

Joint RIS Phase Profile Design and Power Allocation for Parameter Estimation in Presence of Eavesdropping

Erfan Mehdipour Abadi^{1b}, *Graduate Student Member, IEEE*,
Ayda Nodel Hokmabadi^{1b}, *Graduate Student Member, IEEE*, and Sinan Gezici^{1b}, *Senior Member, IEEE*

Abstract—We consider secure transmission of a deterministic complex-valued parameter vector from a transmitter to an intended receiver in the presence of an eavesdropper in a reconfigurable intelligent surface (RIS)-integrated environment. We aim to jointly optimize the RIS phase profile and the power allocation matrix at the transmitter to enhance the estimation accuracy at the intended receiver while limiting that at the eavesdropper. We utilize the trace of the Fisher information matrix (FIM), equivalently, the average Fisher information, as the estimation accuracy metric, and obtain its closed form expression for the intended receiver and the eavesdropper. Accordingly, the joint RIS phase profile and power allocation problem is formulated, and it is solved via alternating optimization. When the power allocation matrix is fixed during alternating optimization, the optimal RIS phase profile design problem is formulated as a non-convex problem and it is solved via semidefinite relaxation and rank reduction. When the RIS phase profile is fixed, a linear programming formulation is obtained for optimal power allocation. Via simulations, the effects of RIS phase design and power allocation are illustrated individually and jointly. Moreover, extensions are provided by considering the presence of line of sight paths in the environment and the availability of RIS elements with adjustable magnitudes.

Index Terms—Estimation, fisher information, power allocation, reconfigurable intelligent surface (RIS), secrecy.

I. INTRODUCTION

A. Literature Review

SECURITY, cost-effectiveness, and energy efficiency are fundamental needs of beyond fifth-generation (B5G) and sixth-generation (6G) systems [1], [2], [3]. Due to the broadcasting nature of wireless channels and security vulnerability in wireless networks, eavesdropping is one of the significant concerns related to the security of B5G and 6G systems [4], [5], [6]. Key-based cryptographic approaches are extensively

studied to provide secrecy in the literature. Meanwhile, heterogeneous and dynamic networks cause a variety of challenges and cost-inefficiency in terms of key generation and distribution in these methods [7], [8]. For cost, power, latency, and bandwidth limitations of massive device networks, physical layer security (PLS) has attracted significant attention as an alternative to traditional approaches due to its information-theoretic security base and cryptography-free characteristics [9], [10]. The key idea behind PLS, first proposed by Wyner [11], is to securely transmit parameters to intended (legitimate) receivers in presence of eavesdroppers by exploiting their wireless channel characteristics [12].

In order to improve security with low power consumption and in a cost-efficient way, reconfigurable intelligent surfaces (RISs) have recently attracted significant research attention. RIS is a planar surface with a programmable structure equipped with low-cost and passive meta-surface components. An RIS can alter the propagation direction of electromagnetic waves by appropriately shifting the phases of signals without any additional equipment such as RF processing [13], [14], whereby the security can be increased by manipulating the channel characteristics of the intended receiver and the eavesdropper [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28]. For PLS purposes, different types of metrics, such as information, detection, or estimation theoretic metrics, are used in the literature to quantify the amount of secrecy.

Information theoretic metrics commonly consist of mutual information, secrecy rate (SR), secrecy outage probability (SOP), and secrecy capacity (SC). [11] shows that a non-zero SR is achievable at the intended receiver providing zero information to the eavesdropper if the channel of the eavesdropper is a degraded version of that of the intended receiver. In addition, [29] and [30] utilize artificial noise (AN) and beamforming in order to maximize the secrecy communication rate. In [15], [16], [17], [18], [19], [20], integration of RIS into a multi-input single-output (MISO) system is studied for maximizing the achievable SR, SR, minimum SR, and weighted sum SR with the combination of linear precoding, beamforming, and power allocation by considering delay-limitations for quality of service (QoS). [21] and [22] aim to minimize the transmitted power and maximize the harvested power of the receiver subject to the SR constraint, while [23] focuses on minimizing the transmitted

Manuscript received 19 September 2023; revised 18 April 2024 and 7 August 2024; accepted 12 August 2024. Date of publication 16 August 2024; date of current version 19 December 2024. The review of this article was coordinated by Dr. Balasubramaniam Natarajan. (Corresponding author: Sinan Gezici.)

Erfan Mehdipour Abadi is with Wayne State University, Detroit, MI 48202 USA (e-mail: mehdipour.erfan96@gmail.com).

Ayda Nodel Hokmabadi and Sinan Gezici are with the Department of Electrical and Electronics Engineering, Bilkent University, Ankara 06800, Türkiye (e-mail: nodel@ee.bilkent.edu.tr; gezici@ee.bilkent.edu.tr).

Digital Object Identifier 10.1109/TVT.2024.3445114

power subject to SR and SOP constraints. Moreover, in [24], achievable SR is maximized with AN, precoding, and RIS phase shifts in a multiple-input multiple-output (MIMO) system, and [25] performs joint optimization of beamforming and RIS phase shifts in order to maximize the SR in a MIMO system. Also, [26] aims to maximize the achievable ergodic rate under the QoS constraint by joint optimization of AN and RIS phase shifts in a MIMO system. Meanwhile, the ergodic secrecy rate in a single-input single-output (SISO) system is maximized in [27] via optimization of RIS phase shifts. Furthermore, the average worst-case SR of a simultaneous wireless information and power transfer (SWIPT) system is investigated in [28] for joint optimization of beamforming and RIS phase shifts. SOP is adopted as a secrecy metric in various settings such as [31], [32], [33], and the studies in [34], [35], [36], [37] consider integration of RIS into SISO systems and derive analytical expressions for SOP, average SR, and non-zero SR. Besides, [38] formulates the SOP minimization problem via joint optimization of beamforming and RIS phase shifts in multiple-input multiple-output multiple-antenna-eavesdropper (MIMOME) channels. SC is another secrecy metric that is utilized in the literature. For example, [39] considers the SC in a RIS-integrated SISO system in a measurement-based manner. Also, [40] formulates the average SC in a RIS-integrated SISO system and [41] adjusts the SC for a high-speed railway system for joint beamforming and RIS phase shift design.

For secure information transmission, estimation theoretic metrics, such as Fisher information, mean-squared error (MSE), and Cramér-Rao lower bound (CRLB), are also employed in various work in the literature. CRLB provides a lower bound on MSEs of unbiased estimators and is derived from the inverse of the Fisher information matrix (FIM) [42]. In [43], a secure inference problem is introduced for an Internet of Things (IoT) network with sufficient data for deterministic parameter estimation under spoofing and man-in-the-middle attack (MiMA) based on the CRLB metric. In [44], [45], [46], [47], [48], secure estimation of a random parameter is investigated in the presence of an eavesdropper in various scenarios and setups. In particular, in [44] and [46], minimization of the expectation of the conditional Cramér-Rao lower bound (ECRLB) at the intended receiver is performed by optimizing the deterministic encoding at the transmitter for random scalar and vector parameters under the condition that the linear minimum mean-squared error (LMMSE) of the eavesdropper is above a specific secrecy bound. Moreover, [45] proposes the worst-case CRLB of the parameter as a performance metric for achieving robust parameter encoding. In [47], optimal power allocation (OPA) for secure estimation of vector parameters is proposed under a total power constraint while keeping the MSE of the eavesdropper above a certain value by assuming the use of the maximum likelihood (ML) estimator at the eavesdropper. In the aforementioned studies, it is assumed that the eavesdropper is not aware of encoding at the transmitter. On the other hand, in [48], OPA and optimal linear encoding (OLE) are proposed by assuming that the eavesdropper is aware of the encoding at the transmitter (i.e., a smart eavesdropper), which presents a worst-case scenario for the estimation performance of the intended receiver. By considering the CRLB and the determinant of the FIM as the

estimation accuracy metrics, OPA and OLE are performed under power and secrecy constraints in [48]. In another line of work, CRLB is used in various RIS-integrated setups for improvement of system performance in the absence of eavesdropping. In [49], the goal is to minimize the multi-user interference (MUI) in a MISO system, while RIS elements have constant-modulus and discrete phase values under the CRLB constraint for direction of arrival (DOA) estimation. In addition, [50] investigates joint optimization of beamforming and RIS phase profile for minimizing the CRLB of point and extended targets. Investigation of FIM and CRLB for RIS-integrated systems requires analysis for complex parameters, and the derivation of FIM and CRLB for complex parameters can be found in [51], [52].

Estimation theoretic metrics for physical layer security are not limited to the CRLB. Other metrics, such as total MMSE, average MSE, and Fisher information, are also used to quantify the secrecy of various systems [53], [54], [55]. Specifically, in [54], a Bayesian framework with a Gaussian prior distribution for both intended receivers and eavesdroppers is considered, where the total MMSE of the intended receivers is minimized under a constraint on the MMSE at the eavesdroppers using joint AN and linear encoding. Additionally, for distributed parameter estimation, optimal transmit power allocation policies are derived in [55] when the employed metrics are the average MSEs of the parameter of interest at the eavesdroppers. Furthermore, [53] adopts a non-Bayesian parameter estimation framework for ensuring the privacy of smart meter data in a smart grid network based on the Fisher information metric, namely, the Fisher information for a single variable and the trace of the FIM for the multi-variable parameter estimation problem. Moreover, in [56], [57], the trace and the log-determinant of the Bayesian FIM are introduced as other useful metrics for estimation problems without considering any eavesdroppers in the system.

B. Contributions

Secure parameter transmission problems have been investigated in various studies in the literature, e.g., [44], [45], [46], [47], [48], [54], by utilizing various estimation theoretic metrics, such as the CRLB and MSE, and considering both random and deterministic parameters. In these studies, optimal parameter encoding and optimal power allocation problems are formulated for enhancing the estimation accuracy at an intended receiver while imposing a constraint on estimation accuracy of eavesdropping. A recent advancement in communication systems is the introduction of RIS, which can play a vital role in system performance improvement through proper control of its elements. Although secure parameter transmission problems have been investigated in the aforementioned studies from an estimation theoretic perspective, there exists no work in the literature that considers the presence of an RIS in a secure parameter transmission system and performs joint optimization of RIS phase profile and power allocation based on estimation theoretic metrics.

In this manuscript, we propose a secure parameter transmission problem in the presence of an RIS in order to enhance estimation accuracy of an intended receiver while keeping

the estimation accuracy of an eavesdropper below a certain limit. To this aim, we formulate a problem that involves the joint optimization of power allocation and RIS phase profile according to the average Fisher information metric. Namely, by considering a deterministic and complex-valued unknown parameter vector, the objective is to maximize the trace of the FIM at the intended receiver under the constraints that the trace of the FIM is below a certain limit for the eavesdropper, the reflection coefficients of the RIS elements have unit amplitudes, and the total transmit power is limited by a certain value. By deriving a closed form expression for the trace of the FIM, we formulate the joint power allocation and RIS phase profile design problem, and propose an alternating optimization approach to solve it. During alternating optimization, when power allocation is fixed, the optimal RIS phase profile design problem is formulated as a non-convex problem, and it has been solved via semidefinite relaxation (SDR) and rank reduction. When the RIS phase profile is fixed, a linear programming formulation is obtained for optimal power allocation. Although it is initially assumed that the transmitter is in non-line-of-sight (NLoS) with both the intended receiver and the eavesdropper, extensions are also provided by considering the presence of line-of-sight paths in the environment. Moreover, the problem formulation is also extended to the scenario when the RIS elements have reflection coefficients with adjustable magnitudes. The key contributions and novelty of this manuscript can be outlined as follows:

- For the first time in the literature, we propose a joint RIS phase profile design and power allocation problem for secure transmission of a complex-valued parameter vector in an RIS-integrated environment to maximize the average Fisher information at the intended receiver while ensuring that the average Fisher information at the eavesdropper remains below a predefined threshold. These objectives are accomplished under the total transmit power constraint and the requirement of unit-modulus reflection coefficients for the RIS elements.
- FIMs are explicitly derived for the intended receiver and the eavesdropper regarding the estimation of a complex-valued parameter vector in an RIS-integrated environment.
- An alternating optimization solution is proposed for obtaining the (sub)optimal power allocation and RIS phase profile. During alternating optimization, for fixed power allocation, the optimal RIS phase profile design problem is formulated as a non-convex problem, which is solved via SDR and rank reduction. On the other hand, for a fixed RIS phase profile, a linear programming formulation is obtained for optimal power allocation.
- It is shown that the results obtained for the NLoS scenario can also be extended to cases in the presence of LoS paths in the environment via homogenizing the optimization problem developed for the NLoS scenario.
- It is shown that the unit modulus constraint imposed on the RIS elements can lead to infeasibility problems in some cases, particularly when the secrecy constraint is set to low values. However, when the RIS elements have reflection coefficients with adjustable magnitudes, this infeasibility

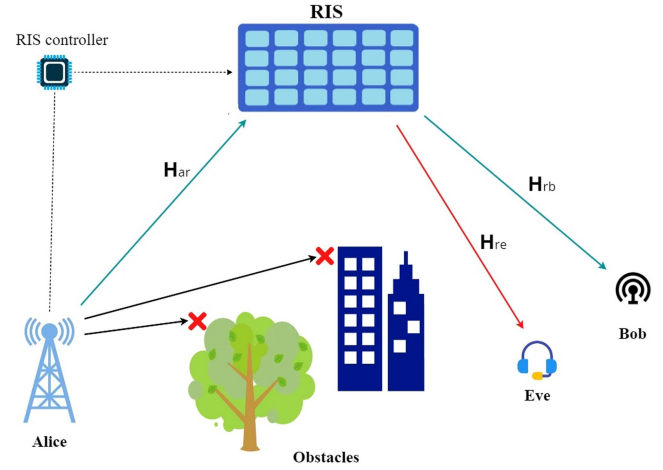


Fig. 1. RIS-assisted system in the presence of an eavesdropper.

issue is resolved and the problem formulation is extended to cover this scenario, as well.

C. Organization

The remainder of the manuscript is structured as follows. Section II provides a description of the system model and introduces the problem formulation. In Section III, the proposed approaches for RIS phase profile design and power allocation are developed by considering the average Fisher information criterion. Section IV presents various numerical examples for investigating the performance of the proposed approaches. Section V extends the theoretical results to account for the presence of dominant LoS components and RIS elements with adjustable magnitudes. Finally, concluding remarks are made in Section VI.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A k -dimensional complex parameter vector denoted by $\theta = [\theta_1, \theta_2, \dots, \theta_k]^T \in \mathbb{C}^k$ is to be sent from a transmitter, Alice, to an intended receiver, Bob, in the presence of an eavesdropper, Eve, when the LoS paths are blocked by obstacles, as depicted in Fig. 1. By assuming no prior statistical information about θ at the intended receiver and the eavesdropper, θ is modeled as a deterministic unknown parameter vector for Bob and Eve. The aim is to improve the parameter estimation performance at Bob while keeping that below a particular limit at Eve by designing a proper RIS phase profile in the smart radio environment and performing optimal power allocation at the transmitter (Alice). It is assumed that the transmitter has a reliable connection to the RIS for adjusting the phases of the RIS elements, as shown in Fig. 1.

