Minimization of Secrecy Outage Probability in Intelligent Reflecting Surfaces-Assisted MIMOME System

Yiliang Liu, *Member, IEEE*, Zhou Su, *Senior Member, IEEE*,
Chi Zhang, and Hsiao-Hwa Chen, *Fellow, IEEE*

Abstract

This article investigates physical layer security (PLS) in intelligent reflecting surface (IRS)-assisted multiple-input multiple-output multiple-antenna-eavesdropper (MIMOME) channels. Existing researches ignore the problem that secrecy rate can not be calculated if the eavesdropper's instantaneous channel state information (CSI) is unknown. Further, without the secrecy rate expression, beamforming and phase shifter optimization with the purpose of PLS enhancement is not available. To address these problems, we first give the expression of secrecy outage probability for any beamforming vector and phase shifter matrix as the IRS-assisted PLS metric, which is measured based on the eavesdropper's statistical CSI. Then, with the aid of the expression, we formulate the minimization problem of secrecy outage probability that is solved via alternately optimizing beamforming vectors and phase shift matrices. In the case of single-antenna transmitter or single-antenna legitimate receiver, the proposed alternating optimization scheme can be simplified to reduce computational complexity. Finally, it is demonstrated that the secrecy outage probability is significantly reduced with the proposed methods compared to current IRS-assisted PLS systems.

Index Terms

Intelligent reflecting surfaces, physical layer security, secrecy outage probability, beamforming, phase shifter optimization

Y. Liu (email: liuyiliang@xjtu.edu.cn) and Z. Su (email: zhousu@ieee.org) are with the School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 710049, China. C. Zhang (email: maye1998@163.com) is with the School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, China. H.-H. Chen (email: hshwchen@mail.ncku.edu.tw) is with the Department of Engineering Science, National Cheng Kung University, Tainan 70101, Taiwan.

I. INTRODUCTION

Serious concerns on information security have been raised in 5G and beyond eras due to the broadcasting nature of wireless channels and hundreds of millions of vulnerable connected devices [1]. Nowadays, physical layer security (PLS) has attracted much attention for strengthening information security as it is capable of achieving confidential information transmission by exploring random characteristics of the wireless medium. The information-theoretic security and cryptography-free characteristic of the PLS technology have received intensive research interests in wireless communications and networks [2].

The secrecy capacity of PLS highly depends on the channel difference between legitimate users and eavesdropping users, whereas the channel of legitimate users is usually highly correlated with the eavesdropping channels in most of wireless scenarios, resulting in a low secrecy capacity or secrecy rate [2]. Recent investigations show that IRS composed of a large number of low-cost passive reflecting elements can control the direction of the electromagnetic wave by adaptively adjusting the phase shift of each element of IRS [3], whereby the channel difference between legitimate users and eavesdropping users is enlarged, and the secrecy capacities of legitimate users can be improved consequently. Following that, plenty of researches have been conducted to investigate IRS-assisted PLS, including information-theoretic aspects [4]–[6] and secure beamforming with phase shifter adjustments [7]–[14].

The instantaneous CSIs of eavesdroppers are usually unknown when the eavesdroppers keep silent, which is a usual issue but ignored in recent IRS-assisted PLS researches [7]–[13]. The above works maximize the secrecy capacity or secrecy rate via beamforming and phase shifter optimization, assuming that instantaneous CSIs of eavesdroppers are available. However, the secrecy capacity or secrecy rate can not be measured if instantaneous CSIs of eavesdroppers are unknown. To address the eavesdropper's CSI issue, typical methodologies are secure beamforming technologies with secrecy outage-based PLS coding [15], [16], where secure beamforming can reduce the secrecy outage probability. Regarding the secrecy outage probability as a threshold, the PLS coding rate is adjusted during confidential data transmission phases. However, the existing expressions of secrecy outage probability for IRS-assisted PLS focus on single-antenna scenarios [4], [5] or are deduced with fixed phase shifter matrices and beamforming vectors [6], which are not suitable for beamforming and phase shifter optimization. Feng *et al.* proposed an alternating guideline to solve this eavesdropper's CSI problem [14]. They simulate a great

deal of the eavesdropper's CSIs by sample average approximation-based method, and use these simulated CSIs as the instantaneous CSIs of eavesdroppers to calculate an approximate secrecy rate as the optimization objective of beamforming and phase shifter optimization algorithms. The generation process of many CSI samples causes a large latency, which inevitably increases the cost of computing modules.

According to the above discussion, the first concerned problem in this paper is to find an expression of secrecy outage probability in MIMOME scenarios as the performance metric of IRS-assisted PLS. Then, an optimization algorithm should be designed to minimize the secrecy outage probability. The main contributions of this work are summarized as follows.

1) Firstly, we formulate the PLS model of an IRS-assisted MIMOME channel, where beamforming and phase shifter are optimized for security purposes. As the eavesdropper's instantaneous CSI is unknown, the optimization objective is to minimize the secrecy outage probability measured with the eavesdropper's statistical CSI.
2) Due to the mathematical complexity of the IRS-assisted MIMOME channel model, it is hard to get the exact expressions of secrecy outage probability. Here, we use the Gamma distribution to fit the closed-form expression of secrecy outage probability for any beamforming vector and phase shifter matrix, then apply KolmogorovSmirnov (KS) test to examine the fitting goodness.
3) With the expression of secrecy outage probability, we transform the minimization problem of secrecy outage probability into two sub-problems, i.e., beamforming vector and phase shifter matrix optimization, which are solved optimally by generalized Rayleigh quotient and quadratic optimization methods, respectively. Then, an alternating optimization algorithm is proposed to find the global results for the beamforming vector and phase shifter matrix. Also, secure beamforming and phase shift schemes are presented for the single-antenna transmitter or single-antenna legitimate receiver case, which have lower computational complexity than the aforementioned alternating optimization algorithm.

The remainder of the paper is organized as follows. Section II surveys the related works. Section III describes the system model and problem formulation. The expressions of secrecy outage probability are given in Section IV. The optimization algorithms of beamforming vector and phase shifter matrix are proposed in Section V. The optimization algorithms in single-antenna cases are presented in Section VI. We show simulation results in Section VII, and conclude this

paper in Section VIII.

