A}_e(\tilde{\mathbf{s}}_1 - \tilde{\mathbf{s}}_0) = (\mathbf{s}_1^* - \mathbf{s}_0^*)^T\mathbf{A}_e(\mathbf{s}_1^* - \mathbf{s}_0^*)$. Furthermore, $\|\tilde{\mathbf{s}}_1\| = \|\tilde{\mathbf{s}}_0\| = \frac{\|\mathbf{s}_1^* - \mathbf{s}_0^*\|}{2} \leq \frac{\|\mathbf{s}_1^*\| + \|\mathbf{s}_0^*\|}{2} \leq \sqrt{P}$, which follows from the triangle inequality and the power constraints in (P1-c). Hence, $(\tilde{\mathbf{s}}_1, \tilde{\mathbf{s}}_0)$ maximize the objective function while satisfying the constraints. □

In the light of the Lemma, $\mathbf{s}_1^* = -\mathbf{s}_0^* = \mathbf{x}^*$ can be employed without any loss in optimality, where $\mathbf{x}^*$ is a solution to

$$\begin{aligned} &\underset{\mathbf{x}\in\mathbb{R}^k}{\text{maximize}} \;\; \mathbf{x}^T\mathbf{A}_r\mathbf{x} \\ &\text{subject to} \;\; \mathbf{x}^T\mathbf{A}_e\mathbf{x} \leq \kappa \text{ and } \|\mathbf{x}\|^2 \leq P\,, \end{aligned} \tag{P2}$$

with $\kappa = \eta/4$. The optimization problem (P2) involves the *maximization* of a convex quadratic function subject to two convex quadratic constraints. The feasible region is the intersection of an ellipsoid and a sphere. Since the maximum of a convex function over a closed bounded convex set is achieved at an extreme point [13], solution is an extreme point of the feasible set. Before proceeding further, we present some information for the *general* quadratic optimization problem, which is known to be NP-hard:

$$\begin{aligned} &\underset{\mathbf{x}\in\mathbb{R}^k}{\text{minimize}} \;\; \mathbf{x}^T\mathbf{Q}_0\mathbf{x} + 2\mathbf{b}_0^T\mathbf{x} + c_0 \\ &\text{subject to} \;\; \mathbf{x}^T\mathbf{Q}_i\mathbf{x} + 2\mathbf{b}_i^T\mathbf{x} + c_i \leq 0\,, \quad i = 1, \ldots, m \end{aligned} \tag{QP}$$

where $\mathbf{Q}_i \in \mathbb{S}^{k\times k}$, $\mathbf{b}_i \in \mathbb{R}^k$ and $c_i \in \mathbb{R}$ for each $i = 0, 1, \ldots, m$. $\mathbf{Q}_i \succeq 0$ is not assumed in (QP), meaning that the quadratic objective and constraint

functions need not be convex. In the case of a single constraint (i.e., $m = 1$), strong duality holds provided Salter's constraint qualification is satisfied, i.e., if there exists an $\mathbf{x}$ such that $\mathbf{x}^T\mathbf{Q}_1\mathbf{x} - 2\mathbf{b}_1^T\mathbf{x} + c_1 < 0$ [13, Appendix B]. There is also no duality gap in optimizing an indefinite quadratic function under a single (non-convex) quadratic equality constraint, or under a convex quadratic inequality constraint and a linear inequality constraint [14]. Related to our problem is also the Celis-Dennis-Tapia (CDT) quadratic subproblem, which minimizes a non-convex quadratic function subject to two convex quadratic constraints, at least one of which is strictly convex [15], i.e., $\mathbf{Q}_0 \in \mathbb{S}^{k\times k}, \mathbf{Q}_1 \succeq 0, \mathbf{Q}_2 \succ 0$ with $\mathbf{b}_i \in \mathbb{R}^k, c_i \in \mathbb{R}$ and $m = 2$ in (QP). Since the CDT problem is non-convex, it can have a duality gap [16]. For example, this can happen when the Hessian of the Lagrangian in the CDT problem has one negative eigenvalue at a global solution [17].