Measurements are obtained at Bob and Eve via the following linear models [16], [58]:

$$\mathbf{y}_b = (\mathbf{H}_{rb}\mathbf{\Omega}\mathbf{H}_{ar}) \mathbf{P}\theta + \eta_b \quad (1)$$

$$\mathbf{y}_e = (\mathbf{H}_{re}\mathbf{\Omega}\mathbf{H}_{ar}) \mathbf{P}\theta + \eta_e \quad (2)$$

where $\mathbf{y}_b \in \mathbb{C}^{n_b}$ and $\mathbf{y}_e \in \mathbb{C}^{n_e}$ denote the measurements at Bob and Eve, respectively. Also, $\mathbf{H}_{ar} \in \mathbb{C}^{r \times k}$, $\mathbf{H}_{rb} \in \mathbb{C}^{n_b \times r}$, and $\mathbf{H}_{re} \in \mathbb{C}^{n_e \times r}$ are channel coefficient matrices

for Alice-RIS, RIS-Bob, and RIS-Eve channels, respectively, and k , n_b , n_e , and r are the size of the parameter vector, the number of antenna elements at Bob, the number of antenna elements at Eve, and the number of RIS elements, respectively. Also, $\boldsymbol{\eta}_b \in \mathbb{C}^{n_b}$ and $\boldsymbol{\eta}_e \in \mathbb{C}^{n_e}$ are additive circularly-symmetric Gaussian noise vectors at Bob and Eve, with distributions $\boldsymbol{\eta}_b \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Sigma}_b)$ and $\boldsymbol{\eta}_e \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Sigma}_e)$, respectively, where $\boldsymbol{\Sigma}_b$ and $\boldsymbol{\Sigma}_e$ are the covariance matrices, which are assumed to be positive definite. In addition, $\mathbf{P} = \text{diag}\{\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_k}\}$ and $\boldsymbol{\Omega} = \text{diag}\{\omega_1, \omega_2, \dots, \omega_r\}$ are, respectively, the power allocation matrix and the RIS phase profile to be optimized, where p_j 's are non-negative real numbers for $j = 1, 2, \dots, k$ and $\omega_i = e^{j\phi_i}$ for $i = 1, 2, \dots, r$ with ϕ_i denoting the phase of the i th RIS element. It is assumed that the channels are slowly fading with the channel coefficients being constant for a specific time interval.¹

In this study, the aim is to design the RIS phase profile, $\boldsymbol{\Omega}$, and the power allocation matrix, $\mathbf{P}$, for enhancing the estimation performance at the intended receiver, Bob, while keeping the estimation performance at the eavesdropper, Eve, below a particular limit. For quantifying estimation performance, Fisher information based optimality criteria can be preferred as they do not depend on specific estimator structures and lead to compact expressions [57], [59], [60], [61], [62]. The most commonly used Fisher information based optimality criteria are the trace of the inverse FIM, i.e., the Cramér-Rao lower bound (CRLB), the log-determinant of the FIM, the maximum eigenvalue of the CRLB, the largest diagonal entry of the CRLB, the trace of the FIM, and the minimum diagonal element of the FIM [57], [59], [60].² Among these optimality criteria, we employ the trace of the FIM (i.e., the average Fisher information criterion) in this study due to two main reasons: *i*) Since the informativeness of the measurement for estimating the i th element of the parameter vector corresponds to the i th diagonal entry of the FIM, the trace of the FIM indicates the overall usefulness of the measurement for vector parameter estimation [57]. *ii*) For the considered problem, the trace of the FIM can be derived in closed form, which facilitates theoretical analyses and provides intuition.

Let $\mathbf{I}(\mathbf{y}_b; \boldsymbol{\theta})$ and $\mathbf{I}(\mathbf{y}_e; \boldsymbol{\theta})$, denote, respectively, the FIMs corresponding to measurements $\mathbf{y}_b$ and $\mathbf{y}_e$, with respect to the complex parameter vector $\boldsymbol{\theta}$ (which will be derived in Section III). Based on these FIMs and by considering the trace of FIM as the performance metric, the following problem formulation is proposed.

$$\max_{\mathbf{P} \in \mathcal{D}^{k \times k}, \boldsymbol{\Omega} \in \tilde{\mathcal{D}}^{r \times r}} \text{tr}\{\mathbf{I}(\mathbf{y}_b; \boldsymbol{\theta})\} \quad (3a)$$

$$\text{s.t.} \quad \text{tr}\{\mathbf{I}(\mathbf{y}_e; \boldsymbol{\theta})\} \leq \Delta \quad (3b)$$

¹There is no assumption related to the correlation among the channel matrices since the proposed RIS phase profile design and power allocation problems in (3)–(5) will be solved for fixed (given) channel matrices. That is, having correlated or uncorrelated channels does not affect the formulations; they can just change the resulting parameter estimation performance under the secrecy constraint.

²The CRLB, the log-determinant of the FIM, the maximum eigenvalue of the CRLB, and the largest diagonal entry of the CRLB are also referred as A-optimality, D-optimality, E-optimality, and G-optimality criteria, respectively [57], [59], [60].

$$\text{tr}\{\mathbf{P}\mathbf{P}^T\} \leq P_\Sigma \quad (3c)$$

$$\mathbf{P}\mathbf{P}^T \succeq \mathbf{0} \quad (3d)$$

$$|[\boldsymbol{\Omega}]_{\ell, \ell}| = 1, \ell = 1, \dots, r \quad (3e)$$

where $\mathcal{D}^{k \times k}$ denotes the set of $k \times k$ real diagonal matrices, $\tilde{\mathcal{D}}^{r \times r}$ represents the set of $r \times r$ complex diagonal matrices, (3b) corresponds to the secrecy constraint with $0 \leq \Delta < \infty$ denoting the secrecy limit, (3d) and (3e) impose, respectively, non-negativity of power levels and the total power constraint at Alice with $0 < P_\Sigma < \infty$ representing the power limit, and (3e) states the unit amplitude nature of the RIS phase profile. It is noted that unlike the physical-layer security problem formulations for communications systems, information leakage is not defined with respect to the information at Bob. Namely, the information leaked to Eve is specified by the average Fisher information at Eve, which is an estimation theoretic measure.

As (3) is very challenging to solve directly, we employ an alternative optimization approach [15], [16], [21], [38], [63], and divide the problem into two separate problems. First, the optimal RIS phase profile is designed by considering a given power allocation matrix based on the following problem:

$$\max_{\boldsymbol{\Omega} \in \tilde{\mathcal{D}}^{r \times r}} \text{tr}\{\mathbf{I}(\mathbf{y}_b; \boldsymbol{\theta})\} \quad (4a)$$

$$\text{s.t.} \quad \text{tr}\{\mathbf{I}(\mathbf{y}_e; \boldsymbol{\theta})\} \leq \Delta \quad (4b)$$

$$|[\boldsymbol{\Omega}]_{\ell, \ell}| = 1, \ell = 1, \dots, r \quad (4c)$$

Then, the optimal power allocation matrix is derived for a given RIS phase profile via the following formulation:

$$\max_{\mathbf{P} \in \mathcal{D}^{k \times k}} \text{tr}\{\mathbf{I}(\mathbf{y}_b; \boldsymbol{\theta})\} \quad (5a)$$

$$\text{s.t.} \quad \text{tr}\{\mathbf{I}(\mathbf{y}_e; \boldsymbol{\theta})\} \leq \Delta \quad (5b)$$

$$\text{tr}\{\mathbf{P}\mathbf{P}^T\} \leq P_\Sigma \quad (5c)$$

$$\mathbf{P}\mathbf{P}^T \succeq \mathbf{0} \quad (5d)$$

We can obtain the solution of (3) via an alternating optimization approach by solving the problems in (4) and (5) iteratively. Detailed investigations are provided in the following sections.³

III. RIS PHASE PROFILE DESIGN AND POWER ALLOCATION BASED ON AVERAGE FISHER INFORMATION CRITERION

In this section, we first derive the FIM and calculate the trace of the FIM explicitly. Then, we obtain the sub-optimal RIS phase profile and optimal power allocation matrix in different subsections. Finally, we focus on the joint alternating optimization problem in the last part.

According to (1) and (2), the conditional distributions of the measurements at Bob and Eve can be written as $\mathbf{y}_b | \boldsymbol{\theta} \sim \mathcal{CN}((\mathbf{H}_{rb}\boldsymbol{\Omega}\mathbf{H}_{ar})\mathbf{P}\boldsymbol{\theta}, \boldsymbol{\Sigma}_b)$ and $\mathbf{y}_e | \boldsymbol{\theta} \sim \mathcal{CN}((\mathbf{H}_{re}\boldsymbol{\Omega}\mathbf{H}_{ar})\mathbf{P}\boldsymbol{\theta}, \boldsymbol{\Sigma}_e)$, respectively. Since the parameters

³As the channels are slowly fading, we can consider a block fading scenario where the channel coefficients are constant for a block of transmissions and solve the proposed optimization problem for each block.

are complex-valued, the FIMs related to the measurements can be calculated based on the following formula [51], [64]:

$$\mathbf{I}(\mathbf{y}_i; \underline{\boldsymbol{\theta}}) = \mathbb{E} \left\{ \left[\frac{\partial \ln(p_{\boldsymbol{\theta}}(\mathbf{y}_i))}{\partial \underline{\boldsymbol{\theta}}^*} \right] \left[\frac{\partial \ln(p_{\boldsymbol{\theta}}(\mathbf{y}_i))}{\partial \underline{\boldsymbol{\theta}}^*} \right]^H \right\} \quad (6)$$

for $i \in \{b, e\}$, where $\underline{\boldsymbol{\theta}} \triangleq [\boldsymbol{\theta}^T \boldsymbol{\theta}^H]^T$, $\boldsymbol{\theta}^*$ denotes the conjugate of $\boldsymbol{\theta}$, and $p_{\boldsymbol{\theta}}(\mathbf{y}_b)$ and $p_{\boldsymbol{\theta}}(\mathbf{y}_e)$ are the likelihood functions of the measurements at Bob and Eve, respectively. Based on the expression in (6), the FIMs at Bob and Eve can be obtained as in the following lemma.

Lemma 1: The FIMs at Bob and Eve can be expressed as in (7) at the bottom of the page for $i \in \{b, e\}$.

Proof: The probability density function of a circularly symmetric complex Gaussian random vector $\mathbf{Z} \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Sigma}_z)$ can be written as [65]

$$p(\mathbf{z}) = \frac{1}{\pi^n \det(\boldsymbol{\Sigma}_z)} e^{-\mathbf{z}^H \boldsymbol{\Sigma}_z^{-1} \mathbf{z}} \quad (8)$$

where $\boldsymbol{\Sigma}_z = \mathbb{E}\{\mathbf{Z}\mathbf{Z}^H\}$ and $\mathbb{E}\{\mathbf{Z}\mathbf{Z}^T\} = \mathbf{0}$. By employing (8) for $\boldsymbol{\eta}_b$ in (1) and $\boldsymbol{\eta}_e$ in (2), $p_{\boldsymbol{\theta}}(\mathbf{y}_b)$ and $p_{\boldsymbol{\theta}}(\mathbf{y}_e)$ can be obtained, and the derivatives required for (6) can be written as follows [51], [66, eqns. (81), (82)]:

$$\begin{aligned} \frac{\partial \ln(p_{\boldsymbol{\theta}}(\mathbf{y}_i))}{\partial \boldsymbol{\theta}} &= \frac{\partial}{\partial \boldsymbol{\theta}} \left(-(\mathbf{y}_i - \mathbf{H}_i \boldsymbol{\theta})^H \boldsymbol{\Sigma}_{n_i}^{-1} (\mathbf{y}_i - \mathbf{H}_i \boldsymbol{\theta}) \right) \\ &= [-(\mathbf{y}_i - \mathbf{H}_i \boldsymbol{\theta})^H \boldsymbol{\Sigma}_{n_i}^{-1} (-\mathbf{H}_i)]^T \\ &= \mathbf{H}_i^T \boldsymbol{\Sigma}_{n_i}^{-1} (\mathbf{y}_i - \mathbf{H}_i \boldsymbol{\theta})^*, \end{aligned} \quad (9)$$

$$\begin{aligned} \frac{\partial \ln(p_{\boldsymbol{\theta}}(\mathbf{y}_i))}{\partial \boldsymbol{\theta}^*} &= \frac{\partial}{\partial \boldsymbol{\theta}^*} \left((\mathbf{y}_i - \mathbf{H}_i \boldsymbol{\theta})^H \boldsymbol{\Sigma}_{n_i}^{-1} (\mathbf{y}_i - \mathbf{H}_i \boldsymbol{\theta}) \right) \\ &= \mathbf{H}_i^H \boldsymbol{\Sigma}_{n_i}^{-1} (\mathbf{y}_i - \mathbf{H}_i \boldsymbol{\theta}) \end{aligned} \quad (10)$$

where $\mathbf{H}_i \triangleq \mathbf{H}_{ri} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P}$. By defining $l_i \triangleq \ln(p_{\boldsymbol{\theta}}(\mathbf{y}_i))$ and inserting the results in (9) and (10) into (6), the following expressions can be obtained:

$$\begin{aligned} \mathbf{I}(\mathbf{y}_i; \underline{\boldsymbol{\theta}}) &= \mathbb{E} \left\{ \begin{bmatrix} \left[\frac{\partial l_i}{\partial \boldsymbol{\theta}^*} \right] & \left[\frac{\partial l_i}{\partial \boldsymbol{\theta}^*} \right]^H \\ \left[\frac{\partial l_i}{\partial \boldsymbol{\theta}} \right] & \left[\frac{\partial l_i}{\partial \boldsymbol{\theta}} \right]^H \end{bmatrix} \right\} \\ &= \mathbb{E} \left\{ \begin{bmatrix} \left(\frac{\partial l_i}{\partial \boldsymbol{\theta}^*} \right) \left(\frac{\partial l_i}{\partial \boldsymbol{\theta}^*} \right)^H & \left(\frac{\partial l_i}{\partial \boldsymbol{\theta}^*} \right) \left(\frac{\partial l_i}{\partial \boldsymbol{\theta}} \right)^H \\ \left(\frac{\partial l_i}{\partial \boldsymbol{\theta}} \right) \left(\frac{\partial l_i}{\partial \boldsymbol{\theta}^*} \right)^H & \left(\frac{\partial l_i}{\partial \boldsymbol{\theta}} \right) \left(\frac{\partial l_i}{\partial \boldsymbol{\theta}} \right)^H \end{bmatrix} \right\} \\ &= \begin{bmatrix} \mathbf{H}_i^H \boldsymbol{\Sigma}_{n_i}^{-1} \mathbb{E} \{ \boldsymbol{\eta}_i \boldsymbol{\eta}_i^H \} \boldsymbol{\Sigma}_{n_i}^{-1*} \mathbf{H}_i & \mathbf{H}_i^H \boldsymbol{\Sigma}_{n_i}^{-1} \mathbb{E} \{ \boldsymbol{\eta}_i \boldsymbol{\eta}_i^T \} \boldsymbol{\Sigma}_{n_i}^{-1*} \mathbf{H}_i^* \\ \mathbf{H}_i^T \boldsymbol{\Sigma}_{n_i}^{-1} \mathbb{E} \{ \boldsymbol{\eta}_i^* \boldsymbol{\eta}_i^H \} \boldsymbol{\Sigma}_{n_i}^{-1*} \mathbf{H}_i & \mathbf{H}_i^T \boldsymbol{\Sigma}_{n_i}^{-1} \mathbb{E} \{ \boldsymbol{\eta}_i^* \boldsymbol{\eta}_i^T \} \boldsymbol{\Sigma}_{n_i}^{-1*} \mathbf{H}_i^* \end{bmatrix}. \end{aligned} \quad (11)$$