Notations: Bold uppercase letters, such as $\mathbf{A}$, denote matrices, and bold lowercase letters, such as $\mathbf{a}$, denote column vectors. $\mathbf{A}^{\dagger}$, $\mathbf{A}^{\mathrm{T}}$, and $\mathbf{A}^{\mathrm{H}}$ represent the conjugate transformation, transpose, and conjugate transpose of $\mathbf{A}$, respectively. $\mathbf{I}_a$ is an identity matrix with its rank a. $\mathcal{CN}(\mu, \sigma^2)$ is a complex normal (Gaussian) distribution with mean μ and variance σ^2. $(\mathbf{A})^{-1}$ is the inverse function of $\mathbf{A}$. $|\mathbf{x}|$ is the Euclidean norm of $\mathbf{x}$. $\mathrm{diag}(\mathbf{x})$ is the diagonal matrix of $\mathbf{x}$. $\mathbb{E}(\cdot)$ is the expectation operation. $\mathrm{vec}(\mathbf{A})$ is the vectorization of the diagonal elements of $\mathbf{A}$. $\arg(x)$ is the angle of complex variable x. An $a \times (b+c)$ matrix $[\mathbf{A}, \mathbf{B}]$ denotes a combined matrix between an $(a \times b)$ matrix $\mathbf{A}$ and an $(a \times c)$ matrix $\mathbf{B}$. $\circ$ is the Hadamard product. $\Re(x)$ means the real part of complex variable x.

II. Related Works

A. Information-Theoretic Research on IRS-assisted PLS

As mentioned in [6], the information-theoretic research about is fundamental that provides optimization objectives, constraint functions, as well as performance metrics for beamforming and phase shifter. The channel models with IRS are the main mathematical challenges of this research. Yang *et al.* considered the IRS-assisted single-antenna case, i.e., every transmitter, legitimate receiver, and eavesdropper has one antenna, then used the Gaussian distribution to get the expression of secrecy outage probability [4]. Trigui *et al.* gave the expressions of ergodic secrecy rate and secrecy outage probability in the IRS-assisted single-antenna case, simultaneously [5]. They used Fox's H transform theory and the Mellin-Barnes integrals to get these expressions. The IRS-assisted MIMOME channel model was taken into account by Zhang *et al.* [6], where the model is based on the zero-forcing phase shifter matrix and maximal ratio combining receiving vector proposed in [17] for security purposes. Also, they deduced the expression of ergodic secrecy rate and secrecy outage probability by the $\kappa - \mu$ distribution [18].

B. Secure beamforming with Phase Shifter Adjustments

The feature of secure beamforming in IRS-assisted PLS is the phase shifter adjustment. The secrecy rate maximization with respect to the variables of beamforming vectors and phase shifter matrices is a non-convex problem and is usually solved by alternating optimization over individual beamforming and phase shifter [7]–[13]. Especially, Cui *et al.* considered the IRS-assisted multiple-input single-output multiple-antenna-eavesdropper (MISOME) model. In

this model, the secrecy rate is maximized by alternating optimization between beamforming vector and phase shifter matrix, in which the subproblems of beamforming and phase shifter optimization are solved by generalized Rayleigh quotient and semidefinite programming (SDP), respectively [7]. Shen *et al.* simplified the phase shifter optimization via the minorization-maximization (MM) [8] and element-wise block coordinate descent (BCD)-based methods [9]. Further, Xu *et al.* introduced the artificial noise (AN) technique in IRS-assisted PLS to improve the secrecy rate [10]. Dong *et al.* considered the IRS-assisted MIMOME model, and used the MM algorithm to optimize the phase shifter matrix for maximizing the secrecy rate [11]. Niu *et al.* formulated the weighted sum secrecy rate maximization problem in the IRS-assisted multiple user MISOME scenarios, where a successive convex approximation (SCA) technique is employed to find the optimal beamforming and AN signals [12]. Yu *et al.* extended the work of [12] by adding the multiple IRS devices and considered the error of channel estimation [13].

C. Discussion

The existing investigations of IRS-assisted PLS do not concern secrecy outage probability in the MIMOME model. Besides, the optimization algorithm should be presented for secrecy outage probability minimization. In this work, we first provide the expression of secrecy outage probability in the IRS-assisted MIMOME channel for any beamforming vector and phase shifter matrix, followed by secure beamforming and phase shifter optimization schemes that can reduce the secrecy outage probability.

III. System Model and Problem Formulation

Considering that the eavesdropper's instantaneous CSI is unknown for legitimate users, the channel model of IRS-assisted MIMOME is established in this section.

A. Channel Model

This article considers an IRS-assisted MIMOME channel, as shown in Fig. 1, including a transmitter (Alice) with N_t antennas, an eavesdropper (Eve) with N_e antennas, an IRS equipped with N_s programmable phase shifter elements, and a legitimate user (Bob) with N_r antennas. Assume that all wireless channels obey spatial-uncorrelated Rayleigh fading, i.e., the channel from Alice to Eve is defined as $\mathbf{H}_e \sim \mathcal{CN}_{N_e,N_t}(\mathbf{0}, \mathbf{I}_{N_e} \otimes \mathbf{I}_{N_t})$, the channel from Alice to Bob is defined as $\mathbf{H}_b \sim \mathcal{CN}_{N_r,N_t}(\mathbf{0}, \mathbf{I}_{N_r} \otimes \mathbf{I}_{N_t})$, the channel from Alice to IRS is defined as $\mathbf{H} \sim$