In the following, we employ the strong duality result presented in [18, Section 2.2] for quadratic optimization problems with $m = 2$, where the two constraint functions and the objective function are all homogeneous quadratic functions, i.e., there are no linear terms: $\mathbf{b}_i = 0$ for each $i = 0, 1, 2$ in (QP) and at least one of $\mathbf{Q}_1$ and $\mathbf{Q}_2$ matrices is positive definite. More explicitly, it is shown in [18, Section 2.2] that the following optimization problem

$$\begin{aligned} \underset{\mathbf{x}\in\mathbb{R}^k}{\text{minimize}} \quad & \mathbf{x}^T\mathbf{Q}_0\mathbf{x} \\ \text{subject to} \quad & \mathbf{x}^T\mathbf{Q}_1\mathbf{x} \leq 1\,, \\ & \mathbf{x}^T\mathbf{Q}_2\mathbf{x} \leq 1\,, \end{aligned} \tag{QHP}$$

where $\mathbf{Q}_0 \in \mathbb{S}^{k\times k}, \mathbf{Q}_1 \in \mathbb{S}^{k\times k}, \mathbf{Q}_2 \succ 0$, enjoys strong duality. The optimization problem (P2) can be put in the form of the problem (QHP) by selecting $\mathbf{Q}_0 = -\mathbf{A}_r, \mathbf{Q}_1 = \mathbf{A}_e/\kappa$ and $\mathbf{Q}_2 = \mathbf{I}/P$. Based on this result, an optimal solution of the signal design problem (P2) can be characterized.

Proposition: *Let $\mathbf{A}_r, \mathbf{A}_e, \eta$, and P be as specified in (P1) and $\kappa = \eta/4$. Let $\mathbf{v}_r^{\max}$ be an eigenvector of $\mathbf{A}_r$ corresponding to its maximum eigenvalue and have unit-norm, i.e., $\|\mathbf{v}_r^{\max}\| = 1$. If $(\mathbf{v}_r^{\max})^T \mathbf{A}_e \mathbf{v}_r^{\max} \leq \kappa/P$, an optimal solution of (P1) is given by*

$$\mathbf{s}_1^* = -\mathbf{s}_0^* = \sqrt{P}\, \mathbf{v}_r^{\max}\,. \qquad \text{(Case 1)}$$

Otherwise, let $\mathbf{w}^{\max}$ represent a generalized eigenvector of $(\mathbf{A}_r, \mathbf{A}_e)$ corresponding to the maximum generalized eigenvalue and $\mathbf{w}^{\max}$ is normalized to satisfy $(\mathbf{w}^{\max})^T \mathbf{A}_e \mathbf{w}^{\max} = 1$. If $\|\mathbf{w}^{\max}\|^2 \leq P/\kappa$, an optimal solution of (P1) is given by

$$\mathbf{s}_1^* = -\mathbf{s}_0^* = \sqrt{\kappa}\, \mathbf{w}^{\max}\,. \qquad \text{(Case 2)}$$

Otherwise, an optimal solution of (P1) is given by $\mathbf{s}_1^* = -\mathbf{s}_0^* = \mathbf{x}^*$, where $\mathbf{x}^*$ is characterized by the following necessary and sufficient conditions:

- *There exist $\lambda^* > 0$ and $\mu^* > 0$ such that $\mathbf{x}^*$ is an eigenvector of $\mathbf{A}_r - \lambda^* \mathbf{A}_e$ corresponding to its maximum eigenvalue, denoted as μ^*.*
- $\mathbf{x}^{*T} \mathbf{A}_e \mathbf{x}^* = \kappa$.
- $\|\mathbf{x}^*\|^2 = P$. (Case 3)

Proof: Since strong duality holds for (P2), the dual problem admits no gap with the optimal value. Lagrangian of (P2) is

$$\mathcal{L}(\mathbf{x}, \lambda, \mu) = \mathbf{x}^T (\mathbf{A}_r - \lambda \mathbf{A}_e - \mu \mathbf{I}) \mathbf{x} + \lambda\kappa + \mu P\,,$$

and the dual function is

$$g(\lambda, \mu) = \sup_{\mathbf{x}} \mathcal{L}(\mathbf{x}, \lambda, \mu) = \begin{cases} \lambda\kappa + \mu P & \text{if } \mathbf{A}_r - \lambda \mathbf{A}_e - \mu \mathbf{I} \preceq 0 \\ \infty & \text{otherwise} \end{cases}.$$