Since $\boldsymbol{\eta}_b$ and $\boldsymbol{\eta}_e$ are circularly symmetric complex Gaussian random vectors, it is known that $\mathbb{E}\{\boldsymbol{\eta}_i \boldsymbol{\eta}_i^T\} = \mathbf{0}$ and $\mathbb{E}\{\boldsymbol{\eta}_i \boldsymbol{\eta}_i^H\} =$

$\boldsymbol{\Sigma}_i$. Also, it is noted that $\mathbb{E}\{\boldsymbol{\eta}_i^* \boldsymbol{\eta}_i^T\} = \mathbb{E}\{(\boldsymbol{\eta}_i \boldsymbol{\eta}_i^H)^*\} = \boldsymbol{\Sigma}_i^*$. Thus, the proof is completed by inserting these values into the final expression in (11). ■

Since the first half of the parameter vector $\underline{\boldsymbol{\theta}}$ corresponds to the main parameter $\boldsymbol{\theta}$ of interest, we focus on the trace of the first $k \times k$ block of the FIM in (7) shown at the bottom of this page of Lemma 1. Accordingly, the trace of the FIM related to $\boldsymbol{\theta}$ can be calculated, for $i \in \{b, e\}$, as follows:

$$\text{tr}\{\mathbf{I}(\mathbf{y}_i; \boldsymbol{\theta})\} = \text{tr}\{(\mathbf{H}_{ri} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P})^H \boldsymbol{\Sigma}_i^{-1*} (\mathbf{H}_{ri} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P})\} \quad (12)$$

Since $\boldsymbol{\Sigma}_i$ is positive definite for $i \in \{b, e\}$, the overall matrix in the trace operator in (12) has real-valued diagonal elements (as it can be expressed as the multiplication of a complex matrix with its Hermitian transpose). Therefore, taking the conjugate of the matrix inside trace operator in (12) results in the same trace; i.e.,

$$\text{tr}\{\mathbf{I}(\mathbf{y}_i; \boldsymbol{\theta})\} = \text{tr}\{(\mathbf{H}_{ri} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P})^T \boldsymbol{\Sigma}_i^{-1} (\mathbf{H}_{ri} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P})^*\} \quad (13)$$

In addition, since $\text{tr}\{\mathbf{A}\} = \text{tr}\{\mathbf{A}^T\}$, (13) can also be stated as

$$\text{tr}\{\mathbf{I}(\mathbf{y}_i; \boldsymbol{\theta})\} = \text{tr}\{(\mathbf{H}_{ri} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P})^H \boldsymbol{\Sigma}_i^{-1} (\mathbf{H}_{ri} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P})\} \quad (14)$$

which is considered as the performance metric to quantify the estimation accuracy.

Remark 1: For the proposed optimal RIS design and power allocation problem in (3) (similarly for (4) and (5)), the transmitter is assumed to know the channel coefficients (i.e., $\mathbf{H}_{ar}$, $\mathbf{H}_{rb}$, and $\mathbf{H}_{re}$), and the covariance matrices ($\boldsymbol{\Sigma}_b$ and $\boldsymbol{\Sigma}_e$), as can be noted from (14). As the transmitter and the intended receiver are cooperating, information about $\mathbf{H}_{ar}$, $\mathbf{H}_{rb}$, and $\boldsymbol{\Sigma}_b$ can be obtained by the transmitter via conventional estimation and feedback procedures. For learning $\mathbf{H}_{re}$ and $\boldsymbol{\Sigma}_e$, the transmitter is required to have some information about the location of the eavesdropper, the channel model in the environment, and the receiver at the eavesdropper. If $\mathbf{H}_{re}$ and $\boldsymbol{\Sigma}_e$ can be learned perfectly, the analysis in this manuscript applies directly. On the other hand, in the case of imperfect information, the inaccuracy about $\mathbf{H}_{re}$ and $\boldsymbol{\Sigma}_e$ can be modeled by statistical knowledge, and an averaging operation can be performed as follows: Based on (14), the trace of the FIM can be expressed for the eavesdropper as

$$\text{tr}\{\mathbf{I}(\mathbf{y}_e; \boldsymbol{\theta})\} = \text{tr}\{\mathbf{P} \mathbf{H}_{ar}^H \boldsymbol{\Omega}^H \mathbf{E} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P}\} \quad (15)$$

where $\mathbf{E} \triangleq \mathbf{H}_{re}^H \boldsymbol{\Sigma}_e^{-1} \mathbf{H}_{re}$. Suppose that the transmitter does not know $\mathbf{E}$ perfectly but it has statistical information that $\mathbf{E}$ takes M_e possible values with known probabilities. Namely, $\mathbf{E} = \mathbf{E}^{(j)}$ with probability $\varsigma^{(j)}$ for $j = 1, \dots, M_e$. Then, the average value of the trace of the FIM can be calculated for the eavesdropper as

$$\sum_{j=1}^{M_e} \varsigma^{(j)} \text{tr}\{\mathbf{P} \mathbf{H}_{ar}^H \boldsymbol{\Omega}^H \mathbf{E}^{(j)} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P}\} \quad (16)$$

$$\mathbf{I}(\mathbf{y}_i; \underline{\boldsymbol{\theta}}) = \begin{bmatrix} (\mathbf{H}_{ri} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P})^H \boldsymbol{\Sigma}_i^{-1*} (\mathbf{H}_{ri} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P}) & \mathbf{0} \\ \mathbf{0} & (\mathbf{H}_{ri} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P})^T \boldsymbol{\Sigma}_i^{-1} (\mathbf{H}_{ri} \boldsymbol{\Omega} \mathbf{H}_{ar} \mathbf{P})^* \end{bmatrix} \quad (7)$$

$$= \text{tr}\{\mathbf{P}\mathbf{H}_{ar}^H \mathbf{\Omega}^H \mathbf{\bar{E}} \mathbf{\Omega} \mathbf{H}_{ar} \mathbf{P}\} \quad (17)$$

where $\mathbf{\bar{E}} \triangleq \sum_{j=1}^{M_e} \varsigma^{(j)} \mathbf{E}^{(j)}$. Since (17) is in the same form as (15), the analysis for the case of perfect knowledge applies for the case of imperfect statistical knowledge, as well, by considering the average value of the trace of the FIM as the estimation performance metric. $\square$

A. RIS Phase Profile Design

In this section, we assume $\mathbf{P}$ to be fixed and aim to solve (4) for deriving the optimal RIS phase profile for maximizing the average Fisher information at Bob under the secrecy constraint. Based on (14), we can reformulate (4) as

$$\max_{\mathbf{\Omega}} \quad \text{tr}\{(\mathbf{H}_{rb} \mathbf{\Omega} \mathbf{H}_{ar} \mathbf{P})^H \mathbf{\Sigma}_b^{-1} (\mathbf{H}_{rb} \mathbf{\Omega} \mathbf{H}_{ar} \mathbf{P})\} \quad (18a)$$

$$\text{s.t.} \quad \text{tr}\{(\mathbf{H}_{re} \mathbf{\Omega} \mathbf{H}_{ar} \mathbf{P})^H \mathbf{\Sigma}_e^{-1} (\mathbf{H}_{re} \mathbf{\Omega} \mathbf{H}_{ar} \mathbf{P})\} \leq \Delta \quad (18b)$$

$$|\mathbf{\Omega}|_{\ell,\ell} = 1, \quad \ell = 1, \dots, r \quad (18c)$$

To solve this problem, the following proposition is provided.

Proposition 1: Define $\boldsymbol{\omega} \in \mathbb{C}^r$ as a column vector consisting of the diagonal elements of $\mathbf{\Omega}$; that is, $\boldsymbol{\omega} = [\omega_1, \dots, \omega_r]^T$. Then, we can reformulate (18) as follows:

$$\max_{\boldsymbol{\omega}} \quad \boldsymbol{\omega}^H \mathbf{Q}_b \boldsymbol{\omega} \quad (19a)$$

$$\text{s.t.} \quad \boldsymbol{\omega}^H \mathbf{Q}_e \boldsymbol{\omega} \leq \Delta \quad (19b)$$

$$|\omega_\ell| = 1, \quad \ell = 1, \dots, r \quad (19c)$$

where $\mathbf{Q}_i \in \mathbb{C}^{r \times r}$ is a Hermitian matrix that is positive definite for each $i \in \{b, e\}$.

Proof: Considering the expressions in (18a) and (18b), we first express the elements of the matrices $\mathbf{H}_{rb}$, $\mathbf{H}_{re}$, and $\mathbf{H}_{ar} \mathbf{P}$ as follows:

$$\mathbf{H}_{ri} \triangleq \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \vdots & & \ddots & \\ a_{n_i1} & a_{n_i2} & \dots & a_{n_i r} \end{bmatrix} \quad \text{for } i \in \{b, e\} \quad (20)$$

$$\mathbf{H}_{ar} \mathbf{P} \triangleq \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1k} \\ b_{21} & b_{22} & \dots & b_{2k} \\ \vdots & & \ddots & \\ b_{r1} & b_{r2} & \dots & b_{rk} \end{bmatrix} \quad (21)$$

Accordingly, $\mathbf{H}_i$, which was defined as $\mathbf{H}_i \triangleq \mathbf{H}_{ri} \mathbf{\Omega} \mathbf{H}_{ar} \mathbf{P}$ in the proof of Lemma 1, can be obtained as

$$\mathbf{H}_i = \begin{bmatrix} \sum_{j=1}^r (a_{1j} \omega_j b_{j1}) & \sum_{j=1}^r (a_{1j} \omega_j b_{j2}) & \dots & \sum_{j=1}^r (a_{1j} \omega_j b_{jk}) \\ \sum_{j=1}^r (a_{2j} \omega_j b_{j1}) & \sum_{j=1}^r (a_{2j} \omega_j b_{j2}) & \dots & \sum_{j=1}^r (a_{2j} \omega_j b_{jk}) \\ \vdots & & \ddots & \vdots \\ \sum_{j=1}^r (a_{n_i j} \omega_j b_{j1}) & \dots & \dots & \sum_{j=1}^r (a_{n_i j} \omega_j b_{jk}) \end{bmatrix} \quad (22)$$

$$= \sum_{j=1}^r \omega_j \mathbf{S}_{i,j} \quad (23)$$

where $\mathbf{S}_{i,j}$ is defined as

$$\mathbf{S}_{i,j} \triangleq \begin{bmatrix} a_{1j} b_{j1} & a_{1j} b_{j2} & \dots & a_{1j} b_{jk} \\ a_{2j} b_{j1} & a_{2j} b_{j2} & \dots & a_{2j} b_{jk} \\ \vdots & & \ddots & \vdots \\ a_{n_i j} b_{j1} & a_{n_i j} b_{j2} & \dots & a_{n_i j} b_{jk} \end{bmatrix}. \quad (24)$$

Similarly, $\mathbf{H}_i^H$ can be written as $\mathbf{H}_i^H = \sum_{j=1}^r \omega_j^* \mathbf{S}_{i,j}^H$. Based on the preceding expressions for $\mathbf{H}_i$ and $\mathbf{H}_i^H$, (18a) and (18b) can be calculated as follows:

$$\begin{aligned} & \text{tr}\{\mathbf{H}_i^H \mathbf{\Sigma}_i^{-1} \mathbf{H}_i\} \\ &= \text{tr}\left\{\left(\sum_{j=1}^r \omega_j^* \mathbf{S}_{i,j}^H\right) \mathbf{\Sigma}_i^{-1} \left(\sum_{l=1}^r \omega_l \mathbf{S}_{i,l}\right)\right\} \\ &= \sum_{j=1}^r \sum_{l=1}^r \omega_j^* \omega_l \text{tr}\{\mathbf{S}_{i,j}^H \mathbf{\Sigma}_i^{-1} \mathbf{S}_{i,l}\}. \end{aligned} \quad (25)$$

Next, we define matrix $\mathbf{Q}_i \in \mathbb{C}^{r \times r}$ such that its entry in the j th row and the l th column is given by $[\mathbf{Q}_i]_{j,l} = \text{tr}\{\mathbf{S}_{i,j}^H \mathbf{\Sigma}_i^{-1} \mathbf{S}_{i,l}\}$. Then, it is noted that the expression in (25) can be stated as $\boldsymbol{\omega}^H \mathbf{Q}_i \boldsymbol{\omega}$ with $\boldsymbol{\omega} = [\omega_1, \omega_2, \dots, \omega_r]^T$. Therefore, (18a) and (18b) are equal to (19a) and (19b), respectively, as claimed in the proposition. In addition, the elements of $\mathbf{Q}_i$ satisfy the following relations:

$$\begin{aligned} [\mathbf{Q}_i]_{j,l}^* &= \text{tr}\{\mathbf{S}_{i,j}^H \mathbf{\Sigma}_i^{-1} \mathbf{S}_{i,l}\}^* \\ &= \text{tr}\{\mathbf{S}_{i,j}^T (\mathbf{\Sigma}_i^{-1})^* \mathbf{S}_{i,l}^*\} \\ &= \text{tr}\{(\mathbf{S}_{i,j}^T (\mathbf{\Sigma}_i^{-1})^* \mathbf{S}_{i,l}^*)^T\} \\ &= \text{tr}\{\mathbf{S}_{i,l}^H (\mathbf{\Sigma}_i^{-1})^H \mathbf{S}_{i,j}^H\} \\ &= \text{tr}\{\mathbf{S}_{i,l}^H \mathbf{\Sigma}_i^{-1} \mathbf{S}_{i,j}\} \\ &= [\mathbf{Q}_i]_{l,j}. \end{aligned} \quad (26)$$

where the third equality is based on the property that $\text{tr}\{\mathbf{A}\} = \text{tr}\{\mathbf{A}^T\}$ and the fifth equality is due to the fact that the covariance matrix of a complex random vector is a Hermitian matrix (so is its inverse). Overall, it is shown in (26) that $[\mathbf{Q}_i]_{j,l}^* = [\mathbf{Q}_i]_{l,j}$ for any l and j , implying that $\mathbf{Q}_i$ is a Hermitian matrix.