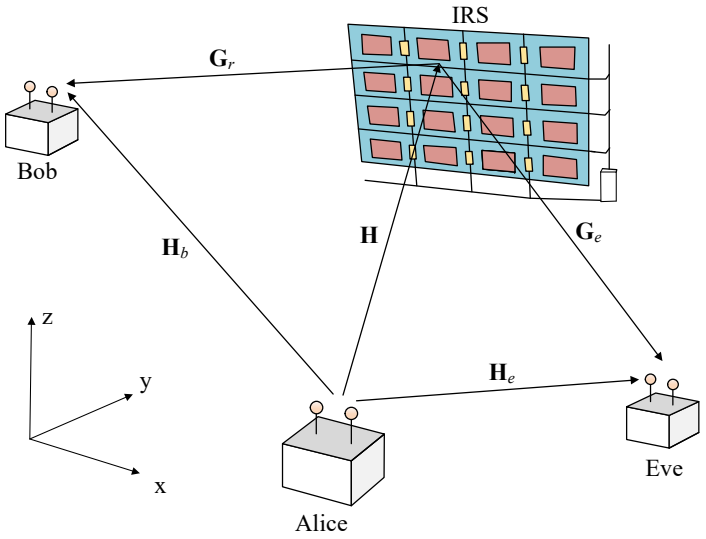


Fig. 1: IRS-assisted MIMOME model, where $(\alpha\mathbf{H}_b + \mathbf{G}_r\mathbf{\Phi}\mathbf{H})$ and $(\beta\mathbf{H}_e + \mathbf{G}_e\mathbf{\Phi}\mathbf{H})$ are defined as the main channel and wiretap channel, respectively. The main and wiretap channels can be adjusted for the PLS purpose by phase shift matrix $\mathbf{\Phi}$ of the IRS.

$\mathcal{CN}_{N_s,N_t}(\mathbf{0}, \mathbf{I}_{N_s} \otimes \mathbf{I}_{N_t})$, the channel from IRS to Bob is defined as $\mathbf{G}_r \sim \mathcal{CN}_{N_r,N_s}(\mathbf{0}, \mathbf{I}_{N_r} \otimes \mathbf{I}_{N_s})$, and the channel from IRS to Eve is defined as $\mathbf{G}_e \sim \mathcal{CN}_{N_e,N_s}(\mathbf{0}, \mathbf{I}_{N_e} \otimes \mathbf{I}_{N_s})$. Let $\alpha \in [0, 1]$ and $\beta \in [0, 1]$ denote the existence probabilities of the channel from Alice to Bob and the channel from Alice to Eve, e.g., $\alpha = 1$ means that there is the direct channel between Alice to Bob, and $\beta = 0.3$ means a 30% probability that the direct channel from Alice to Eve is existed.

Alice uses beamforming vector $\mathbf{w} \in \mathbb{C}^{N_t \times 1}$ to transmit confidential information-bearing signal x to Bob, where $\mathbf{w}^{\mathrm{H}}\mathbf{w} = P \leq \rho$, P is the actual transmission power, ρ is the transmission power constraint, and $\mathbb{E}(xx^{\mathrm{H}}) = 1$. In addition, IRS controls programmable phase shifter elements via a phase shifter matrix, where the phase shifter matrix is defined as an $N_s \times N_s$ matrix $\mathbf{\Phi}$, i.e.,

$$\mathbf{\Phi} = \mathrm{diag}[\exp(j\theta_1), ..., \exp(j\theta_n), ..., \exp(j\theta_{N_s})], \tag{1}$$

and $\theta_n \in [0, 2\pi)$ is the phase introduced by the nth phase shifter element of IRS.

With beamforming vector $\mathbf{w}$ and phase shifter matrix $\mathbf{\Phi}$, the received signals at Bob and Eve can be expressed as

$$\mathbf{y} = (\alpha\mathbf{H}_b + \mathbf{G}_r\mathbf{\Phi}\mathbf{H})\mathbf{w}x + \mathbf{n}, \tag{2}$$

$$\mathbf{y}_e = (\beta\mathbf{H}_e + \mathbf{G}_e\mathbf{\Phi}\mathbf{H})\mathbf{w}x + \mathbf{n}_e, \tag{3}$$

where $(\alpha\mathbf{H}_b+\mathbf{G}_r\mathbf{\Phi}\mathbf{H})$ and $(\beta\mathbf{H}_e+\mathbf{G}_e\mathbf{\Phi}\mathbf{H})$ are known as the main channel and wiretap channel, respectively. $\mathbf{n}$ and $\mathbf{n}_e$ is the additive white Gaussian noise (AWGN) obeying $\mathcal{CN}_{N_r,1}(\mathbf{0},\sigma^2\mathbf{I}_{N_r})$ and $\mathcal{CN}_{N_e,1}(\mathbf{0},\sigma_e^2\mathbf{I}_{N_e})$, respectively.

Considering a pessimistic scenario that Eve knows the instantaneous CSI of all channels, including $\mathbf{G}_r$, $\mathbf{H}_b$, $\mathbf{H}$, $\mathbf{G}_e$, $\mathbf{\Phi}$, and $\mathbf{H}_e$, while Alice, Bob, and IRS only know the instantaneous CSIs of legitimate devices, including $\mathbf{G}_r$, $\mathbf{H}_b$, $\mathbf{H}$, and $\mathbf{\Phi}$. Since instantaneous CSI $\mathbf{H}_e$ and $\mathbf{G}_e$ are unknown for legitimate users, with the diversity technology of multiple-input multiple-output (MIMO), the phase shifter matrix is usually adjusted for maximizing diversity gain via maximal-ratio transmission (MRT), i.e., $\max_{\mathbf{\Phi}}\lambda_{\max}[(\alpha\mathbf{H}_b+\mathbf{G}_r\mathbf{\Phi}\mathbf{H})^{\mathrm{H}}(\alpha\mathbf{H}_b+\mathbf{G}_r\mathbf{\Phi}\mathbf{H})]$, where $\lambda_{\max}(\mathbf{A})$ is the largest eigenvalue of $\mathbf{A}$ [19], it is just a method of capacity improvement but is not a desired design for secrecy performance of IRS-assisted PLS.