The dual problem is

$$\begin{aligned} \underset{\lambda \geq 0, \mu \geq 0}{\text{minimize}} \quad & \lambda\kappa + \mu P \\ \text{subject to} \quad & \mathbf{A}_r - \lambda \mathbf{A}_e - \mu \mathbf{I} \preceq 0 \,. \end{aligned} \tag{P3}$$

For a problem with strong duality, $\mathbf{x}^*$ and λ^*, μ^* are primal and dual optimal solutions if and only if $\mathbf{x}^*$ and λ^*, μ^* satisfy the Karush-Kuhn-Tucker (KKT) conditions. Hence, the point $\mathbf{x}^*$ maximizes $\mathcal{L}(\mathbf{x}, \lambda^*, \mu^*)$ over $\mathbf{x} \in \mathbb{R}^k$. For $\mathbf{A}_r - \lambda^* \mathbf{A}_e - \mu^* \mathbf{I} \preceq 0$, $\mathcal{L}(\mathbf{x}, \lambda^*, \mu^*)$ is maximized only if $\mathbf{x}^*$ is a solution to

$$\text{stationarity:} \quad (\mathbf{A}_r - \lambda^* \mathbf{A}_e - \mu^* \mathbf{I})\mathbf{x}^* = 0 \qquad . \tag{6}$$

Hence, $\mathbf{x}^*$ is an eigenvector of $\mathbf{A}_r - \lambda^* \mathbf{A}_e$ with the corresponding eigenvalue μ^*; or equivalently, $\mathbf{x}^*$ is a generalized eigenvector of $(\mathbf{A}_r - \mu^* \mathbf{I}, \mathbf{A}_e)$ with the corresponding generalized eigenvalue λ^*. Furthermore, from the dual problem (P3), it is seen that $\lambda\kappa + \mu P$ is minimized while satisfying $\mathbf{A}_r - \lambda \mathbf{A}_e - \mu \mathbf{I} \preceq 0$, which holds only if μ^* is the maximum eigenvalue of $\mathbf{A}_r - \lambda^* \mathbf{A}_e$; or equivalently, λ^* is the maximum generalized eigenvalue of $(\mathbf{A}_r - \mu^* \mathbf{I}, \mathbf{A}_e)$. The remaining KKT conditions are primal feasibility: $\mathbf{x}^{*T} \mathbf{A}_e \mathbf{x}^* \leq \kappa$ and $\|\mathbf{x}^*\|^2 \leq P$, dual feasibility: $\lambda^* \geq 0$ and $\mu^* \geq 0$, and complementary slackness: $\lambda^* \left(\mathbf{x}^{*T} \mathbf{A}_e \mathbf{x}^* - \kappa \right) = 0$ and $\mu^* (\|\mathbf{x}^*\|^2 - P) = 0$. Note that although $\mathbf{x} = 0$ is a solution of (6), it is not a solution of (P2) since in this case the complementary slackness condition requires $\lambda = 0$, $\mu = 0$, and it follows from the constraint in (P3) that $\mathbf{A}_r \preceq 0$ resulting in a contradiction. Based on these observations, an optimal solution to (P2) can be specified in three different cases:

Case 1: $\lambda^* = 0$, $\mu^* > 0$: In this case, $\mathbf{x}^*$ is chosen along an eigenvector of $\mathbf{A}_r$ corresponding to its maximum eigenvalue. Let $\mathbf{v}_r^{\max}$ denote such a unit-norm eigenvector. From complementary slackness, we also get $\|\mathbf{x}^*\|^2 = P$.

Therefore, $\mathbf{x}^* = \sqrt{P}\,\mathbf{v}_r^{\max}$. This solution will be optimal if it also satisfies the secrecy constraint, i.e., $\mathbf{x}^{*T}\mathbf{A}_e\mathbf{x}^* \leq \kappa$.

Case 2: $\lambda^* > 0$, $\mu^* = 0$: In this case, $\mathbf{x}^*$ is chosen along a generalized eigenvector of $(\mathbf{A}_r, \mathbf{A}_e)$ corresponding to the maximum generalized eigenvalue. Let $\mathbf{w}^{\max}$ denote such a generalized eigenvector, normalized to satisfy $(\mathbf{w}^{\max})^T\mathbf{A}_e\mathbf{w}^{\max} = 1$. Since $\mathbf{x}^{*T}\mathbf{A}_e\mathbf{x}^* = \kappa$ by complementary slackness, we get $\mathbf{x}^* = \sqrt{\kappa}\,\mathbf{w}^{\max}$. This solution will be optimal if the power constraint holds as well, i.e., $\|\mathbf{x}^*\|^2 \leq P$.