To prove the positive definiteness of $\mathbf{Q}_i$, consider a generic non-zero complex vector $\mathbf{z} \in \mathbb{C}^r$. Then, the following relations can be obtained (cf. (25)):

$$\begin{aligned} \mathbf{z}^H \mathbf{Q}_i \mathbf{z} &= \sum_{j=1}^r \sum_{l=1}^r z_j^* z_l \text{tr}\{\mathbf{S}_{i,j}^H \mathbf{\Sigma}_i^{-1} \mathbf{S}_{i,l}\} \\ &= \text{tr}\left\{\left(\sum_{j=1}^r z_j^* \mathbf{S}_{i,j}^H\right) \mathbf{\Sigma}_i^{-1} \left(\sum_{l=1}^r z_l \mathbf{S}_{i,l}\right)\right\} \\ &\triangleq \text{tr}\{\mathbf{X}_i^H \mathbf{\Sigma}_i^{-1} \mathbf{X}_i\} > 0 \end{aligned} \quad (27)$$

where $\mathbf{X}_i$ is defined as $\mathbf{X}_i \triangleq \sum_{l=1}^r z_l \mathbf{S}_{i,l}$. The last expression in (27) is positive due to the positive definiteness of Σ_i . (In particular, if $\mathbf{x}_{i,j}$ denotes the j th column of $\mathbf{X}_i$, (27) becomes $\sum_j \mathbf{x}_{i,j}^H \Sigma_i^{-1} \mathbf{x}_{i,j}$, which is always positive.) Hence, $\mathbf{Q}_i$ is a positive definite matrix for each $i \in \{b, e\}$. ■

Remark 2: Since the expressions in (19a) and (19b) correspond to the traces of the FIMs (see (14) and (18)), they should be non-negative for any ω by definition. Therefore, $\mathbf{Q}_b$ in (19a) and $\mathbf{Q}_e$ in (19b) being positive definite matrices is in compliance with this intuition. □

Remark 3: Since $\mathbf{Q}_i$ is a Hermitian matrix for each $i \in \{b, e\}$, its eigenvalues are real-valued and (19a) (similarly, (19b)) can be upper and lower bounded as follows [67]:

$$\lambda_{i,\min} \omega^H \omega \leq \omega^H \mathbf{Q}_i \omega \leq \lambda_{i,\max} \omega^H \omega \quad (28)$$

where $\lambda_{i,\min}$ and $\lambda_{i,\max}$ denote, respectively, the minimum and maximum eigenvalues of $\mathbf{Q}_i$. Since $\omega^H \omega = r$ due to the constraint in (19c), $r\lambda_{i,\min} \leq \omega^H \mathbf{Q}_i \omega \leq r\lambda_{i,\max}$ can be obtained. However, $r\lambda_{i,\min}$ and $r\lambda_{i,\max}$ may not be tight bounds for $\omega^H \mathbf{Q}_i \omega$ in (19) since the eigenvectors corresponding to the minimum and maximum eigenvalues of $\mathbf{Q}_i$ may not be multiples of the all-ones vector. □

Based on Proposition 1, the RIS phase profile design problem in (18) is stated in a more explicit form as in (19). The objective function in (19a) and the first constraint in (19b) involve quadratic functions of the optimization variables. However, due to the constraints in (19c), the RIS phase profile optimization becomes a non-convex problem, namely, non-convex quadratic constrained quadratic programming (QCQP). As in [68], this problem can be solved via the SDR approach. Since $\omega^H \mathbf{Q}_i \omega = \text{tr}\{\omega^H \mathbf{Q}_i \omega\} = \text{tr}\{\mathbf{Q}_i \omega \omega^H\}$, the problem in (19) can be reformulated as

$$\max_{\mathbf{W}} \quad \text{tr}\{\mathbf{Q}_b \mathbf{W}\} \quad (29a)$$

$$\text{s.t.} \quad \text{tr}\{\mathbf{Q}_e \mathbf{W}\} \leq \Delta \quad (29b)$$

$$[\mathbf{W}]_{ii} = 1 \quad \text{for } i = 1, \dots, r \quad (29c)$$

$$\mathbf{W} \succeq \mathbf{0}, \text{rank}(\mathbf{W}) = 1 \quad (29d)$$

where $\mathbf{W} \triangleq \omega \omega^H$. After relaxing the rank constraint, the following convex formulation is obtained:

$$\max_{\mathbf{W}} \quad \text{tr}\{\mathbf{Q}_b \mathbf{W}\} \quad (30a)$$

$$\text{s.t.} \quad \text{tr}\{\mathbf{Q}_e \mathbf{W}\} \leq \Delta \quad (30b)$$

$$[\mathbf{W}]_{ii} = 1 \quad \text{for } i = 1, \dots, r \quad (30c)$$

$$\mathbf{W} \succeq \mathbf{0} \quad (30d)$$

As stated in [68], the problem in (30) can be solved via various approaches such as the interior point methods [69], first-order methods [70, Chapter 23], and sequential quadratic programming (SQP) [71]. MATLAB toolboxes such as CVX [72], [73] and YALMIP [74] are two powerful and well-known frameworks based on interior point methods for solving this sort of problems. The solution based on the SDR approach, i.e., the solution of (30), does not necessarily satisfy the rank-one constraint in (29).

Therefore, various approaches, such as eigenvalue decomposition (ED) and Gaussian randomization (GR), are employed to derive a sub-optimal rank-one solution [75]. In the ED method, the eigenvector corresponding to the maximum eigenvalue of the solution of (30) is considered as the sub-optimal solution of (29). In the GR method, after obtaining the eigenvalue decomposition, $\mathbf{W}^* = \mathbf{U} \mathbf{\Lambda} \mathbf{U}^H$, random vectors are generated as $\tilde{\omega} = \mathbf{U} \mathbf{\Lambda}^{\frac{1}{2}} \mathbf{g}$, where $\mathbf{g} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_r)$. Then, $\hat{\omega} = e^{j\angle \tilde{\omega}}$ is considered as the sub-optimal solution of (30). The preceding sub-optimal rank-one solutions do not necessarily satisfy the secrecy constraint in (19b) or (29b). Therefore, we combine them as follows by considering the secrecy constraint: First, the sub-optimal rank-one solution is obtained via the ED method, and the corresponding secrecy constraint is checked. If the secrecy constraint is satisfied, that rank-one solution is declared as the sub-optimal solution of (19). Otherwise, rank-one sub-optimal solutions are generated based on the GR method until the secrecy constraint is satisfied, where the random nature of the GR method is utilized to get a feasible solution.

Regarding the computational complexity of the RIS phase profile optimization problem, we consider the semidefinite programming (SDP) problem in (30). According to [68], the worst-case computational complexity of solving a generic SDP using CVX is given by $\mathcal{O}(\max\{m, n\}^4 n^{1/2} \log(1/\epsilon_1))$, where m is the number of constraints, n is the size of the positive semidefinite matrix in the objective, and $\epsilon_1 > 0$ is a constant reflecting the solution accuracy of the CVX solver. Accordingly, the complexity order of (30) is stated as $\mathcal{O}(\max\{3, r\}^4 r^{1/2} \log(1/\epsilon_1))$, where r is the number of RIS elements. Given that r is typically greater than 3, the complexity order can be simplified as $\mathcal{O}(r^{4.5} \log(1/\epsilon_1))$.

Remark 4: Another approach to deal with rank-one relaxation is to use a penalty method [76], [77]. In this approach, a penalty component can be added to the objective function to obtain a feasible solution. For instance, [76] uses a factor of the difference between the nuclear norm and the spectral norm of the optimization variable (matrix) as the penalty term. Furthermore, Taylor series expansion is used to obtain a convex upper bound for the penalty term and CVX in MATLAB is employed to solve the resulting problem. Another method for obtaining a rank-one solution from SDP is sequential rank-one constraint relaxation (SROCR) [78], [79], [80]. In this method, an eigenvalue-related constraint is added to the main problem and the problem is iteratively solved until the convergence criteria hold. In some setups where the Gaussian randomization technique has difficulty in obtaining a rank-one solution in a limited amount of time, the penalty or SROCR approaches can be helpful in deriving a feasible solution. Although the solutions obtained by the penalty and SROCR methods may be close to optimal solutions in most cases, their computational complexity is high due to the iterative solution of the problem by CVX, especially for large RIS phase profile matrices; hence, we choose to employ the ED and GR approaches in this study. □

As stated in Remark 3, there exists a certain lower bound for $\omega^H \mathbf{Q}_e \omega$. Hence, if the secrecy limit Δ is lower than that bound, (19) becomes infeasible. For example, (19) is infeasible

if $\Delta < r\lambda_{e,\min}$, where $\lambda_{e,\min}$ denotes the minimum eigenvalue of $\mathbf{Q}_e$. However, as stated in Remark 3, $r\lambda_{e,\min}$ is not a tight bound in general. To specify the feasibility region for (19) more accurately, the following problem can be defined:

$$\min_{\{\omega_i\}_{i=1}^r} \omega^H \mathbf{Q}_e \omega \quad (31a)$$

$$\text{s.t. } |\omega_i| = 1 \quad \text{for } i = 1, 2, \dots, r \quad (31b)$$

Similar to (19), this problem can also be solved via the SDR approach to derive a sub-optimal solution. If the minimum value of (31a) corresponding to the sub-optimal solution is denoted by $\Delta_{\min}$, the problem in (19) becomes feasible for all $\Delta \geq \Delta_{\min}$.

B. Optimal Power Allocation

In this section, we assume $\mathbf{\Omega}$ to be fixed and aim to solve (5) for deriving the optimal power allocation matrix. Based on (14), we can rewrite (5) as

$$\max_{\mathbf{P}} \text{tr}\{\mathbf{P}^H \mathbf{A}_b \mathbf{P}\} \quad (32a)$$

$$\text{s.t. } \text{tr}\{\mathbf{P}^H \mathbf{A}_e \mathbf{P}\} \leq \Delta \quad (32b)$$

$$\text{tr}\{\mathbf{P} \mathbf{P}^T\} \leq P_{\Sigma} \quad (32c)$$

$$\mathbf{P} \mathbf{P}^T \succeq \mathbf{0}. \quad (32d)$$

where $\mathbf{A}_i$ is defined as $\mathbf{A}_i \triangleq (\mathbf{H}_{ri} \mathbf{\Omega} \mathbf{H}_{ar})^H \mathbf{\Sigma}_i^{-1} (\mathbf{H}_{ri} \mathbf{\Omega} \mathbf{H}_{ar})$ for $i \in \{b, e\}$. Since $\mathbf{P}$ is a real diagonal matrix represented by $\mathbf{P} = \text{diag}\{\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_k}\}$, (32) is equivalent to

$$\max_{\{p_i\}_{i=1}^k} \sum_{i=1}^k \alpha_i p_i \quad (33a)$$

$$\text{s.t. } \sum_{i=1}^k \beta_i p_i \leq \Delta \quad (33b)$$

$$\sum_{i=1}^k p_i \leq P_{\Sigma} \quad (33c)$$

$$p_i \geq 0 \quad \text{for } i = 1, 2, \dots, k \quad (33d)$$

where $\alpha_i \triangleq [\mathbf{A}_b]_{ii}$ and $\beta_i \triangleq [\mathbf{A}_e]_{ii}$. The problem in (33) corresponds to a standard linear programming (LP) formulation, which can be solved via conventional algorithms for LP [81]. (The linear programming solver in MATLAB [82], 'linprog', is used in this study for solving (33).)

According to [83], the computational complexity order of solving the problem in (33) (i.e., subproblem 2) using the simplex method is $\mathcal{O}(2^k)$ where k is the number of variables (parameters).

Remark 5: As an extension of the discussion in Remark 1, the cases with statistical knowledge about the channel coefficients and/or the noise covariance matrices can also be treated in the subproblems given by (30) and (32). By assuming statistical knowledge about the $\mathbf{Q}_i$ and $\mathbf{A}_b$ matrices in (30) and (32), respectively, with $i \in \{b, e\}$, the average values of the traces of the FIMs can be obtained by replacing $\mathbf{Q}_i$ and $\mathbf{A}_b$ with their expected values; i.e., $\bar{\mathbf{Q}}_i = \mathbb{E}\{\mathbf{Q}_i\}$ and $\bar{\mathbf{A}}_i = \mathbb{E}\{\mathbf{A}_i\}$,

respectively. Hence, the problem structures remain the same by considering the expected value of the trace of the FIM as the performance metric. $\square$

C. Joint Optimization of RIS Phase Profile and Power Allocation

This section presents the proposed alternating optimization approach for solving the joint RIS phase profile design and power allocation problem in (3). Namely, a solution to (3) is obtained by iteratively solving the RIS phase design problem in (29) and the power allocation problem in (33). The details are shown in Algorithm 1. In this algorithm, the RIS phase profile is initially set to a random phase profile, where the elements have uniformly distributed i.i.d. random phases between 0 and 2π . Then, the power allocation matrix is optimized based on (33) considering the RIS phase profile to be fixed, and then the RIS phase profile is updated by solving (30) for the power allocation matrix obtained in the previous step and by applying rank reduction to obtain a rank-one solution. These iterations continue until the objective function does not change significantly, which is determined by parameter ϵ in Algorithm 1, or until the number n of iterations reaches the maximum number of iterations, $n_{\max}$. (The values of the RIS phase profile and the power allocation matrix at iteration n are denoted by $\omega^{(n)}$ and $\mathbf{P}^{(n)}$, respectively, and $\mathbf{W}^{(n)}$ denotes the solution of (30) in the n th iteration.) At the end of the iterations, the final values of the RIS phase profile and the power allocation matrix are considered as a solution of (3), which are denoted by $\mathbf{\Omega}^*$ and $\mathbf{P}^*$ in Algorithm 1.

In Algorithm 1, the rank reduction approach discussed in Section III-A is utilized to obtain a rank-one solution for the RIS phase profile based on the solution of (30), which is shown in Algorithm 2. Since a complex Gaussian random variable is utilized to obtain a solution in the GR part of Algorithm 2, it is possible for the average Fisher information at Bob and Eve to have some fluctuation between certain values. The resulting objective values are saved in a vector named $\mathbf{f}_b$ at each iteration of Algorithm 1, and when the iteration number reaches $n_{\max}$, the value of ω calculated in the iteration that achieves the maximum value of $\mathbf{f}_b$ is chosen as the optimal solution.

In addition, in Algorithm 2, which is used as an inner layer of Algorithm 1, the main steps that dominate the complexity are steps 6 and 11, which are the ED and GR, respectively. The computational complexity of the ED is given as $\mathcal{O}(n^3)$ for a square matrix with size $(n \times n)$ [84]. In our proposed algorithm for rank reduction, the ED is applied once, and the GR uses the eigenvectors found in the ED step. Since GR generates random rank-one solutions iteratively until finding the feasible solution, the order of complexity is given by $\mathcal{O}(r^3 + L\epsilon_2)$, where L is the maximum iteration number of Algorithm 2 and ϵ_2 is a constant representing the calculation duration of the GR loop. Therefore, the complexity order of Algorithm 2 is calculated as $\mathcal{O}(r^3 + L\epsilon_2)$.

During the alternating optimization iterations in Algorithm 1, when optimizing the RIS phase profile for a fixed power allocation matrix, the existence of a feasible solution is not guaranteed (please see the explanations at the end of Section III-A).

Algorithm 1: Joint Optimization of Ω and $\mathbf{P}$ for Solving (3).

```

1: Define: convergence tolerance  $\epsilon$ , the maximum number
   of iterations  $n_{\max}$ , iteration index  $n$ ,  $1 \times n_{\max}$  vector  $\mathbf{f}_b$ 
   for saving the average Fisher information at Bob in each
   iteration
2: Initialization:
3:  $n = 1$ 
4:  $\phi_i \leftarrow \mathcal{U}[0, 2\pi]$  i.i.d uniform r.v.'s for  $i = 1, 2, \dots, r$ 
5:  $\omega^{(0)} = [e^{j2\pi\phi_1}, e^{j2\pi\phi_2}, \dots, e^{j2\pi\phi_r}]^T$ 
6: First iteration:
7:  $\mathbf{P}^{(1)} \leftarrow$  solution of (33) for fixed  $\omega^{(0)}$ 
8:  $\mathbf{W}^{(1)} \leftarrow$  solution of (30) for fixed  $\mathbf{P}^{(1)}$ 
9:  $\omega^{(1)} \leftarrow$  rank-one solution obtained from  $\mathbf{W}^{(1)}$  via
   Algorithm 2
10:  $\mathbf{f}_b(1) \leftarrow$  value of (19a) for  $\omega^{(1)}$  and  $\mathbf{P}^{(1)}$ 
11: repeat
12:    $\mathbf{P}^{(n+1)} \leftarrow$  solution of (33) for fixed  $\omega^{(n)}$ ;
13:    $\mathbf{W}^{(n+1)} \leftarrow$  solution of (30) for fixed  $\mathbf{P}^{(n+1)}$ 
14:   run Algorithm 2 based on  $\mathbf{W}^{(n+1)}$ 
15:   if Algorithm 2 returns a feasible solution then
16:      $\omega^{(n+1)} \leftarrow$  rank-one solution obtained from
       Algorithm 2
17:   else
18:      $\omega^{(n+1)} \leftarrow \omega^{(n)}$ 
19:   end if
20:    $\mathbf{f}_b(n+1) \leftarrow$  value of (19a) for  $\omega^{(n+1)}$  and  $\mathbf{P}^{(n+1)}$ 
21:    $n = n + 1$ 
22: until  $\mathbf{f}_b(n) - \mathbf{f}_b(n-1) \leq \epsilon$  or  $n = n_{\max}$ 
23: if  $n = n_{\max}$  then
24:    $n^* = \max_n \mathbf{f}_b(n)$ 
25:    $\Omega^* = \text{diag}\{\omega^{(n^*)}\}$ 
26:    $\mathbf{P}^* = \mathbf{P}^{(n^*)}$ 
27: else
28:    $\Omega^* = \text{diag}\{\omega^{(n)}\}$ 
29:    $\mathbf{P}^* = \mathbf{P}^{(n)}$ 
30: end if

```

However, the optimal power allocation problem for a given RIS phase profile is always feasible (please see (33)). In Algorithm 1, the feasibility issue is addressed by utilizing the power allocation algorithm and the solutions obtained in the previous iterations. Specifically, when the GR technique in Algorithm 2 reaches the maximum iteration number L , due to the infeasibility of the RIS phase profile optimization problem, the solution of the previous iteration in Algorithm 1 is used to derive the rank-one solution for the RIS phase profile.