B. Secrecy Rate and Secrecy Outage Probability

The usual secrecy performance in PLS is secrecy rate [20], which is formulated as follows,

$$C_s=(C_m-C_w)^+, \tag{4}$$

where C_m and C_w are defined as the main channel capacity and wiretap channel capacity, i.e.,

$$C_m=\log_2\left[1+\frac{1}{\sigma^2}|(\alpha\mathbf{H}_b+\mathbf{G}_r\mathbf{\Phi}\mathbf{H})\mathbf{w}|^2\right], \tag{5}$$

$$C_w=\log_2\left[1+\frac{1}{\sigma_e^2}|(\beta\mathbf{H}_e+\mathbf{G}_e\mathbf{\Phi}\mathbf{H})\mathbf{w}|^2\right]. \tag{6}$$

Note that C_m is achievable at Bob when using the matching receiving vector, i.e., $\mathbf{w}_r=[(\alpha\mathbf{H}_b+\mathbf{G}_r\mathbf{\Phi}\mathbf{H})\mathbf{w}]^{\mathrm{H}}/|(\alpha\mathbf{H}_b+\mathbf{G}_r\mathbf{\Phi}\mathbf{H})\mathbf{w}|$. Similarly, C_w is achievable at Eve via its receiving vector $\mathbf{w}_e=[(\beta\mathbf{H}_e+\mathbf{G}_e\mathbf{\Phi}\mathbf{H})\mathbf{w}]^{\mathrm{H}}/|(\beta\mathbf{H}_e+\mathbf{G}_e\mathbf{\Phi}\mathbf{H})\mathbf{w}|$. However, due to the lack of $\mathbf{H}_e$ and $\mathbf{G}_e$, it is hard to check whether an instantaneous secrecy rate is nonnegative or not. In this case, PLS usually uses secrecy outage probability as the security metric for PLS coding or optimization algorithms. The secrecy outage probability is defined as the probability that the targeted PLS coding rate of Alice's encoder, i.e., R_s, is larger than the secrecy rate C_s. From [21, Eq. (4)], the secrecy outage probability can be expressed as

$$P_{\text{out}}=P(C_s\le R_s\big|\text{Transmission})=P(C_w\ge C_m-R_s). \tag{7}$$

It is obvious that the secrecy outage probability is the conditional probability based on reliable transmissions of main channels, i.e., Bob decodes transmitted codewords correctly with the rate

up to C_m. As we assume that Alice has perfect knowledge about the instantaneous CSI of $\mathbf{H}_b$, $\mathbf{G}_r$, $\mathbf{H}$, and $\mathbf{\Phi}$ within coherence time, Alice can use an adaptive rate of transmitted codewords that equals to C_m.

C. Problem Formulation

In this article, the optimization problem is mathematically expressed as the minimization of the secrecy outage probability via phase shifter matrix and beamforming vector optimization, i.e.,

$$\text{P1:} \min_{\mathbf{\Phi},\mathbf{w}} P_{\text{out}}, \tag{8}$$

$$\text{s.t.} \ |\exp(j\theta_n)|^2 = 1, \quad n = 1, ..., N_s, \tag{9}$$

$$\mathbf{w}^{\text{H}}\mathbf{w} \leq \rho, \tag{10}$$

where P_{out} is the secrecy outage probability, $\mathbf{w}$ is the beamforming vector, and $\mathbf{\Phi}$ is the phase shifter matrix. Eq. (9) corresponds to the unit-modulus requirements of the reflection elements at the IRS. Eq. (10) means the transmission power constraint of beamforming vectors. Obviously, the priority of solving this problem is to find the expression of P_{out}.

IV. Expression of Secrecy Outage Probability

In this paper, we use Gamma distributions to fit the expression of secrecy outage probability.

A. Preliminaries

The gain of wiretap channels of the presented system model is seen as a random variable defined by X, and we derive the CDF of X in Lemma 1 via Gamma distributions. The CDP of X is used to deduce the expression of secrecy outage probability. The Gamma distribution can represent the sum of multiple independent exponentially distributed random variables, so it is suitable for representing the gain of IRS-assisted channels, such as [22]–[24].

Lemma 1. For any $n \times 1$ complex vector $\mathbf{u}$, $\beta \in [0, 1]$, two independent random variables $\mathbf{a} \sim \mathcal{CN}_{m,1}(\mathbf{0}, \mathbf{I}_m)$, and $\mathbf{C} \sim \mathcal{CN}_{m,n}(\mathbf{0}, \mathbf{I}_m \otimes \mathbf{I}_n)$, if we have random variable x as

$$x = |\beta\mathbf{a} + \mathbf{C}\mathbf{u}|^2, \tag{11}$$

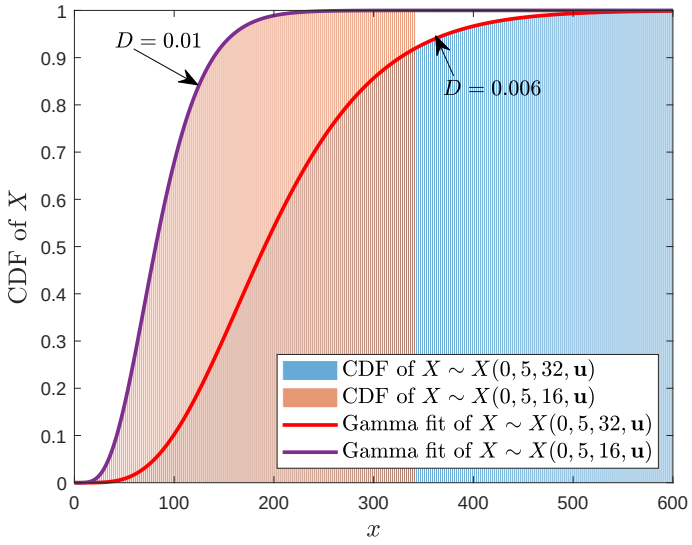


Fig. 2: KS test for Gamma distributions and real distributions of $X \sim X(0.5, 5, 32, \mathbf{u})$ and $X \sim X(0.5, 5, 16, \mathbf{u})$ via 10^5 Monte Carlo simulations, where $\mathbf{u}$ is an arbitrary complex vector as defined in Lemma 1.

the CDF of $X \sim X(\beta, m, n, \mathbf{u})$ can be expressed as

$$F_X(x) = 1 - \frac{1}{\Gamma(m)}\Gamma\left(m, \frac{x}{\beta^2 + |\mathbf{u}|^2}\right), \tag{12}$$

where $\Gamma(x)$ is the Gamma function with respect to x, and $\Gamma(\epsilon, \eta)$ is the upper incomplete Gamma function defined as follows,

$$\Gamma(\epsilon, \eta) = \int_{\eta}^{\infty} \exp(-z) z^{\epsilon - 1} \mathrm{d}z, \tag{13}$$

Proof: See in Appendix A. ■

Then, the KS test is used to examine the fitting goodness between the Gamma distribution and the actual distribution [25], where statistic D is defined as the maximum divergence between fitting and actual CDF,

$$D = \max |F_X(x) - \hat{F}_X(x)|, \tag{14}$$

where $\hat{F}_X(x)$ is the actual CDF of $X \sim X(\beta, m, n, \mathbf{u})$ obtained by Monte Carlo simulations. As shown in Fig. 2, D is with an order of magnitude around 10^{-2}, which means that the Gamma distributions are in a good agreement with the actual distributions.