Case 3: $\lambda^* > 0$, $\mu^* > 0$: If a solution is not obtained from Cases 1 and 2, then by strong duality and the feasibility of the primal and the dual problems, the existence of $\mathbf{x}^*$ and $\lambda^* > 0$, $\mu^* > 0$ is guaranteed. In this case, $\mathbf{x}^*$ is chosen along an eigenvector of $\mathbf{A}_r - \lambda^*\mathbf{A}_e$ corresponding to its maximum eigenvalue μ^*. From complementary slackness, both constraints are satisfied with equality, i.e., $\mathbf{x}^{*T}\mathbf{A}_e\mathbf{x}^* = \kappa$ and $\|\mathbf{x}^*\|^2 = P$.

By the Lemma, $\mathbf{s}_1^* = -\mathbf{s}_0^* = \mathbf{x}^*$ yields an optimal solution of (P1). □

In the Proposition, the characterization of a solution to the optimal signal design problem is provided. While a closed form solution is not available, a numerical solution can be obtained efficiently by transforming the problem into the SDP form. To this end, it is noted that (P2) is equivalent to

$$\begin{aligned} &\underset{\mathbf{X}\in\mathbb{S}^{k\times k},\mathbf{x}\in\mathbb{R}^k}{\text{maximize}} \quad \operatorname{tr}(\mathbf{A}_r\mathbf{X}) \\ &\text{subject to } \operatorname{tr}(\mathbf{A}_e\mathbf{X}) \leq \kappa\,, \quad \operatorname{tr}(\mathbf{X}) \leq P\,, \text{ and } \mathbf{X} = \mathbf{x}\mathbf{x}^T\,, \end{aligned} \tag{P4}$$

where a new variable $\mathbf{X} = \mathbf{x}\mathbf{x}^T$ is introduced and the quadratic terms are expressed as $\mathbf{x}^T\mathbf{A}_i\mathbf{x} = \operatorname{tr}(\mathbf{A}_i\mathbf{x}\mathbf{x}^T) = \operatorname{tr}(\mathbf{A}_i\mathbf{X})$ for $i \in \{r, e\}$. The SDP relaxation

of (P4) (and hence (P2)) is given by:

$$\begin{aligned} &\underset{\mathbf{X}\in\mathbb{S}^{k\times k}}{\text{maximize}} \;\; \text{tr}(\mathbf{A}_r\mathbf{X}) \\ &\text{subject to} \;\; \text{tr}(\mathbf{A}_e\mathbf{X}) \leq \kappa\,, \quad \text{tr}(\mathbf{X}) \leq P\,, \;\text{and}\; \mathbf{X} \succeq 0\,. \end{aligned} \tag{P5}$$

It is straightforward to check that the SDP problem (P5) is the Lagrangian dual of the dual problem specified in (P3). Combining the strong duality between (P2) and (P3) with strong duality between the dual SDP's (P3) and (P5), it is concluded that strong duality holds between the original non-convex problem (P2) and the SDP problem (P5) (since (P2) is strictly feasible). Hence, an optimal solution of (P2) can be obtained from a matrix rank-one decomposition of a solution of its SDP relaxation specified in (P5).

4. Numerical Results and Concluding Remarks

In this section, we present some examples that illustrate the properties of an optimal solution specified in the Proposition. The simulations are performed in Matlab programming environment. The maximum (generalized) eigenvalue problem described in Case 1 (and respectively, Case 2) of the Proposition is solved using the *eig* command. The feasibility of the returned results is checked to see whether they satisfy the constraints. If the answer is in the affirmative, an optimal solution of (P2) is obtained such that only one of the two constraints is binding. If neither of the results obtained from Cases 1 and 2 of the Proposition is feasible, we proceed with Case 3 where a solution is obtained based on the SDP relaxation followed by a matrix rank-one decomposition. A solution of the corresponding SDP problem is obtained using CVX, a Matlab software package for specifying and solving

convex programs [19]. In the simulations, the positive definite matrix $\mathbf{A}_r$ (and likewise $\mathbf{A}_e$) is formed as $\mathbf{A}_r = \mathbf{Q}_r \mathbf{\Lambda} \mathbf{Q}_r^T$, where $\mathbf{Q}_r$ is a $k \times k$ orthonormal matrix obtained from the QR-decomposition of a random Gaussian matrix with zero-mean and unit variance independent and identically distributed entries, and $\mathbf{\Lambda}$ is a $k \times k$ diagonal matrix where its i-th diagonal entry for $i = 1, 2, \ldots, k$ is generated independently from the Rayleigh distribution with scale parameter i. The code is shared as supplementary material.