Combining the complexity orders of the different steps mentioned in the previous parts, it is concluded that the worst-case complexity of the overall proposed algorithm is $\mathcal{O}(n_{\max}(r^{4.5} \log(1/\epsilon_1) + r^3 + L\epsilon_2 + 2^k))$, where $n_{\max}$ is the maximum number of iterations in Algorithm 1.

Remark 6: While the proposed alternating optimization (AO) approach may not guarantee optimality in all scenarios, its

Algorithm 2: Rank Reduction via ED and GR.

```

1: Define: randomization index  $l$ , maximum number of
   randomization operations  $L > 1$ 
2: Given: Solution of (30) denoted by  $\mathbf{W}^*$ 
3: Initialization:  $l = 1$ 
4: ED:  $\{\mathbf{W}^* = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^H\}$ 
5:  $\mathbf{\Lambda} = \text{diag}\{\lambda_1, \lambda_2, \dots, \lambda_r\}$ , where  $\lambda_i$  is the  $i^{th}$ 
   eigenvalue of  $\mathbf{W}^*$ 
6: Find the maximum eigenvalue  $\lambda_{\max}$  of  $\mathbf{W}^*$  and the
   corresponding eigenvector  $\mathbf{v}_{\max}$ 
7:  $\omega \leftarrow \mathbf{v}_{\max}$ 
8: if (19b) holds for  $\omega$  then
9:    $\omega^* \leftarrow \omega$ 
10: else
11:   GR:
12:   repeat
13:      $\mathbf{g} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_r)$ 
14:      $\omega \leftarrow \mathbf{U}\mathbf{\Lambda}^{\frac{1}{2}}\mathbf{g}$ 
15:      $l = l + 1$ 
16:   until (19b) holds or  $l = L$ 
17:   if  $l < L$  then
18:      $\omega^* \leftarrow \omega$ 
19:   else
20:     no feasible solution is available
21:   end if
22: end if

```

efficacy in providing near-optimal solutions to the original joint optimization problem can be evaluated from multiple perspectives. First, the optimality of the solutions for the subproblems within AO can be considered. Subproblem 2 given by (33) is solved via linear programming, which ensures an optimal solution. On the other hand, subproblem 1, stated as (29), is solved via SDR as in Algorithm 2, which may result in a suboptimal solution. Nevertheless, SDR solutions serve as theoretical upper bounds for the suboptimal RIS phase profile [85], [86], [87], [88], [89]. Moreover, the iterative refinement process within AO plays a pivotal role in approaching optimality. The optimality of the SDR based solution (Algorithm 2) and the convergence of the AO algorithm depend on the severity of the secrecy constraint, which can vary with Δ and P_{Σ} . Specifically, when the secrecy constraint is inactive or very strict, Algorithm 2 yields a very close solution to the relaxed problem in (30), which presents an upper bound, and the proposed AO approach converges after multiple iterations. However, in cases with critical severity of the secrecy constraint, the difference from the upper bound can be larger and the AO algorithm may not converge to a particular solution within the iteration limit, potentially resulting in selection of suboptimal solutions. However, even in such scenarios, the proposed AO approach can provide significant improvements compared to performing power allocation only or RIS phase optimization only, as investigated in Section IV. $\square$

IV. NUMERICAL RESULTS

In this section, we investigate the theoretical results and the proposed approach based on various numerical examples. As adopted in [48], the real and imaginary parts of the channel matrices $\mathbf{H}_{ar}$, $\mathbf{H}_{rb}$, and $\mathbf{H}_{re}$ in (1) and (2) are generated as i.i.d. uniform random variables ranging over $[-0.1, 0.1]$ by utilizing a single realization in MATLAB with seed 1. Also, the additive noise vectors in Bob and Eve (η_b in (1) and η_e in (2), respectively) are modeled as independent zero-mean circularly-symmetric Gaussian random vectors with i.i.d. components, where the variance of each component is set to 10^{-5} . In addition, the observation sizes at Bob and Eve are considered to be $n_b = n_e = 2k$, where k denotes the number of parameters [48]. Moreover, the size of the RIS is taken as $r = 36$ (6×6) or $r = 64$ (8×8) in the simulations. Finally, the convergence metric in Algorithm 1 is set to $\epsilon = 10^{-1}$.

For each case, we compare our proposed approach of alternating optimization (AO) with two benchmarks referred to as “RIS only”, “power allocation (PA) only”. In the RIS only algorithm, we set the power allocation matrix $\mathbf{P}$ to be an equal-power allocation matrix, namely, $\mathbf{P} = \text{diag}\{\sqrt{P_\Sigma/k}, \sqrt{P_\Sigma/k}, \dots, \sqrt{P_\Sigma/k}\}$. The aim of this case is to investigate the effects of optimizing the RIS phase profile with the unit modulus constraint for secure estimation of an unknown deterministic complex parameter vector by solving (4). In the PA only algorithm, a fixed RIS phase profile $\mathbf{\Omega} = \text{diag}\{e^{j\phi_1}, e^{j\phi_2}, \dots, e^{j\phi_r}\}$ is considered to be generated randomly with ϕ_i 's being i.i.d. uniform random variables over $[0, 2\pi)$. The aim of this case is to analyze the effects of secure power allocation with the total power constraint, similar to [48] but for a different optimization metric of average Fisher information, by solving (5). We compare these benchmarks with the joint optimization of the RIS phase profile and power allocation via the proposed AO approach.

First, the trace of the FIM is evaluated at Bob and Eve versus the secrecy parameter Δ for $k \in \{10, 15\}$, $r \in \{36, 64\}$, and $P_\Sigma = 30$ in Fig. 2. It can be observed that by increasing the number of elements at the RIS (i.e., the r value), the information at Bob increases under the secrecy constraint at Eve (please see Fig. 6 for more details.) On the other hand, we cannot make a general conclusion about the effect of k , as it directly depends on the conditions of the channels while using different k values (to be investigated later in Fig. 5). Also, it is noted that received signals at Bob are more informative than those at Eve when the secrecy constraint is satisfied. For lower values of Δ , the secrecy constraint is active and the trace of the FIM is equal to the value of Δ at Eve and higher at Bob. This result would extend similarly for lower values of Δ . As Δ increases, the secrecy constraint gets less restrictive and holds with inequality, which leads to certain fixed values for all of the cases depending on the system parameters. As mentioned in Section II, information leakage in this framework is represented by the average Fisher information at Eve. When Δ increases, the secrecy limit on the average Fisher information at Eve gets higher, which provides more flexibility to increase the average Fisher information at Bob. Therefore, it can be the case that the RIS design and power allocation can be

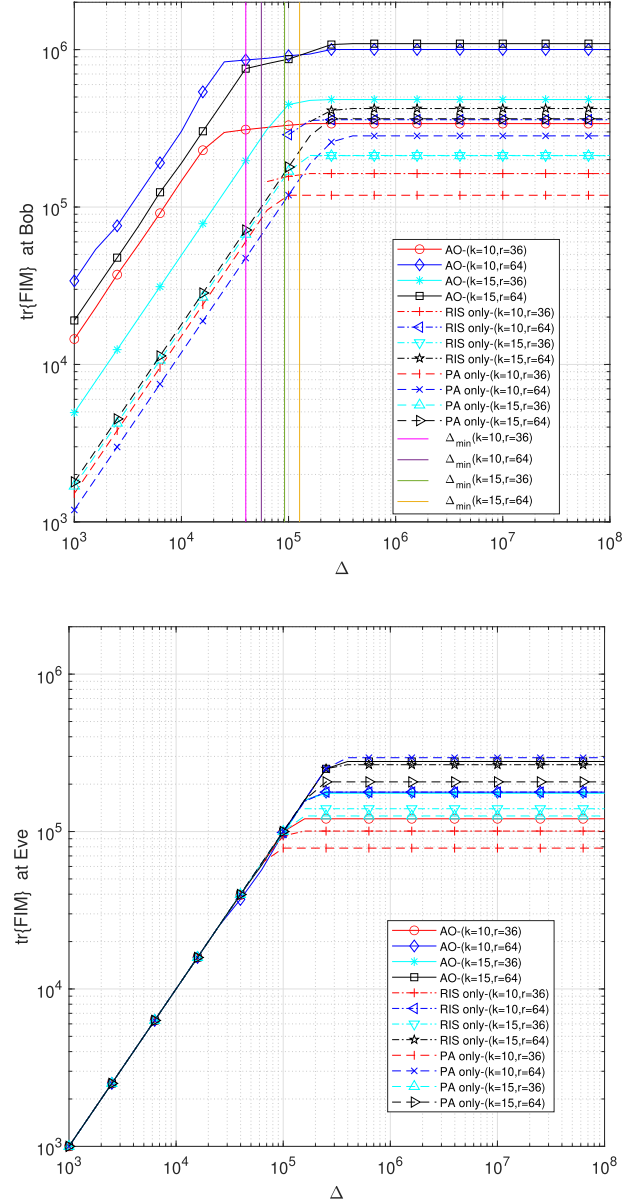


Fig. 2. Trace of FIM achieved by the AO, RIS only, and PA only algorithms versus Δ for various values of k and r , where $P_\Sigma = 30$. Also, the feasibility analysis is included with vertical lines for each k and r pair.

performed to increase the average Fisher information at Bob by causing an increase in that at Eve. Such a situation means that Eve can estimate the parameter more accurately; however, this is still limited by Δ , which should be chosen to guarantee that Eve cannot estimate the parameter above a permitted level of accuracy.

Meanwhile, the proposed AO algorithm has better performance than the benchmark algorithms, RIS only and PA only. For instance, in the case of $k = 10$ and $r = 64$, the information at Bob is approximately five times of that at Eve for the AO algorithm, whereas the information ratio between Bob and Eve achieved by the RIS only and PA only algorithms are approximately two and one, respectively. In addition, the RIS only algorithm has improved performance compared to PA only,

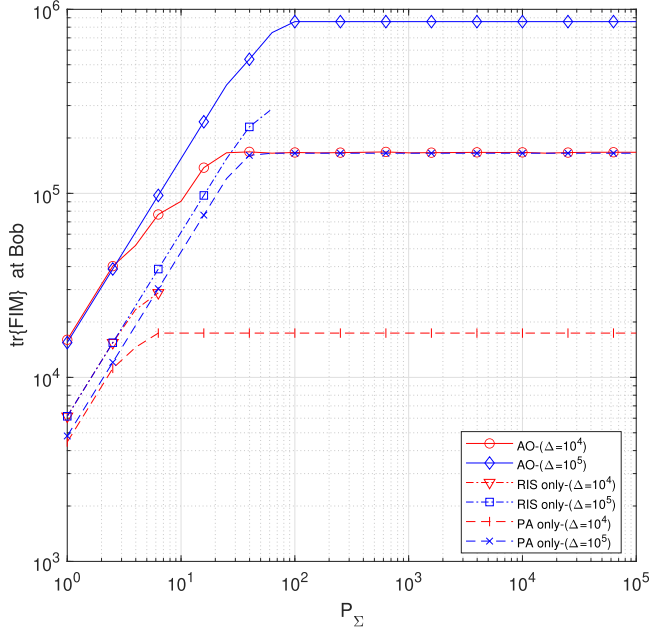


Fig. 3. Trace of FIM achieved by AO, RIS only, and PA only algorithms versus P_Σ for various values of Δ where $k = 10$ and $r = 36$.

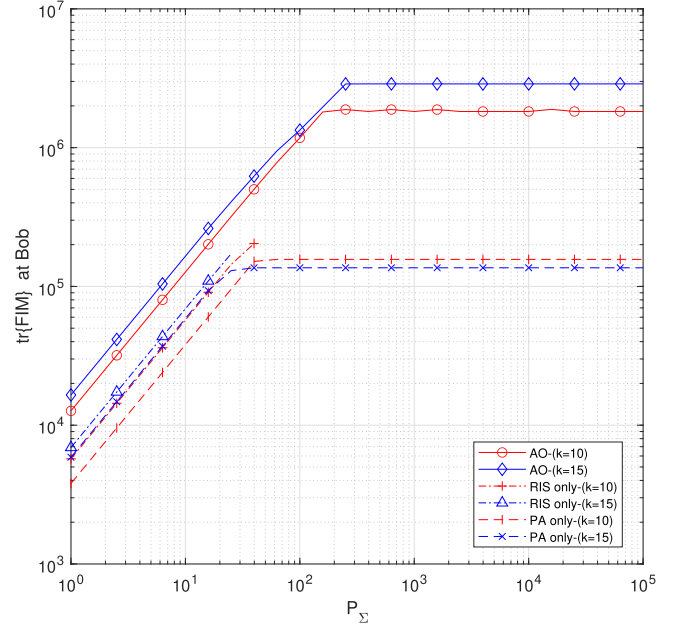


Fig. 4. Trace of FIM achieved by AO, RIS only, and PA only algorithms versus P_Σ for various values of k , where $\Delta = 10^5$ and $r = 36$.

which is intuitive since it has more degrees of freedom. However, this claim does not necessarily hold at Eve since the values at Eve are either equal to the secrecy constraint, Δ , or depend on the structure of the system (the maximum value of A_b , P_Σ , and k are the parameters that determine the trace of the FIM in this scenario). Moreover, as mentioned in (31), a feasibility region analysis takes place for the RIS only approach. In this scenario, $\Delta_{\min}$'s are derived for all the setups that are illustrated with the vertical lines in Fig. 2. It is observed that the RIS only algorithm yields solutions when Δ is higher than these specified values.