B. Expression of Secrecy Outage Probability

Here, we use Lemma 1 to deduce the expression of secrecy outage probability.

Theorem 1 (Expression of secrecy outage probability)**.** The secrecy outage probability of R_s, i.e., P_{out}, is expressed as

$$P_{\text{out}} = 1 - F_X(\phi_1) = \frac{1}{\Gamma(N_e)}\Gamma\left(N_e, \frac{\phi_1}{\beta^2 + |\mathbf{\Phi H b}|^2}\right), \tag{15}$$

where $\phi_1 = \sigma_e^2(2^{C_m - R_s} - 1)/P$, C_m is defined in Eq. (5), $F_X(x)$ is defined in Eq. (12), $|(\beta\mathbf{H}_e + \mathbf{G}_e\mathbf{\Phi H})\mathbf{b}|^2 \sim X(\beta, N_e, N_s, \mathbf{\Phi H b})$ represents a random variable, $\mathbf{b} = \mathbf{w}/\sqrt{P}$, and P is the actual transmission power with $P \leq \rho$.

Proof: As channel capacity C_m can be calculated by Eq. (5), with a pre-defined R_s, we can transform P_{out} into

$$P_{\text{out}} = P(C_w > C_m - R_s|\text{Transmission}) = P(|(\beta\mathbf{H}_e + \mathbf{G}_e\mathbf{\Phi H})\mathbf{b}|^2 \geq \phi_1). \tag{16}$$

Since random matrix $\mathbf{H}_e$ is a cyclic symmetry complex Gaussian matrix and fixed $\mathbf{b}$ is an unitary vector, $\mathbf{H}_e\mathbf{b}$ is a cyclic symmetry complex Gaussian vector, i.e., $\mathbf{H}_e\mathbf{b} \sim \mathcal{CN}_{N_e,1}(\mathbf{0}, \mathbf{I}_{N_e})$ [26]. It means that $|(\beta\mathbf{H}_e + \mathbf{G}_e\mathbf{\Phi H})\mathbf{b}|^2$ belongs to $X(\beta, N_e, N_s, \mathbf{u})$ in Lemma 1 where $\mathbf{u} = \mathbf{\Phi H b}$. According to Eq. (12), we get the expression of secrecy outage probability as shown in Eq. (15). ■

Corollary 1 (High SNR case)**.** In the case of $\frac{P}{\sigma_e^2} \to \infty$, the lower bound of secrecy outage probability can be expressed as

$$P_{\text{out}} \geq \frac{1}{\Gamma(N_e)}\Gamma\left(N_e, \frac{\sigma_e^2|(\alpha\mathbf{H}_b + \mathbf{G}_r\mathbf{\Phi H})\mathbf{b}|^2}{\sigma^2 2^{R_s}(\beta^2 + |\mathbf{\Phi H b}|^2)}\right). \tag{17}$$

It means that in high SNR cases, the secrecy outage probability reaches to a constraint, i.e., it decreases with an increasing P at the beginning, but boundlessly increasing the transmission power can not provide the infinite help for reducing secrecy outage probability.

Proof: In the case of $\frac{P}{\sigma_e^2} \to \infty$, ϕ_1 can be re-written as

$$\begin{aligned}
\phi_1 &= \frac{\sigma_e^2(2^{C_m - R_s} - 1)}{P} \\
&= \frac{\sigma_e^2|(\alpha\mathbf{H}_b + \mathbf{G}_r\mathbf{\Phi H})\mathbf{b}|^2}{\sigma^2 2^{R_s}} + \frac{\sigma_e^2}{P}\left(\frac{1}{2^{R_s}} - 1\right) \\
&\leq \frac{\sigma_e^2|(\alpha\mathbf{H}_b + \mathbf{G}_r\mathbf{\Phi H})\mathbf{b}|^2}{\sigma^2 2^{R_s}}.
\end{aligned} \tag{18}$$

Since $N_e > 0$ and $z = \frac{\phi_1}{\beta^2+|\mathbf{\Phi H b}|^2} > 0$, we have

$$\frac{\partial \Gamma(N_e, z)}{\partial z} = -z^{N_e-1}\exp(-z), \tag{19}$$

and it is concluded that P_{out} decreases with an increasing z, ϕ_1, and P. Substituting Eq. (18) into Eq. (15), we can get the the lower bound of secrecy outage probability, as shown in Eq. (17). ■

Corollary 2 (Single-antenna Alice case)**.** For the case of $N_t = 1$, P_{out} can be simplified to

$$P_{\text{SAT}} = 1 - F_X(\phi_2) = \frac{1}{\Gamma(N_e)}\Gamma\left(N_e, \frac{\phi_2}{\beta^2 + |\mathbf{\Phi h}_0|^2}\right), \tag{20}$$

where $\mathbf{h}_0 \sim \mathcal{CN}_{N_s,1}(\mathbf{0}, \mathbf{I}_{N_s})$ is the the channel between single-antenna Alice and IRS, $\phi_2 = \sigma_e^2(2^{C'_m - R_s} - 1)/P$, C'_m is defined as

$$C'_m = \log_2\left(1 + \frac{\rho}{\sigma^2}|\alpha\mathbf{h}_b + \mathbf{G}_r\mathbf{\Phi h}_0|^2\right), \tag{21}$$

$\mathbf{h}_b \sim \mathcal{CN}_{N_r,1}(\mathbf{0}, \mathbf{I}_{N_r})$ is the channel between single-antenna Alice and Bob, $F_X(\phi_2)$ is defined in Eq. (12), $|(\beta\mathbf{h}_e + \mathbf{G}_e\mathbf{\Phi h}_0)|^2 \sim X(\beta, N_e, N_s, \mathbf{\Phi h}_0)$ represents a random variable, and $\mathbf{h}_e \sim \mathcal{CN}_{N_e,1}(\mathbf{0}, \mathbf{I}_{N_e})$ is the channel from single-antenna Alice to Eve.