For illustrative purposes, in this part, the signal dimension is set as $k = 2$, while a solution can still be rapidly obtained in the case of higher dimensional signals owing to the polynomial complexity. The constraints in (P2) are set to $\kappa = 1$ (i.e., $\eta = 4$) and $P = 1$. Fig. 1 illustrates the three different cases that can be observed for the solution of the optimal signal design problem. Different values are assumed for $\mathbf{A}_r$ and $\mathbf{A}_e$ matrices in each case. All the points that satisfy the (first) eavesdropper constraint in (P2) reside inside the red ellipses. Likewise, all the points that satisfy the (second) power constraint in (P2) are located inside the green circles. The set of feasible points is the intersection of these two sets.

The value of the objective function at the optimal solution $\mathbf{x}^*$ is computed and the ellipse that is formed by all the points that yield the same value is plotted with blue color. The optimal signal pair $(\mathbf{s}_1^*, \mathbf{s}_0^*) = (\mathbf{x}^*, -\mathbf{x}^*)$ is depicted with bold asterisk. As expected, the optimal solution occurs at an extreme point of the feasible set. It can also be visually inferred that the value of the objective function, i.e., $\mathbf{x}^T \mathbf{A}_r \mathbf{x}$, is maximized at $\mathbf{x} = \mathbf{x}^*$. In other words, the ellipse characterized by the equation $\mathbf{x}^T \mathbf{A}_r \mathbf{x} = c$ attains its maximum value for c over the feasible set when $c^* = \mathbf{x}^{*T} \mathbf{A}_r \mathbf{x}^*$. Equivalently, c^* is the minimum value such that all points in the feasible set are contained within the ellipse described by the equation $\mathbf{x}^T \mathbf{A}_r \mathbf{x} = c^*$. For the example presented

in Fig. 1a, optimal signals are obtained as $\mathbf{s}_1^* = -\mathbf{s}_0^* = (-0.9908, 0.1351)$ and the eavesdropper constraint is not binding (i.e., Case 1 of the Proposition is optimal). For the example presented in Fig. 1b, optimal signals are obtained as $\mathbf{s}_1^* = -\mathbf{s}_0^* = (0.2269, 0.8015)$ and the power constraint is not binding (Case 2). Lastly, for the example presented in Fig. 1c, optimal signals are obtained as $\mathbf{s}_1^* = -\mathbf{s}_0^* = (0.9773, 0.2120)$ and both constraints are binding (Case 3).

Next, we present a contour plot for the maximum value of the objective function as a function of the constraint parameters κ and P. Similar to the previous part, positive definite matrices $\mathbf{A}_r$ and $\mathbf{A}_e$ are generated randomly. Fig. 2a depicts the solution of the optimal signal design problem for $\kappa = 1$ and $P = 1$. Then, for fixed $\mathbf{A}_r$ and $\mathbf{A}_e$, as the values of κ and P change, solution of the optimization problem visits all three cases yielding the contours of the maximum objective values plotted in Fig. 2b. Furthermore, based on this setting, the probabilities of error at the intended receiver and at the eavesdropper are plotted as functions of the power constraint in Fig. 3 by considering various secrecy constraints. The case of omitting the secrecy constraint (i.e., $\kappa = \infty$) is also included for comparison purposes. It is noted from the figure that, in compliance with the theoretical results, the probability of error at the intended receiver is affected by a given secrecy constraint after the transmit power exceeds a certain threshold. In particular, for $\kappa = 0.1$, the proposed framework enforces that the error probability at the eavesdropper is not smaller than 0.3759. In this case, for $P < 0.06$, the error probability at the eavesdropper is greater than 0.3759 (depicted with solid black color with dot markers in Fig. 3) meaning that this constraint is not binding and the error probability at the intended receiver (depicted with solid black color without markers in Fig. 3) decreases with increasing power limit by signaling along the eigenvector of $\mathbf{A}_r$ corresponding to the maximum