In Figs. 3 and 4, the traces of the FIMs at Bob and Eve are plotted versus the total power constraint, P_Σ , and the effects

of varying Δ and k are analyzed for a fixed value of the RIS size. From Fig. 3, where $k = 10$, $r = 36$, and $\Delta \in \{10^4, 10^5\}$, it can be realized that as P_Σ increases starting from low values, the average Fisher information at Bob and Eve increases up to certain levels. While the secrecy constraint is inactive for low values of P_Σ , it gets active when P_Σ increases up to certain values. In that case, the trace of the FIM at Eve becomes equal to Δ . Also, it is noted that the RIS-only scheme becomes infeasible for high values of P_Σ . Since RIS phase profile optimization is performed for the equal-power allocation matrix in the RIS-only scheme, the problem becomes infeasible for high values of P_Σ due to the violation of the secrecy constraint. In other words, for

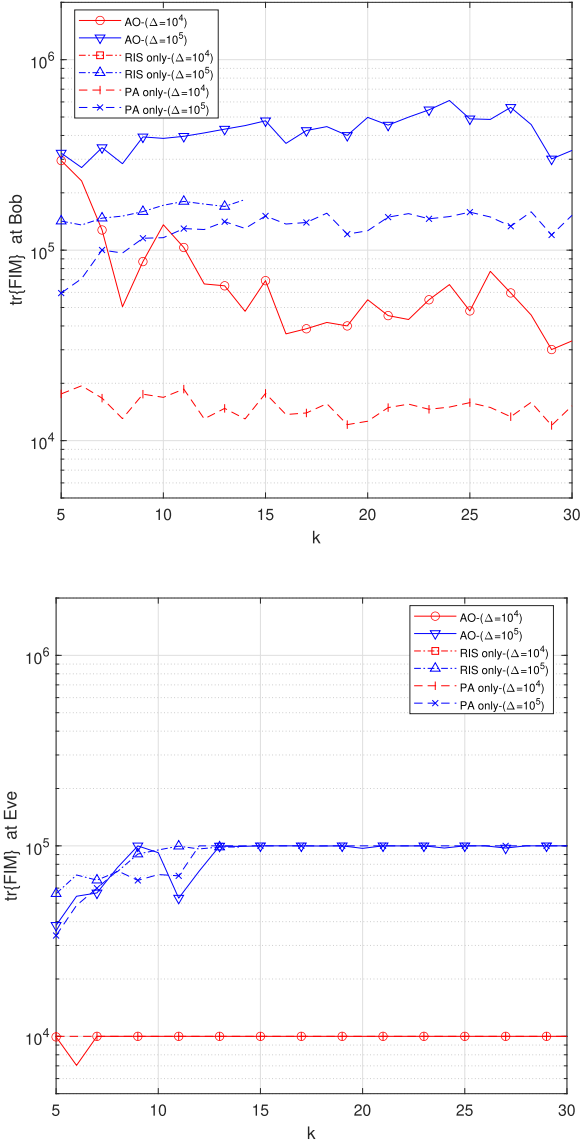


Fig. 5. Trace of FIM achieved by AO, RIS only, and PA only algorithms versus k for various values of Δ , where $P_{\Sigma} = 30$ and $r = 36$.

the given system parameters r , k , and P_{Σ} , there may not exist a feasible solution within the bounds outlined in (28) that could satisfy the secrecy constraint. Therefore, the RIS-only algorithm can provide feasible solutions only up to a certain level of P_{Σ} depending on the system parameters. For both values of Δ in Fig. 3, the AO algorithm achieves higher average Fisher information at Bob than both of the benchmarks while satisfying the secrecy constraint for Eve. Also, Bob receives more informative signals than Eve, as observed in the previous scenario. From Fig. 4, where $k \in \{10, 15\}$, $r = 36$, and $\Delta = 10^5$, it is observed that by increasing the parameter size at Alice (from $k = 10$ to $k = 15$), and accordingly the observation sizes at Bob and Eve (since $n_b = n_e = 2k$), higher Fisher information can be achieved at Bob. In addition, similar to Fig. 2, the AO approach outperforms the benchmark algorithms, and the RIS only algorithm is more effective than the PA only algorithm in its feasible regions.

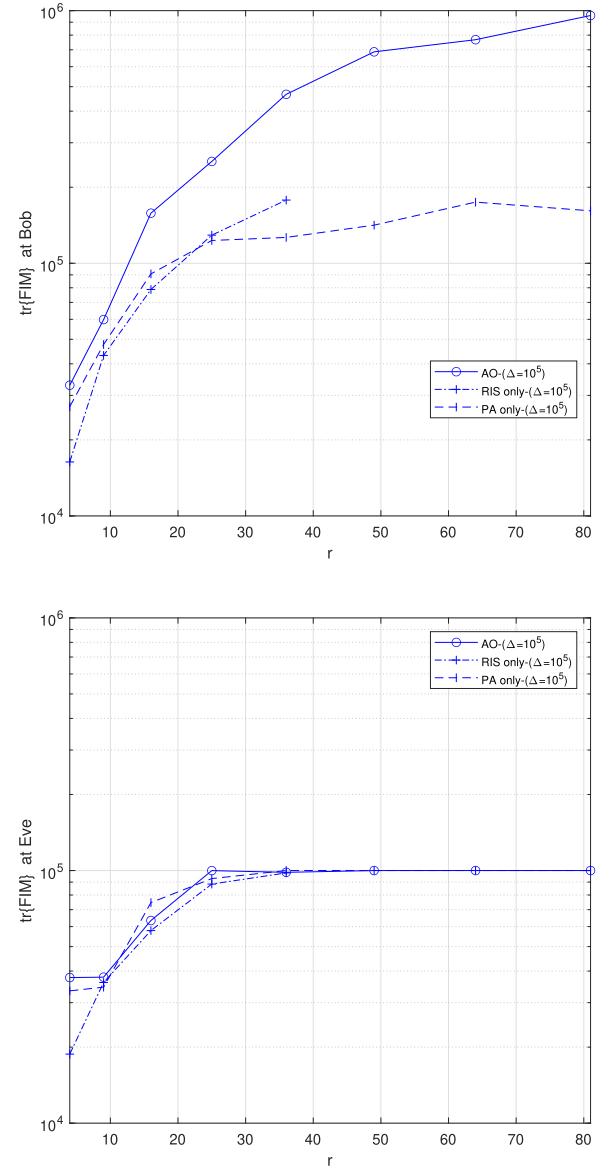


Fig. 6. Trace of FIM achieved by AO, RIS only, and PA only algorithms versus r , where $P_{\Sigma} = 30$, $\Delta = 10^5$, and $k = 15$.

Next, the traces of the FIMs at Bob and Eve achieved by the three aforementioned approaches are plotted versus the number of parameters, k , in Fig. 5, considering various values of Δ with $P_{\Sigma} = 30$ and $r = 36$. It is observed that as the value of the secrecy threshold, Δ , increases, the received signal at Bob becomes more informative as the secrecy constraint gets less restrictive. Moreover, the average Fisher information at Bob is higher than that at Eve for every value of k while maintaining compliance with the secrecy constraints. Also, at Eve, the effectiveness of the secrecy constraint is observed at all points in the figure, except for $k \in \{1, 2, \dots, 13\}$ with $\Delta = 10^5$. Furthermore, due to the random generation of channel matrices and the direct dependence of matrices $\mathbf{Q}_b$, $\mathbf{Q}_e$, $\mathbf{A}_b$, and $\mathbf{A}_e$ on them, increasing the size of the parameter does not necessarily lead to an increase in the information at Bob for a given value of the total power constraint, as observed from Fig. 5.

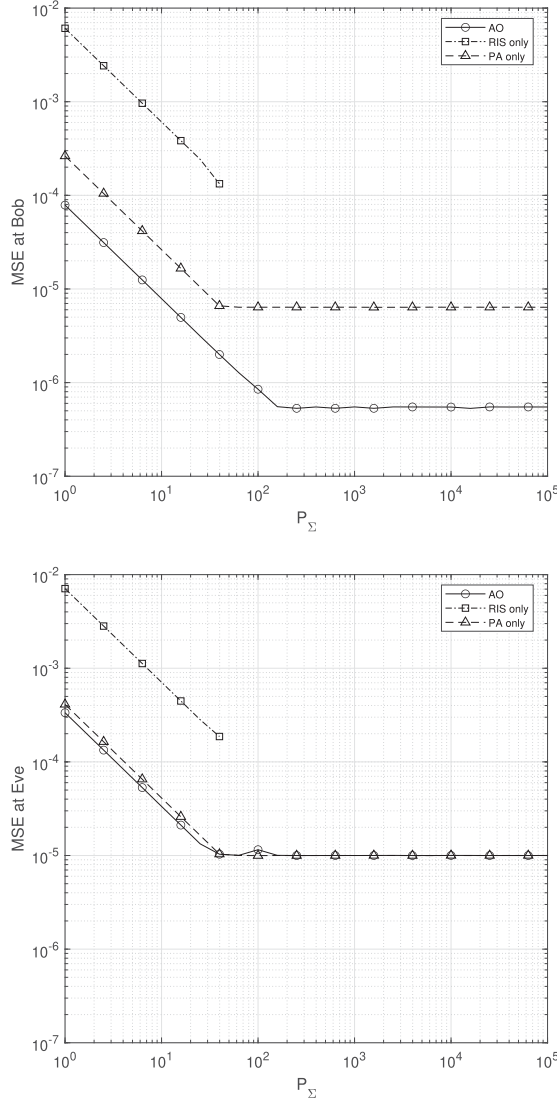


Fig. 7. MSEs of ML estimators corresponding to the AO, RIS only, and PA only algorithms versus P_Σ , where $r = 36$, $\Delta = 10^5$, and $k = 10$.

Fig. 6 presents the trace of the FIM with respect to the number of RIS elements, r , for comparing the AO approach with the benchmarks, where $\Delta = 10^5$, $k = 15$, and $P_\Sigma = 30$. The observed trends show that an increase in the value of r leads to a corresponding increase in the amount of information at Bob, and the proposed AO algorithm improves the performance at Bob significantly compared to the RIS only and PA only approaches. Additionally, the RIS only approach has feasibility only for values of r below 36. Notably, due to the presence of Eve, for the values of r higher than 36, the performance is affected by the secrecy constraint for preventing Eve from obtaining information exceeding the constraint Δ .

Finally, in order to observe the usefulness of the proposed AO algorithm for practical estimators, the MSEs of the ML estimators (MLEs) are plotted in Fig. 7 with respect to P_Σ for the AO, RIS only and PA only algorithms, where $r = 36$, $k = 10$, and $\Delta = 10^5$. In particular, the solution of the AO algorithm, as obtained from Algorithm 1, is used to set the RIS phase profile

and power allocation matrices, and the resulting MSE of the ML estimator is plotted in the figure for the AO algorithm. Similarly, the RIS only and PA only solutions are obtained according to the trace of the FIM metric proposed in this study and the resulting matrices are employed when implementing the ML estimators. In calculating the MSE, 1000 Monte-Carlo trials are performed for each setting, and the average MSE is calculated by dividing the total MSE by the number of parameters sent by Alice. (It is important to mention that in the AO and the PA only algorithms, powers of some parameters may be set to zero, meaning that they are not sent from Alice; hence, such parameters are not included in the average MSE calculation.) It is noted from Fig. 7 that the proposed AO algorithm is also useful for the practical ML estimator as it leads to lower MSEs at Bob.

V. EXTENSIONS TO OTHER SCENARIOS

A. Presence of Dominant LoS Components

Since RISs can provide significant benefits in the absence of LoS, a system model with LoS blockage is considered in the previous sections, as shown in Fig. 1. In order to investigate the effects of RIS in the presence of LoS components, in this section we assume the presence of dominant LoS paths for both Bob and Eve. Accordingly, the received signals can be written, by adapting (1) and (2) to this scenario, as follows:

$$\mathbf{y}_b = (\mathbf{H}_{rb}\mathbf{\Omega}\mathbf{H}_{ar} + \mathbf{H}_{ab})\mathbf{P}\boldsymbol{\theta} + \boldsymbol{\eta}_b \quad (34)$$

$$\mathbf{y}_e = (\mathbf{H}_{re}\mathbf{\Omega}\mathbf{H}_{ar} + \mathbf{H}_{ae})\mathbf{P}\boldsymbol{\theta} + \boldsymbol{\eta}_e \quad (35)$$

where $\mathbf{H}_{ab} \in \mathbb{C}^{n_b \times k}$ and $\mathbf{H}_{ae} \in \mathbb{C}^{n_e \times k}$ represent the channel coefficient matrices for the Alice-Bob and Alice-Eve channels, respectively, and the other parameters are as defined in Section II.

By following the same ideas as in Lemma 1 and the equations in (11)–(14), the average Fisher information related to the measurements in (34) and (35) can be obtained, for $i \in \{b, e\}$, as follows:

$$\text{tr}\{\mathbf{I}(\mathbf{y}_i; \boldsymbol{\theta})\} = \text{tr}\{((\mathbf{H}_{ri}\mathbf{\Omega}\mathbf{H}_{ar} + \mathbf{H}_{ai})\mathbf{P})^H \quad (36a)$$

$$\boldsymbol{\Sigma}_i^{-1}((\mathbf{H}_{ri}\mathbf{\Omega}\mathbf{H}_{ar} + \mathbf{H}_{ai})\mathbf{P})\}$$

$$= \text{tr}\{(\mathbf{H}_{ri}\mathbf{\Omega}\mathbf{H}_{ar}\mathbf{P})^H \boldsymbol{\Sigma}_i^{-1}(\mathbf{H}_{ri}\mathbf{\Omega}\mathbf{H}_{ar}\mathbf{P})\} \quad (36b)$$

$$+ \text{tr}\{\mathbf{P}\mathbf{H}_{ai}^H \boldsymbol{\Sigma}_i^{-1} \mathbf{H}_{ai} \mathbf{P}\} \quad (36c)$$

$$+ \text{tr}\{\mathbf{P}\mathbf{H}_{ai}^H \boldsymbol{\Sigma}_i^{-1} \mathbf{H}_{ri} \mathbf{\Omega} \mathbf{H}_{ar} \mathbf{P}\} \quad (36d)$$

$$+ \text{tr}\{\mathbf{P}(\mathbf{H}_{ri}\mathbf{\Omega}\mathbf{H}_{ar})^H \boldsymbol{\Sigma}_i^{-1} \mathbf{H}_{ai} \mathbf{P}\} \quad (36e)$$

It is noted that the first term in (36b) is equal to (14). In addition, since (36c) is not a function of $\mathbf{\Omega}$, it can be omitted for the RIS phase design problem. Meanwhile, the terms in (36d) and (36e) can be reformulated as in the following lemma.

Lemma 2: (36d) and (36e) can be expressed as

$$\text{tr}\{\mathbf{P}\mathbf{H}_{ai}^H \boldsymbol{\Sigma}_i^{-1} \mathbf{H}_{ri} \mathbf{\Omega} \mathbf{H}_{ar} \mathbf{P}\} = \boldsymbol{\omega}^T \tilde{\mathbf{q}}_i \quad (37a)$$

$$\text{tr}\{\mathbf{P}(\mathbf{H}_{ri}\mathbf{\Omega}\mathbf{H}_{ar})^H \boldsymbol{\Sigma}_i^{-1} \mathbf{H}_{ai} \mathbf{P}\} = \boldsymbol{\omega}^H \tilde{\mathbf{q}}_i^* \quad (37b)$$

with $\tilde{\mathbf{q}}_i \triangleq [\text{tr}\{\tilde{\mathbf{S}}_{i,1}\}, \dots, \text{tr}\{\tilde{\mathbf{S}}_{i,r}\}]^T$, where $\tilde{\mathbf{S}}_{i,j} \triangleq \mathbf{P}\mathbf{H}_{ai}^H \Sigma_i^{-1} \mathbf{S}_{i,j}$ and $\mathbf{S}_{i,j}$ is as defined in (24) (please see the proof of Proposition 1).