Proof: In the case of single-antenna Alice, beamforming vector $\mathbf{w}$ is not existed. Replacing $\mathbf{H}_e$ and $\mathbf{H}$ of Theorem 1 with $\mathbf{h}_e$ and $\mathbf{h}_0$, respectively, we can obtain Corollary 2. ■

Corollary 3 (Single-antenna Bob case)**.** The secrecy outage probability of the single-antenna Bob case has the similar form with Eq. (15) via replacing C_m by C''_m, where

$$C''_m = \log_2\left[1 + \frac{P}{\sigma^2}|(\alpha\mathbf{h}_b^{\text{H}} + \mathbf{h}^{\text{H}}\mathbf{\Phi H})\mathbf{b}|^2\right], \tag{22}$$

$\mathbf{h}_b^{\text{H}}$ is the channel vector between Alice and single-antenna Bob obeying $\mathbf{h}_b^{\text{H}} \sim \mathcal{CN}_{1,N_t}(\mathbf{0}, \mathbf{I}_{N_t})$, and the channel from IRS to Bob is defined as $\mathbf{h}^{\text{H}} \sim \mathcal{CN}_{1,N_s}(\mathbf{0}, \mathbf{I}_{N_s})$.

Corollary 4 (Single-antenna Eve case)**.** For the case of $N_e = 1$, P_{out} can be simplified to

$$P_{\text{SAE}}(R_s) = \exp\left(-\frac{\phi_1}{\beta^2 + |\mathbf{\Phi Hb}|^2}\right). \tag{23}$$

Proof: As $\Gamma(1, \mu) = \exp(-\mu)$ and $\Gamma(1) = 1$, we can get the CDF of X as $F_X(\phi_1) = 1 - \exp[-\phi_1/(\beta^2 + |\mathbf{\Phi Hb}|^2)]$ based on Eq. (12), then, P_{out} can be deduced in the single-antenna Eve case as shown in Eq. (23). ■

V. Alternating Optimization For Secrecy Outage Probability Minimization

According to the expression of secrecy outage probability, i.e., Eq. (15), the minimization of secrecy outage probability as shown in P1 is re-formulated as follows,

$$\text{P2: } \min_{\mathbf{\Phi},\mathbf{w}} \frac{1}{\Gamma(N_e)}\Gamma\left(N_e, \frac{\phi_1}{\beta^2+|\mathbf{\Phi}\mathbf{H}\mathbf{b}|^2}\right), \tag{24}$$

$$\text{s.t. } \mathbf{b}=\mathbf{w}/\sqrt{P}, \tag{25}$$

$$\text{Eqs. } (9) \text{ and } (10). \tag{26}$$

According to Corollary 1, it is concluded that P_{out} decreases with increasing $z=\frac{\phi_1}{\beta^2+|\mathbf{\Phi}\mathbf{H}\mathbf{b}|^2}$ and P. Hence, P2 can be transformed equivalently into P3 via using total transmission power, and P3 is expressed as

$$\text{P3: } \max_{\mathbf{\Phi},\mathbf{b}} \frac{\phi_1}{\beta^2+|\mathbf{\Phi}\mathbf{H}\mathbf{b}|^2}, \tag{27}$$

$$\text{s.t. } \mathbf{b}^{\mathrm{H}}\mathbf{b}=1, \quad P=\rho, \quad \text{Eq. } (9). \tag{28}$$

It is obvious that the objective function of P3 is non-convex with variables $\mathbf{\Phi}$ and $\mathbf{b}$. We transform P3 into two subproblems as P4 and P5, i.e., the optimization problems of beamforming vector and phase shifter matrix as follows.

$$\text{P4: } \max_{\mathbf{b}} \frac{\phi_1}{\beta^2+|\mathbf{\Phi}\mathbf{H}\mathbf{b}|^2},$$

$$\text{s.t. } \mathbf{b}^{\mathrm{H}}\mathbf{b}=1, \quad P=\rho. \tag{29}$$

$$\text{P5: } \max_{\mathbf{\Phi}} \frac{\phi_1}{\beta^2+|\mathbf{\Phi}\mathbf{H}\mathbf{b}|^2},$$

$$\text{s.t. Eq. } (9). \tag{30}$$

P4 is optimally solved by a closed-form solution in Section V. A, and this paper provides two optimization algorithms to solve P5, namely, semidefinite relaxation (SDR)-based method and manifold-based method in Section V. B and V. C, respectively. Then, we use an alternating optimization algorithm to find the global results for $\mathbf{\Phi}$ and $\mathbf{b}$ of the original problem P3. It is worth mentioning that the SDR-based method can provide the provable convergence condition for alternating optimization, but it has a higher computational complexity. Oppositely, the manifold-based method requires a lower computational complexity, whereas the convergence condition for the alternating optimization algorithm is not clear. The details of the optimization methods of beamforming vector and phase shifter matrix are presented as follows.