eigenvalue as specified in Case 1. For $P \geq 0.06$, the error probability constraint at the eavesdropper becomes active as well, i.e., $\mathrm{P}_e^{err} = 0.3759$. For $0.06 \leq P \leq 0.86$, it is seen that the error probability at the intended receiver still decreases with increasing power limit, but not as rapidly as the case that ignores the eavesdropper constraint, for which P_r^{err} and P_e^{err} are depicted with dotted brown curves without markers and with circular markers, respectively, in Fig. 3. In the interval $0.06 \leq P \leq 0.86$, both constraints are binding and Case 3 of the Proposition applies. Eventually, for $P > 0.86$, the power constraint becomes loose. The error probability at the intended receiver stays constant at 0.1023 as it cannot be decreased by solely increasing the power limit and without further decreasing the error probability constraint at the eavesdropper, corresponding to Case 2 of the Proposition.

As a final remark, we note that although the problem formulation can be generalized in a straightforward manner to the case of multiple eavesdroppers or uncertainty associated with eavesdropper matrix $\mathbf{A}_e$ (can be modeled to take values from a finite set), this would result in additional convex quadratic constraints in the proposed optimization problem and the developed techniques may not be generalized in a straightforward manner due to lack of strong duality results.

References

[1] H. V. Poor, An Introduction to Signal Detection and Estimation, Springer-Verlag, New York, 1994.

[2] X. Zhou, L. Song, Y. Zhang (Eds.), Physical Layer Security in Wireless Communications, CRC Press, 2013.

[3] Y. Liang, H. V. Poor, S. Shamai, Secure communication over fading channels, IEEE Trans. Inf. Theory (2008).

[4] Y. Liang, *et al.*, Capacity of cognitive interference channels with and without secrecy, IEEE Trans. Inf. Theory 55 (2009) 604–619.

[5] A. Ozcelikkale, T. M. Duman, Cooperative precoding and artificial noise design for security over interference channels, IEEE Signal Process. Lett. 22 (2015) 2234–2238.

[6] E. Mehdipour Abadi, *et al.*, Optimal power allocation and optimal linear encoding for parameter estimation in the presence of a smart eavesdropper, IEEE Trans. Signal Process. 70 (2022) 4093–4108.

[7] J. Guo, U. Rogers, X. Li, H. Chen, Secrecy constrained distributed detection in sensor networks, IEEE Trans. Signal Inf. Process. Netw. 4 (2018) 378–391.

[8] H. Xu, L. Sun, Encryption over the air: Securing two-way untrusted relaying systems through constellation overlapping, IEEE Trans. Wireless Commun. 17 (2018) 8268–8282.

[9] O. Ansari, M. Amin, Directional modulation techniques for secure wireless communication: A comprehensive survey, J. Wireless Com. Network 93 (2022).

[10] J. Kim, J. Kim, J. Lee, J. P. Choi, Physical-layer security against smart eavesdroppers: Exploiting full-duplex receivers, IEEE Access 6 (2018) 32945–32957.

[11] P. Moulin, V. V. Veeravalli, Statistical Inference for Engineers and Data Scientists, Cambridge University Press, 2018. doi:10.1017/9781107185920.

[12] T. M. Cover, J. A. Thomas, Elements of Information Theory, Wiley, New York, USA, 2006.

[13] S. Boyd, L. Vandenberghe, Convex Optimization, Cambridge University Press, Cambridge, UK, 2004.

[14] J. F. Sturm, S. Zhang, On cones of nonnegative quadratic functions, Math. Ope. Res. 28 (2003) 246–267.

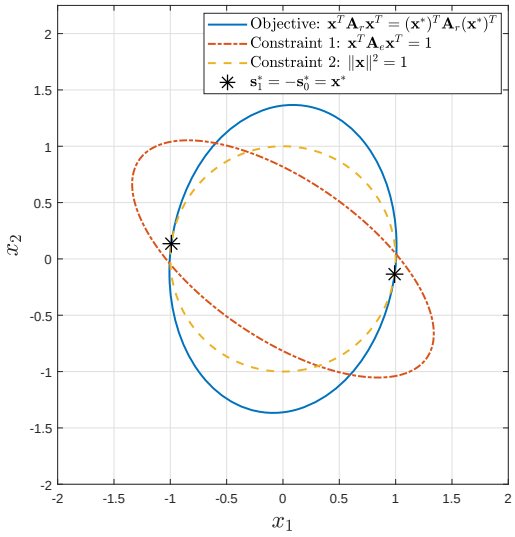
[15] M. Celis, J. Dennis, R. Tapia, A trust-region strategy for nonlinear equality constrained optimization, in: Numerical Optimization: Proc. SIAM Conf. Num. Optim., SIAM, 1985, pp. 71–82.