Proof: Similar to the proof of Proposition 1, define $\mathbf{H}_i \triangleq \mathbf{H}_{ri} \Omega \mathbf{H}_{ar} \mathbf{P}$, which is given by $\mathbf{H}_i = \sum_{j=1}^r \omega_j \mathbf{S}_{i,j}$ as stated in (23) with $\mathbf{S}_{i,j}$ being defined as in (24). Then, if we define $\tilde{\mathbf{S}}_{i,j} \triangleq \mathbf{P}\mathbf{H}_{ai}^H \Sigma_i^{-1} \mathbf{S}_{i,j}$, we can rewrite (36d) and (36e) as follows:

$$\text{tr}\{\mathbf{P}\mathbf{H}_{ai}^H \Sigma_i^{-1} \mathbf{H}_{ri} \Omega \mathbf{H}_{ar} \mathbf{P}\} = \sum_{j=1}^r \omega_j \text{tr}\{\tilde{\mathbf{S}}_{i,j}\} \quad (38a)$$

$$\triangleq \omega^T \tilde{\mathbf{q}}_i \quad (38b)$$

$$\text{tr}\{\mathbf{P}(\mathbf{H}_{ri} \Omega \mathbf{H}_{ar})^H \Sigma_i^{-1} \mathbf{H}_{ai} \mathbf{P}\} = \sum_{j=1}^r \omega_j^* \text{tr}\{\tilde{\mathbf{S}}_{i,j}^H\} \quad (38c)$$

$$\triangleq \omega^H \tilde{\mathbf{q}}_i^* \quad (38d)$$

where $\tilde{\mathbf{q}}_i \triangleq [\text{tr}\{\tilde{\mathbf{S}}_{i,1}\}, \dots, \text{tr}\{\tilde{\mathbf{S}}_{i,r}\}]^T$. Hence, the proof is completed. ■

Based on the results in Lemma 2 and the expression in (36), the RIS phase design problem in (4) can be redefined in this scenario as follows:

$$\max_{\omega} \quad \omega^H \mathbf{Q}_b \omega + \omega^T \tilde{\mathbf{q}}_b + \omega^H \tilde{\mathbf{q}}_b^* \quad (39a)$$

$$\text{s.t.} \quad \omega^H \mathbf{Q}_e \omega + \omega^T \tilde{\mathbf{q}}_e + \omega^H \tilde{\mathbf{q}}_e^* \leq \Delta \quad (39b)$$

$$|\omega_i| = 1 \quad \text{for } i = 1, 2, \dots, r \quad (39c)$$

This inhomogeneous QCQP problem can be homogenized by adopting the approach used in [68] as follows:

$$\max_{\omega, t} \quad \begin{bmatrix} \omega^H & t \end{bmatrix} \begin{bmatrix} \mathbf{Q}_b & \tilde{\mathbf{q}}_b \\ \tilde{\mathbf{q}}_b^T & 0 \end{bmatrix} \begin{bmatrix} \omega \\ t \end{bmatrix} \quad (40a)$$

$$\text{s.t.} \quad \begin{bmatrix} \omega^H & t \end{bmatrix} \begin{bmatrix} \mathbf{Q}_e & \tilde{\mathbf{q}}_e \\ \tilde{\mathbf{q}}_e^T & 0 \end{bmatrix} \begin{bmatrix} \omega \\ t \end{bmatrix} \leq \Delta$$

$$t^2 = 1$$

$$|\omega_i| = 1 \quad \text{for } i = 1, 2, \dots, r \quad (40b)$$

By using SDR relaxation, (40) can be solved similarly to the main RIS phase design problem in (29).

On the other hand, for a given RIS phase profile, the optimal power allocation matrix can be found in closed-form as in Section III-B since the expression in (36) can be stated in the form of $\text{tr}\{\mathbf{P}^H \tilde{\mathbf{A}}_i \mathbf{P}\}$ as in (32). Namely, $\tilde{\mathbf{A}}_i$ becomes $\tilde{\mathbf{A}}_i \triangleq (\mathbf{H}_{ri} \Omega \mathbf{H}_{ar})^H \Sigma_i^{-1} (\mathbf{H}_{ri} \Omega \mathbf{H}_{ar}) + \mathbf{H}_{ai}^H \Sigma_i^{-1} \mathbf{H}_{ai} + \mathbf{H}_{ai}^H \Sigma_i^{-1} \mathbf{H}_{ri} \Omega \mathbf{H}_{ar} + (\mathbf{H}_{ri} \Omega \mathbf{H}_{ar})^H \Sigma_i^{-1} \mathbf{H}_{ai}$ in this scenario based on (36).

Overall, the proposed alternating optimization approach in Algorithm 1 can also be employed for the LoS scenarios as the structure of the optimization problems remains the same.

B. RIS Elements With Adjustable Magnitudes

In most studies in the literature, passive RIS elements are considered, which can control only the phase of the reflected signal, with no control over the magnitude. That is, by considering the signal reflection coefficient for each RIS element as $\omega_i = \beta_i e^{j\phi_i}$, $\beta_i = 1$ is assumed for all $i = 1, 2, \dots, r$ [16], [38], [90], [91]. According to [92], via some techniques such as attaching liquid crystals or graphene under patch elements, one can change the material permeability and permittivity. However, this approach is relatively costly compared to the conventional passive RIS design. In this section, we consider the RIS phase design and power allocation problem when any of these approaches are applied to RIS and the magnitude of the reflected signal at each RIS element can be controlled independently. Since the RIS is still assumed to be passive, the signal magnitudes cannot be increased; hence, the signal reflection coefficient can be controlled to be between 0 and 1, i.e., $0 \leq \beta_i \leq 1$. Thus, the RIS phase profile optimization problem in (4) can be reformulated as

$$\max_{\Omega \in \mathcal{D}^{r \times r}} \quad \text{tr}\{\mathbf{I}(\mathbf{y}_b; \boldsymbol{\theta})\} \quad (41a)$$

$$\text{s.t.} \quad \text{tr}\{\mathbf{I}(\mathbf{y}_e; \boldsymbol{\theta})\} \leq \Delta \quad (41b)$$

$$|[\Omega]_{\ell, \ell}| \leq 1, \quad \ell = 1, \dots, r \quad (41c)$$

where an equality is employed instead of equality in the last constraint. (41) is a convex optimization problem and it does not have a feasibility issue anymore. Hence, it can be solved via CVX for any value of Δ . Therefore, the alternating optimization approach proposed in this study can be applied more effectively in this scenario.

C. Presence of Multiple Eavesdroppers

For the case of multiple eavesdroppers, the theoretical approaches in this manuscript can be extended by two different approaches. Consider the presence of M eavesdroppers with the following measurements (cf. (2)):

$$\mathbf{y}_e^{(j)} = (\mathbf{H}_{re}^{(j)} \Omega \mathbf{H}_{ar}) \mathbf{P} \boldsymbol{\theta} + \boldsymbol{\eta}_e^{(j)} \quad (42)$$

for $j = 1, \dots, M$, where $\mathbf{y}_e^{(j)} \in \mathbb{C}^{n_e^{(j)}}$ is the measurement vector at the j th eavesdropper, $\mathbf{H}_{re}^{(j)}$ is the $n_e^{(j)} \times r$ channel matrix between the RIS and the j th eavesdropper, and $\boldsymbol{\eta}_e^{(j)} \in \mathbb{C}^{n_e}$ is the additive circularly-symmetric Gaussian noise vector at the j th eavesdropper, distributed as $\mathcal{CN}(\mathbf{0}, \Sigma_e^{(j)})$ with $\Sigma_e^{(j)} \succ \mathbf{0}$. Similar to (15), the trace of the FIM can be expressed for the j th eavesdroppers as

$$\text{tr}\{\mathbf{I}(\mathbf{y}_e^{(j)}; \boldsymbol{\theta})\} = \text{tr}\{\mathbf{P}\mathbf{H}_{ar}^H \mathbf{E}^{(j)} \Omega \mathbf{H}_{ar} \mathbf{P}\} \quad (43)$$

with $\mathbf{E}^{(j)} \triangleq (\mathbf{H}_{re}^{(j)})^H (\Sigma_e^{(j)})^{-1} \mathbf{H}_{re}^{(j)}$. Then, based on similar steps, the final form of the RIS phase profile design subproblem can be formulated as follows (cf. Proposition 1):

$$\max_{\omega} \quad \omega^H \mathbf{Q}_b \omega \quad (44a)$$

$$\text{s.t.} \quad \omega^H \mathbf{Q}_e^{(j)} \omega \leq \Delta^{(j)}, \quad j = 1, 2, \dots, M \quad (44b)$$

$$|\omega_\ell| = 1, \ell = 1, \dots, r \quad (44c)$$

where $\Delta^{(j)}$ is the secrecy limit for the j th eavesdropper, and $\mathbf{Q}_b \in \mathbb{C}^{r \times r}$ and $\mathbf{Q}_e^{(j)} \in \mathbb{C}^{r \times r}, j \in \{1, \dots, M\}$ are positive definite Hermitian matrices. Similarly, the second subproblem can be formulated as (cf. (32))

$$\max_{\mathbf{P}} \quad \text{tr}\{\mathbf{P}^H \mathbf{A}_b \mathbf{P}\} \quad (45a)$$

$$\text{s.t.} \quad \text{tr}\{\mathbf{P}^H \mathbf{A}_e^{(j)} \mathbf{P}\} \leq \Delta^{(j)}, j = 1, 2, \dots, M \quad (45b)$$

$$\text{tr}\{\mathbf{P} \mathbf{P}^T\} \leq P_S \quad (45c)$$

$$\mathbf{P} \mathbf{P}^T \succeq \mathbf{0} \quad (45d)$$

where $\mathbf{A}_e^{(j)} \triangleq (\mathbf{H}_{re}^{(j)} \mathbf{\Omega} \mathbf{H}_{ar})^H (\mathbf{\Sigma}_e^{(j)})^{-1} (\mathbf{H}_{re}^{(j)} \mathbf{\Omega} \mathbf{H}_{ar})$. Since the number of secrecy constraints is more than one, using Algorithm 2 for rank reduction may become time-consuming. Therefore, using the penalty method for rank reduction can help find a feasible solution for this problem.

The second approach is to keep the total information leakage to eavesdroppers under a constraint. In this case, the secrecy constraint can be defined as

$$\sum_{j=1}^M \text{tr}\{\mathbf{I}(\mathbf{y}_e^{(j)}; \mathbf{\Theta})\} = \sum_{j=1}^M \text{tr}\{\mathbf{P} \mathbf{H}_{ar}^H \mathbf{\Omega}^H \mathbf{E}^{(j)} \mathbf{\Omega} \mathbf{H}_{ar} \mathbf{P}\} \quad (46)$$

$$= \text{tr}\{\mathbf{P} \mathbf{H}_{ar}^H \mathbf{\Omega}^H \sum_{j=1}^M \mathbf{E}^{(j)} \mathbf{\Omega} \mathbf{H}_{ar} \mathbf{P}\} \quad (47)$$

$$\triangleq \text{tr}\{\mathbf{P} \mathbf{H}_{ar}^H \mathbf{\Omega}^H \bar{\mathbf{E}} \mathbf{\Omega} \mathbf{H}_{ar} \mathbf{P}\} \quad (48)$$

$$\leq \Delta \quad (49)$$

which results in the same form of the problem solved in Section III by replacing $\mathbf{E}$ in (15) with $\bar{\mathbf{E}} = \sum_{j=1}^M \mathbf{E}^{(j)}$.

VI. CONCLUDING REMARKS

We have investigated the secure transmission of a deterministic complex-valued parameter vector from a transmitter to an intended receiver in the presence of an eavesdropper. It has been assumed that the transmitter is in NLoS with both the intended receiver and the eavesdropper, which receive the transmitted signal via an RIS available in the environment. The aim has been to design the RIS phase profile and the power allocation matrix at the transmitter to enhance the estimation accuracy at the intended receiver while limiting that at the eavesdropper. The trace of the FIM, equivalently, the average Fisher information, has been employed as the estimation performance metric, and its closed form expression has been derived. Based on that expression, the joint RIS phase profile and power allocation problem has been formulated, and it has been solved via alternating optimization. During alternating optimization, when the power allocation matrix is fixed, the optimal RIS phase profile design problem has been formulated as a non-convex QCQP, and it has been solved via SDR and rank reduction. When the RIS phase profile is fixed, an LP formulation has been obtained for optimal power allocation. Via simulations, the effects of RIS phase design and power allocation have been illustrated individually and jointly.

Moreover, extensions have been presented by considering the presence of LoS paths in the environment, the availability of RIS elements with adjustable magnitudes, and the presence of multiple eavesdroppers.

REFERENCES

- [1] A. Almohamad et al., "Smart and secure wireless communications via reflecting intelligent surfaces: A short survey," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1442–1456, 2020.
- [2] C. Lipps, S. Baradie, M. Noushinfar, J. Herbst, A. Weinand, and H. D. Schotten, "Towards the sixth generation (6G) wireless systems: Thoughts on physical layer security," in *Proc. IEEE Mobile Commun. - Technol. Appl.: 25th ITG-Symp.*, 2021, pp. 1–6.
- [3] S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, "Security requirements and challenges of 6G technologies and applications," *Sensors*, vol. 22, no. 5, 2022, Art. no. 1969.
- [4] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
- [5] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *Proc. 2015 IEEE Symp. Comput. Commun.*, 2015, pp. 180–187.
- [6] T. Kavitha and D. Sridharan, "Security vulnerabilities in wireless sensor networks: A survey," *J. Inf. Assurance Secur.*, vol. 5, no. 1, pp. 31–44, 2010.
- [7] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
- [8] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.
- [9] D. P. Osorio, J. D. Sánchez, and H. Alves, "Physical-layer security for 5G and beyond," in *Wiley 5G Ref: The Essential 5G Reference Online*. Hoboken, NJ, USA: Wiley, 2019, pp. 1–19.
- [10] Y. Wu, T. Q. Duong, and A. L. Swindlehurst, "Safeguarding 5G-and-beyond networks with physical layer security," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 4–5, Oct. 2019.
- [11] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [12] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.
- [13] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Nov. 2019.
- [14] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.
- [15] G. Amarasinghe, R. F. Schaefer, and H. V. Poor, "Linear precoder design for physical layer security via reconfigurable intelligent surfaces," in *Proc. 2020 IEEE 21st Int. Workshop Signal Process. Adv. Wireless Commun.*, 2020, pp. 1–5.
- [16] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, Oct. 2019.
- [17] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599–82612, 2019.
- [18] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1488–1492, Sep. 2019.
- [19] V. Kumar, M. F. Flanagan, D. W. K. Ng, and L.-N. Tran, "On the secrecy rate under statistical QoS provisioning for RIS-assisted MISO wiretap channel," in *Proc. 2021 IEEE Glob. Commun. Conf.*, 2021, pp. 1–6.
- [20] H. Niu et al., "Joint beamforming design for secure RIS-assisted IoT networks," *IEEE Internet Things J.*, vol. 10, no. 2, pp. 1628–1641, Jan. 2023.
- [21] Z. Chu, W. Hao, P. Xiao, and J. Shi, "Intelligent reflecting surface aided multi-antenna secure transmission," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, Jan. 2020.
- [22] W. Shi, X. Zhou, L. Jia, Y. Wu, F. Shu, and J. Wang, "Enhanced secure wireless information and power transfer via intelligent reflecting surface," *IEEE Commun. Lett.*, vol. 25, no. 4, pp. 1084–1088, Apr. 2021.