A. Closed-Form Optimal Beamforming Vector

For any given phase shifter matrix $\mathbf{\Phi}$ and $P = \rho$, the objective function of P4 is expressed as follows.

$$\frac{\phi_1}{\beta^2 + |\mathbf{\Phi}\mathbf{H}\mathbf{b}|^2} = c\left(\frac{\mathbf{b}^{\mathrm{H}}\mathbf{A}_1\mathbf{b} + t}{\mathbf{b}^{\mathrm{H}}\mathbf{A}_2\mathbf{b} + \beta^2}\right), \tag{31}$$

where $c = \sigma_e^2/(\sigma^2 2^{R_s})$, $t = \sigma^2(1 - 2^{R_s})/\rho$, $\mathbf{A}_1 = (\alpha\mathbf{H}_b + \mathbf{G}_r\mathbf{\Phi}\mathbf{H})^{\mathrm{H}}(\alpha\mathbf{H}_b + \mathbf{G}_r\mathbf{\Phi}\mathbf{H})$, and $\mathbf{A}_2 = \mathbf{H}^{\mathrm{H}}\mathbf{H}$. According to Eq. (31), P4 with the given $\mathbf{\Phi}$ and $P = \rho$ can be transformed as

$$\begin{aligned} \text{P6: } &\max_{\mathbf{b}} c\left(\frac{\mathbf{b}^{\mathrm{H}}\mathbf{A}_1\mathbf{b} + t}{\mathbf{b}^{\mathrm{H}}\mathbf{A}_2\mathbf{b} + \beta^2}\right), \\ &\text{s.t. } \mathbf{b}^{\mathrm{H}}\mathbf{b} = 1. \end{aligned} \tag{32}$$

We use the generalized Rayleigh quotient to solve P6 [27], where the optimal beamforming vector $\mathbf{b}$ is the generalized eigenvector of the matrix pencil $(\mathbf{A}_1 + t\mathbf{I}_{N_t}, \mathbf{A}_2 + \beta^2\mathbf{I}_{N_t})$, i.e., $(\mathbf{A}_2 + \beta^2\mathbf{I}_{N_t})^{-1}(\mathbf{A}_1 + t\mathbf{I}_{N_t})$. In detail, the optimal $\mathbf{b}$ can be deduced as follows,

$$\mathbf{b}^* = \text{eigvec}_{\lambda_{\max}}[(\mathbf{A}_2 + \beta^2\mathbf{I}_{N_t})^{-1}(\mathbf{A}_1 + t\mathbf{I}_{N_t})], \tag{33}$$

where $\text{eigvec}_{\lambda_{\max}}(\mathbf{X})$ means the corresponding eigenvector of the largest eigenvalue of matrix $\mathbf{X}$, and $\lambda_{\max}$ is the largest eigenvalue of $\mathbf{X}$ [27, Pro 2.1.1]. At last, we have the optimal beamforming vector, i.e., $\mathbf{w}^* = \sqrt{\rho}\mathbf{b}^*$. It can be said that the subproblem P4 is solved optimally.

B. Phase Shifter Matrix Optimization via SDR

Here, we use the SDR technique to solve P5. For any given bemforming vector $\mathbf{b}$ and $P = \rho$, the objective function of P5 is given as follows,

$$\frac{\phi_1}{\beta^2 + |\mathbf{\Phi}\mathbf{H}\mathbf{b}|^2} = c\left[\frac{|(\alpha\mathbf{H}_b + \mathbf{G}_r\mathbf{\Phi}\mathbf{H})\mathbf{b}|^2 + t}{\beta^2 + |\mathbf{\Phi}\mathbf{H}\mathbf{b}|^2}\right], \tag{34}$$

where $c = \sigma_e^2/(\sigma^2 2^{R_s})$ and $t = \sigma^2(1 - 2^{R_s})/\rho$. Ignoring the constant c, the bottom part of Eq. (34) is a fixed value with given β, $\mathbf{b}$, and $\mathbf{H}$, which is expressed as

$$\beta^2 + |\mathbf{\Phi}\mathbf{H}\mathbf{b}|^2 = \beta^2 + \mathbf{b}^{\mathrm{H}}\mathbf{H}^{\mathrm{H}}\mathbf{\Phi}^{\mathrm{H}}\mathbf{\Phi}\mathbf{H}\mathbf{b} = \beta^2 + \mathbf{b}^{\mathrm{H}}\mathbf{H}^{\mathrm{H}}\mathbf{H}\mathbf{b}. \tag{35}$$

To address the top part of Eq. (34), $\mathbf{G}_r\mathbf{\Phi}\mathbf{H}\mathbf{b}$ is re-formulated as [3]

$$\mathbf{G}_r\mathbf{\Phi}\mathbf{H}\mathbf{b} = \mathbf{G}_r\text{diag}(\mathbf{H}\mathbf{b})\mathbf{q} = \mathbf{\Sigma}\mathbf{q}, \tag{36}$$

where $\mathbf{q} = \text{vec}(\mathbf{\Phi}) = [\exp(j\theta_1), ..., \exp(j\theta_{N_s})]^{\text{T}}$. By using Eq. (36), the top part of Eq. (34) can be transformed as follows,

$$\begin{aligned}
&|(\alpha\mathbf{H}_b + \mathbf{G}_r\mathbf{\Phi}\mathbf{H})\mathbf{b}|^2 + t \\
&= \mathbf{q}^{\text{H}}\mathbf{\Sigma}^{\text{H}}\mathbf{\Sigma}\mathbf{q} + \alpha^2|\mathbf{H}_b\mathbf{b}|^2 + \alpha\mathbf{b}^{\text{H}}\mathbf{H}_b^{\text{H}}\mathbf{\Sigma}\mathbf{q} + \alpha\mathbf{q}^{\text{H}}\mathbf{\Sigma}^{\text{H}}\mathbf{H}_b\mathbf{b} + t \\
&= \hat{\mathbf{q}}^{\text{H}}\mathbf{W}\hat{\mathbf{q}} + \alpha^2|\mathbf{H}_b\mathbf{b}|^2 + t, \qquad (37)
\end{aligned}$$

where

$$\mathbf{W} = \begin{bmatrix} \mathbf{\Sigma}^{\text{H}}\mathbf{\Sigma} & \alpha\mathbf{\Sigma}^{\text{H}}\mathbf{H}_b\mathbf{b} \\ \alpha\mathbf{b}^{\text{H}}\mathbf{H}_b^{\text{H}}\mathbf{\Sigma} & 0 \end{bmatrix}, \ \hat{\mathbf{q}}^{\text{H}} = \begin{bmatrix} \mathbf{q}^{\text{H}}, & l \end{bmatrix}, \qquad (38)$$