[16] J.-M. Peng, Y.-x. Yuan, Optimality conditions for the minimization of a quadratic with two quadratic constraints, SIAM J. Optim. 7 (1997) 579–594.

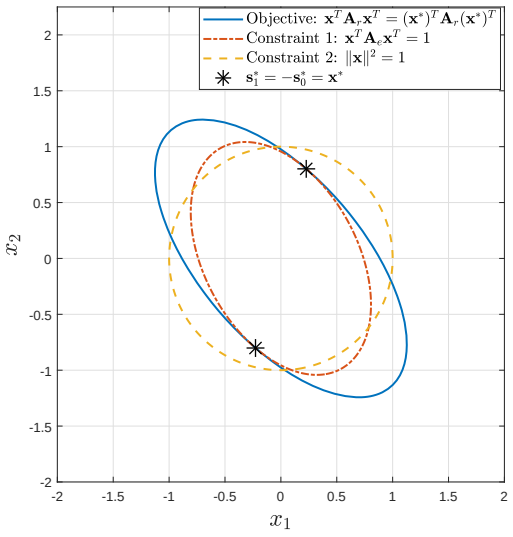
[17] Y.-X. Yuan, On a subproblem of trust region algorithms for constrained optimization, Math. Programming 47 (1990) 53–63.

[18] Y. Ye, S. Zhang, New results on quadratic minimization, SIAM J. Optim. 14 (2003) 245–267.

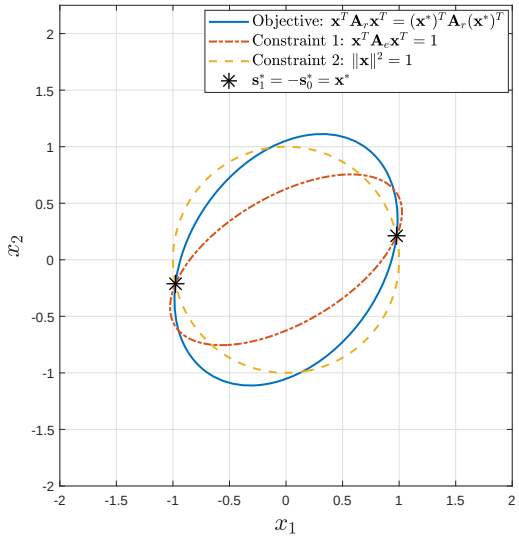
[19] M. Grant, S. Boyd, CVX: Matlab software for disciplined convex programming, version 2.2, `http://cvxr.com/cvx`, 2020.