- [23] S. Hong, C. Pan, G. Zhou, H. Ren, and K. Wang, "Outage constrained robust transmission design for IRS-aided secure communications with direct communication links," *IEEE Trans. Commun.*, vol. 72, no. 3, pp. 1548–1564, Mar. 2024.
- [24] Z. Chu et al., "Secrecy rate optimization for intelligent reflecting surface assisted MIMO system," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1655–1669, 2021.
- [25] F. Shu et al., "Enhanced secrecy rate maximization for directional modulation networks via IRS," *IEEE Trans. Commun.*, vol. 69, no. 12, pp. 8388–8401, Dec. 2021.
- [26] W. Xu, J. Zhang, S. Cai, J. Wang, and Y. Wu, "RIS-assisted MIMO secure communications with Bob's statistical CSI and without Eve's CSI," *Digit. Commun. Netw.*, vol. 9, no. 3, pp. 638–644, 2022.
- [27] P. Xu, G. Chen, G. Pan, and M. Di Renzo, "Ergodic secrecy rate of RIS-assisted communication systems in the presence of discrete phase shifts and multiple eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 629–633, Mar. 2021.
- [28] M.-M. Zhao, K. Xu, Y. Cai, Y. Niu, and L. Hanzo, "Secrecy rate maximization of RIS-assisted SWIPT systems: A two-timescale beamforming design approach," *IEEE Trans. Wireless Commun.*, vol. 22, no. 7, pp. 4489–4504, Jul. 2023.
- [29] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," 2007, *arXiv:0708.4219*.
- [30] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Thirdquarter 2014.
- [31] N.-P. Nguyen, T. L. Thanh, T. Q. Duong, and A. Nallanathan, "Secure communications in cognitive underlay networks over nakagami-m channel," *Phys. Commun.*, vol. 25, pp. 610–618, 2017.
- [32] T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao, "Secrecy performance analysis with relay selection methods under impact of co-channel interference," *IET Commun.*, vol. 9, no. 11, pp. 1427–1435, 2015.
- [33] T. T. Duy, T. L. Thanh, and V. N. Q. Bao, "Secrecy outage probability of dual-hop network in presence of co-channel interference," in *Proc. Int. Conf. Green Hum. Inf. Technol.*, Ho Chi Minh City, Vietnam, 2014, pp. 11–15.
- [34] W. Shi, J. Xu, W. Xu, M. D. Renzo, and C. Zhao, "Secure outage analysis of RIS-assisted communications with discrete phase control," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 5435–5440, Apr. 2023.
- [35] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. Di Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12296–12300, Oct. 2020.
- [36] I. Trigui, W. Ajib, and W.-P. Zhu, "Secrecy outage probability and average rate of RIS-aided communications using quantized phases," *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1820–1824, Jun. 2021.
- [37] M. H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1443–1447, May 2021.
- [38] Y. Liu, Z. Su, C. Zhang, and H.-H. Chen, "Minimization of secrecy outage probability in reconfigurable intelligent surface-assisted mimome system," *IEEE Trans. Wireless Commun.*, vol. 22, no. 2, pp. 1374–1387, Feb. 2023.
- [39] S. Keşir, S. Kayraklık, İ. Hökelek, A. E. Pusane, E. Basar, and A. Görçin, "Measurement-based characterization of physical layer security for RIS-assisted wireless systems," 2022, *arXiv:2212.07254*.
- [40] P. Li et al., "RIS-assisted scheduling for high-speed railway secure communications," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 3488–3501, Mar. 2023.
- [41] A. Almohamad, A. Al-Kababji, A. Tahir, T. Khattab, and M. Hasna, "On optimizing the secrecy performance of RIS-assisted cooperative networks," in *Proc. 2020 IEEE 92nd Veh. Technol. Conf.*, 2020, pp. 1–5.
- [42] H. V. Poor, *An Introduction to Signal Detection and Estimation*. Berlin, Germany: Springer, 1998.
- [43] J. Zhang, R. S. Blum, and H. V. Poor, "Approaches to secure inference in the Internet of Things: Performance bounds, algorithms, and effective attacks on IoT sensor networks," *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 50–63, Sep. 2018.
- [44] Ç. Göken and S. Gezici, "ECRB-based optimal parameter encoding under secrecy constraints," *IEEE Trans. Signal Process.*, vol. 66, no. 13, pp. 3556–3570, Jul. 2018.
- [45] Ç. Göken and S. Gezici, "Optimal parameter encoding based on worst case Fisher information under a secrecy constraint," *IEEE Signal Process. Lett.*, vol. 24, no. 11, pp. 1611–1615, Nov. 2017.
- [46] C. Gökten, S. Gezici, and O. Arikan, "Estimation theoretic optimal encoding design for secure transmission of multiple parameters," *IEEE Trans. Signal Process.*, vol. 67, no. 16, pp. 4302–4316, Aug. 2019.
- [47] D. Gurgunoglu, C. Gökten, and S. Gezici, "Optimal power allocation for secure estimation of multiple parameters," *IEEE Signal Process. Lett.*, vol. 28, pp. 1784–1788, 2021.
- [48] E. M. Abadi, C. Gökten, C. Ozturk, and S. Gezici, "Optimal power allocation and optimal linear encoding for parameter estimation in the presence of a smart Eavesdropper," *IEEE Trans. Signal Process.*, vol. 70, pp. 4093–4108, 2022.
- [49] X. Song, J. Xu, F. Liu, T. X. Han, and Y. C. Eldar, "Intelligent reflecting surface enabled sensing: Cramér-Rao lower bound optimization," in *Proc. 2022 IEEE Globecom Workshops*, 2022, pp. 413–418.
- [50] X. Wang, Z. Fei, J. Huang, and H. Yu, "Joint waveform and discrete phase shift design for RIS-assisted integrated sensing and communication system under Cramér-Rao bound constraint," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 1004–1009, Jan. 2022.
- [51] V. Nagesha and S. M. Kay, "Cramer-Rao lower bounds for complex parameters," [Online]. Available: <https://www.ele.uri.edu/faculty/kay/New%20web/Books.htm>
- [52] T. Menni, E. Chaumette, P. Larzabal, and J. P. Barbot, "New results on deterministic Cramér-Rao bounds for real and complex parameters," *IEEE Trans. Signal Process.*, vol. 60, no. 3, pp. 1032–1049, Mar. 2012.
- [53] F. Farokhi and H. Sandberg, "Fisher information as a measure of privacy: Preserving privacy of households with smart meters using batteries," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4726–4734, Sep. 2018.
- [54] A. Özçelikale and T. M. Duman, "Cooperative precoding and artificial noise design for security over interference channels," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2234–2238, Dec. 2015.
- [55] X. Guo, A. S. Leong, and S. Dey, "Estimation in wireless sensor networks with security constraints," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 53, no. 2, pp. 544–561, Apr. 2017.
- [56] M. Shirazi and A. Vosoughi, "On Bayesian Fisher information maximization for distributed vector estimation," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 5, no. 4, pp. 628–645, Dec. 2019.
- [57] D. Gürgünöglü, B. Dulek, and S. Gezici, "Power adaptation for vector parameter estimation according to Fisher information based optimality criteria," *Signal Process.*, vol. 192, 2022, Art. no. 108390.
- [58] I. Bahceci and A. K. Khandani, "Linear estimation of correlated data in wireless sensor networks with optimum power allocation and analog modulation," *IEEE Trans. Commun.*, vol. 56, no. 7, pp. 1146–1156, Jul. 2008.
- [59] A. F. Emery and A. V. Nenarokomov, "Optimal experiment design," *Meas. Sci. Technol.*, vol. 9, pp. 864–876, Jun. 1998.
- [60] S. Xu and K. Dogancay, "Optimal sensor placement for 3-D angle-of-arrival target localization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 53, no. 3, pp. 1196–1211, Jun. 2017.
- [61] R. Kalaba and K. Spingarn, *Control, Identification, and Input Optimization. Mathematical Concepts and Methods in Science and Engineering*, 1st ed. Berlin, Germany: Springer, 1982.
- [62] E. Tzoreff and A. J. Weiss, "Single sensor path design for best emitter localization via convex optimization," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 939–951, Feb. 2017.
- [63] J. C. Bezdek and R. J. Hathaway, "Some notes on alternating optimization," in *Proc. Adv. Soft Comput.—AFSS 2002: 2002 AFSS Int. Conf. Fuzzy Syst. Calcutta*, India, 2002, pp. 288–300.
- [64] E. Ollila, V. Koivunen, and J. Eriksson, "On the Cramér-Rao bound for the constrained and unconstrained complex parameters," in *Proc. 2008 5th IEEE Sensor Array Multichannel Signal Process. Workshop*, 2008, pp. 414–418.
- [65] R. G. Gallager, *Stochastic Processes: Theory Appl.*, Cambridge: Cambridge University Press, 2013.
- [66] K. B. Petersen et al., "The matrix cookbook," *Tech. Univ. Denmark*, vol. 7, no. 15, 2008, Art. no. 510.
- [67] A. M. Farah, "Generalized and quadratic eigenvalue problems with hermitian matrices," Ph.D. dissertation, University of Birmingham, Birmingham, U.K., 2012.
- [68] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.
- [69] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

- [70] E. K. Chong and S. H. Zak, *An Introduction to Optimization*, vol. 75. Hoboken, NJ, USA: Wiley, 2013.
- [71] P. T. Boggs and J. W. Tolle, "Sequential quadratic programming," *Acta Numerica*, vol. 4, pp. 1–51, 1995.
- [72] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming version 2.1," Mar. 2014. [Online]. Available: <https://cvxr.com/cvx>
- [73] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in *Proc. Recent Adv. Learn. Control*, V. Blondel, S. Boyd, and H. Kimura, eds., Berlin, Germany, 2008, pp. 95–110. [Online]. Available: http://stanford.edu/boyd/graph_dcp.html
- [74] J. Löfberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proc. CACSD Conf.*, Taipei, Taiwan, 2004, pp. 284–289.
- [75] G. Yang, X. Xu, Y.-C. Liang, and M. Di Renzo, "Reconfigurable intelligent surface-assisted non-orthogonal multiple access," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 3137–3151, May 2021.
- [76] X. Mu, Y. Liu, L. Guo, J. Lin, and R. Schober, "Simultaneously transmitting and reflecting (STAR) RIS aided wireless communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 5, pp. 3083–3098, May 2022.
- [77] T. Jiang and Y. Shi, "Over-the-air computation via intelligent reflecting surfaces," in *Proc. 2019 IEEE Glob. Commun. Conf.*, 2019, pp. 1–6.
- [78] M. M. Pishrow and J. Abouei, "A sequential constraint relaxation framework to design phase-coded sequences for radar systems," *Digit. Signal Process.*, vol. 136, 2023, Art. no. 103985.
- [79] Z. Liu, X. Li, H. Ji, H. Zhang, and V. C. M. Leung, "Toward STAR-RIS-Empowered integrated sensing and communications: Joint active and passive beamforming design," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 15991–16005, Dec. 2023.
- [80] P. Cao, J. Thompson, and H. V. Poor, "A sequential constraint relaxation algorithm for rank-one constrained problems," in *Proc. IEEE 2017 25th Eur. Signal Process. Conf.*, 2017, pp. 1060–1064.
- [81] R. J. Vanderbei et al., *Linear Programming*. Berlin, Germany: Springer, 2020.
- [82] A. Geletu, "Solving optimization problems using the MATLAB optimization toolbox - a tutorial," TU-Ilmenau, Fakultät für Mathematik und Naturwissenschaften, Dec. 2007. [Online]. Available: https://www.researchgate.net/publication/255586170_Solving_Optimization_Problems_using_the_Matlab_Optimization_Toolbox_-_a_Tutorial
- [83] S. Voulgaropoulou, "Computational complexity analysis of linear optimization algorithms," Ph.D. dissertation, University of Macedonia, Thessaloniki, Greece, 2022.
- [84] T. Wang, F. Fang, and Z. Ding, "Joint phase shift and beamforming design in a multi-user MISO STAR-RIS assisted downlink NOMA network," *IEEE Trans. Veh. Technol.*, vol. 72, no. 7, pp. 9031–9043, Jul. 2023.
- [85] S. Zhang and R. Zhang, "Intelligent reflecting surface aided multi-user communication: Capacity region and deployment strategy," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 5790–5806, Sep. 2021.
- [86] Y. Shi, H. D. Tuan, S. W. Su, and A. V. Savkin, "Multiple matrix rank constrained optimization for optimal power flow over large scale transmission networks," in *Proc. IEEE 2016 5th Int. Conf. Smart Cities Green ICT Syst.*, 2016, pp. 1–6.
- [87] M. Jiang, Y. Li, G. Zhang, and M. Cui, "Achievable rate region maximization in intelligent reflecting surfaces-assisted interference channel," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 13406–13412, Dec. 2021.
- [88] Y. Shi, H. D. Tuan, D. Hoang, P. Apkarian, and A. V. Savkin, "Global optimal power flow over large-scale power transmission networks," *Syst. Control Lett.*, vol. 118, pp. 16–21, 2018.
- [89] E. Khordad, S. Akhlaghi, and M. Mirzaee, "Maximising the minimum achievable secrecy rate of two-way relay networks using the null space beamforming method," *IET Commun.*, vol. 11, no. 6, pp. 793–800, 2017.
- [90] C. Pan et al., "Multicell MIMO communications relying on intelligent reflecting surfaces," *IEEE Trans. Wireless Commun.*, vol. 19, no. 8, pp. 5218–5233, Aug. 2020.
- [91] W. Yan, X. Yuan, and X. Kuai, "Passive beamforming and information transfer via large intelligent surface," *IEEE Wireless Commun. Lett.*, vol. 9, no. 4, pp. 533–537, Apr. 2020.
- [92] M. M. Amri, "Recent trends in the reconfigurable intelligent surfaces (RIS): Active RIS to brain-controlled RIS," in *Proc. 2022 IEEE Int. Conf. Commun., Satell.*, 2022, pp. 299–304.



Erfan Mehdipour Abadi (Member, IEEE) received the B.S. degree in electrical engineering from the University of Tabriz, Tabriz, Iran, in 2018, and the M.S. degree in electrical engineering from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2021. He is currently working toward the Ph.D. degree in electrical engineering with Wayne State University, Detroit, MI, USA. From 2021 to 2023, he conducted research in electrical and electronic engineering with Bilkent University, Ankara, Türkiye. His research interests include detection and estimation, anomaly detection, and stochastic hybrid system analysis.



Ayda Nodel Hokmabadi (Graduate Student Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Tabriz, Tabriz, Iran, in 2021. She is currently working toward the M.Sc. degree with the Department of Electrical and Electronics Engineering, Bilkent University, Ankara, Türkiye. Her research interests include multiple access techniques, reconfigurable intelligent surfaces, machine learning, and AI-enabled 5G/6G communication networks.



Sinan Gezici (Senior Member, IEEE) received the B.Sc. degree in electrical and electronics engineering from Bilkent University, Ankara, Türkiye, in 2001, and the Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ, USA, in 2006. From 2006 to 2007, he was with Mitsubishi Electric Research Laboratories, Cambridge, MA, USA. Since 2007, he has been with the Department of Electrical and Electronics Engineering, Bilkent University, where he is currently a Professor. Among his publications in these areas is the book *Ultrawideband Positioning Systems: Theoretical Limits, Ranging Algorithms, and Protocols* (Cambridge University Press, 2008). His research interests include areas of detection and estimation theory, wireless communications, and localization systems. He is an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS LETTERS, and *Journal of Communications and Networks*.