(a) Case 1

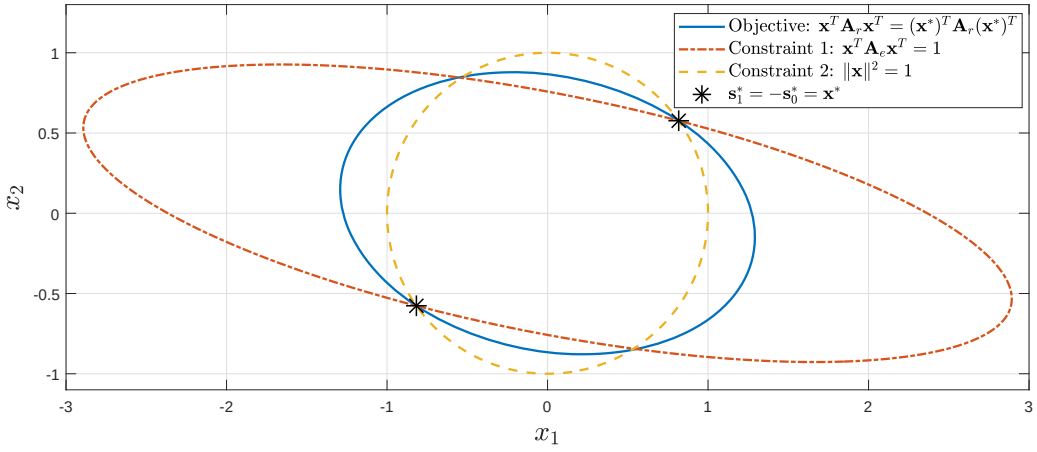


(b) Case 2

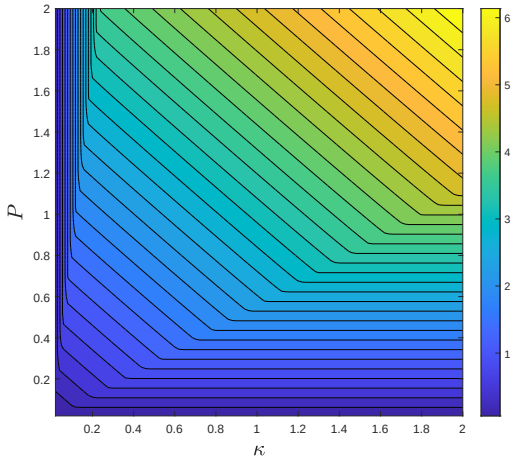


(c) Case 3

Figure 1: Solution of the optimal signal design problem illustrated for three different cases described in the Proposition using $\kappa = 1$ and $P = 1$.



(a)



(b)

Figure 2: (a) Optimal solution for $\kappa = 1$ and $P = 1$. (b) Contour plot for the maximum value of the objective function corresponding to optimal solution as a function of the constraint parameters κ and P.

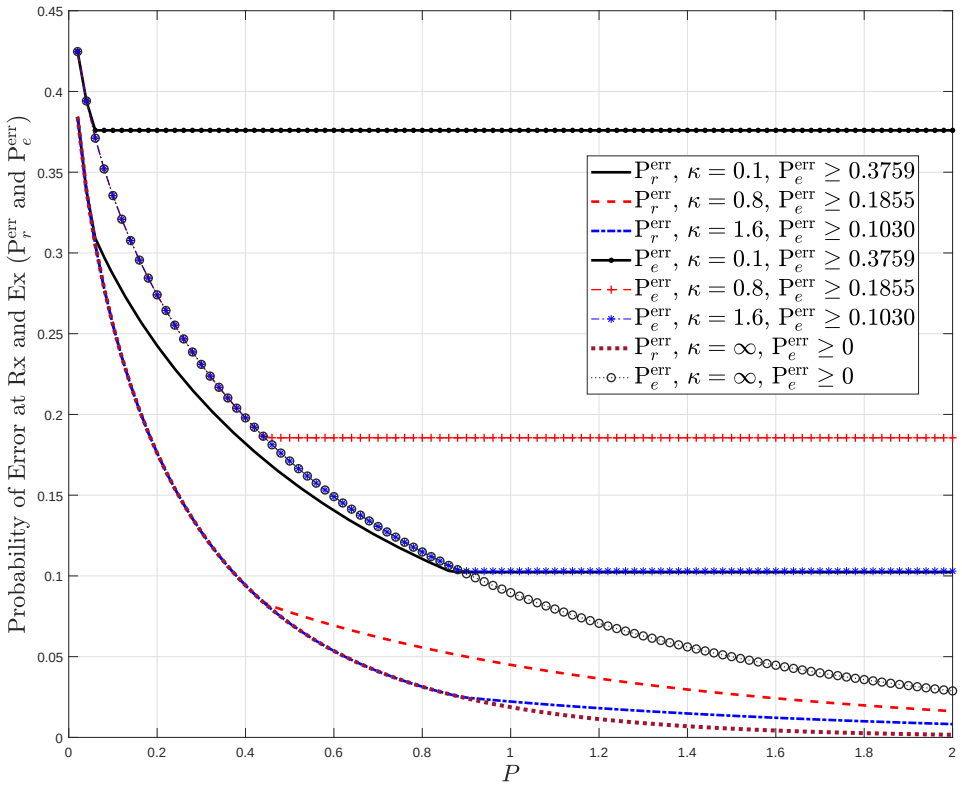


Figure 3: Probabilities of error at the intended receiver and at the eavesdropper versus the power limit P for various secrecy constraints.