and l is an auxiliary variable. According to Eqs. (35) and (37), P5 with given $\mathbf{b}$ and $P = \rho$ can be transformed as

$$\text{P7:} \ \max_{\hat{\mathbf{q}}^{\text{H}}} \hat{\mathbf{q}}^{\text{H}}\mathbf{W}\hat{\mathbf{q}} + \alpha^2|\mathbf{H}_b\mathbf{b}|^2 + t, \qquad (39)$$

$$\text{s.t.} \ |\hat{q}_i|^2 = 1, i = 1, ..., N_s + 1, \qquad (40)$$

where $\hat{q}_i$ is the ith element in $\hat{\mathbf{q}}$. Obviously, P7 is a Boolean quadratic program belonging to the NP-hard problem [28]. To address P7, we use the method in [9] that introduces $N_s + 1$ auxiliary matrices $\mathbf{E}_n, n = 1, ..., N_s + 1$ as follows,

$$[\mathbf{E}_n]_{i,j} = \begin{cases} 1, & i = j = n, \\ 0, & \text{otherwise}, \end{cases} \qquad (41)$$

where $[\mathbf{E}_n]_{i,j}$ is the (i, j)th element of $\mathbf{E}_n$. With $\mathbf{E}_n, \forall n$, the constraint (40) can be transformed as $\hat{\mathbf{q}}^{\text{H}}\mathbf{E}_n\hat{\mathbf{q}} = 1, \forall n$. Then, P7 can be transformed equivalently as

$$\text{P8:} \ \max_{\mathbf{Q}} \text{tr}(\mathbf{W}\mathbf{Q}) + \alpha^2|\mathbf{H}_b\mathbf{b}|^2 + t, \qquad (42)$$

$$\text{s.t.} \ \text{tr}(\mathbf{E}_n\mathbf{Q}) = 1, \forall n, \qquad (43)$$

$$\text{rank}(\mathbf{Q}) = 1, \mathbf{Q} \succeq \mathbf{0}, \qquad (44)$$

where $\mathbf{Q} = \hat{\mathbf{q}}\hat{\mathbf{q}}^{\text{H}}$. Obviously, the objective function and constraints in P8 are convex except that $\text{rank}(\mathbf{Q}) = 1$ is a non-convex constraint, thus, we use SDR technique to drop this rank-one constraint to get a convex problem, i.e., P8 without the rank-one constraint can be optimally solved by convex optimization solvers, such as interior point methods or the MATLAB CVX

tool, resulting optimal $\mathbf{Q}$, i.e., $\mathbf{Q}^*$. However, there is no guarantee that $\mathbf{Q}^*$ is the desired rank-one solution, so the Gaussian randomization method or maximum eigenvalue method is used to obtain the near-optimal $\hat{\mathbf{q}}$, as well as the near-optimal $\mathbf{\Phi}$ [28]. To reduce the computational cost, we chose the maximum eigenvalue method because P8 usually yields rank-one solutions (higher than 99% of the tested cases in the investigation [29]). In detail, we apply the eigenvalue decomposition on $\mathbf{Q}^*$ to get $\mathbf{Q}^* = \sum_{i=1}^{N_s+1} \lambda_i \bar{\mathbf{q}}_i \bar{\mathbf{q}}_i^{\mathrm{H}}$. Then, the near-optimal $\hat{\mathbf{q}} = \bar{\mathbf{q}}_1$, i.e., the eigenvector of the largest eigenvalue λ_1 of $\mathbf{Q}^*$. At last, we get the near-optimal $\mathbf{\Phi} = \mathrm{diag}(\mathbf{q}_1)$ where $\mathbf{q}_1$ is $\bar{\mathbf{q}}_1$ removing the last element.

If using SDR-based approach for the $\mathbf{\Phi}$ generation, the number of variables $\mathbf{Q}$ of P8 is $N_s + 1$, and P8 has one linear matrix inequality (LMI) constraint with size of $N_s + 1$. In this case, the iterations of the interior-point method is $\ln(1/\epsilon)[2(N_s+1)^{4.5} + (N_s+1)^{3.5}]$, where ϵ is the accuracy requirement of the interior-point method [28], [29]. In addition, the maximum eigenvalue method requires $(N_s+1)^3 + N_s$ iterations. In this case, the number of iterations in the SDR-based approach is $\ln(1/\epsilon)[2(N_s+1)^{4.5} + (N_s+1)^{3.5}] + (N_s+1)^3 + N_s$.

C. Phase Shifter Matrix Optimization via Manifolds

Here, we provide another optimization algorithm for phase shifter matrix based on manifold optimization [30], which can handle the unit modulus constraint with lower computational complexity. At first, according to Eq. (37), the minus of the objective function in P5 can be expressed as a function with respect to $\mathbf{q}$, i.e.,

$$\begin{aligned} f(\mathbf{q}) &= \frac{-\phi_1}{\beta^2 + |\mathbf{\Phi}\mathbf{H}\mathbf{b}|^2} \\ &= -k(\mathbf{q}^{\mathrm{H}}\mathbf{\Sigma}^{\mathrm{H}}\mathbf{\Sigma}\mathbf{q} + \alpha^2|\mathbf{H}_b\mathbf{b}|^2 + \alpha\mathbf{b}^{\mathrm{H}}\mathbf{H}_b^{\mathrm{H}}\mathbf{\Sigma}\mathbf{q} + \alpha\mathbf{q}^{\mathrm{H}}\mathbf{\Sigma}^{\mathrm{H}}\mathbf{H}_b\mathbf{b} + t), \end{aligned} \tag{45}$$

where $k = c/(\beta^2 + \mathbf{b}^{\mathrm{H}}\mathbf{H}^{\mathrm{H}}\mathbf{H}\mathbf{b})$ due to Eqs. (34) and (35). Then, the constraint (9) is defined a complex circle manifold as

$$\mathcal{O} = \left\{\mathbf{q} \in \mathbb{C}^{N_s} \middle| |q_i|^2 = 1, i = 1, ..., N_s\right\}. \tag{46}$$

It is obvious that Eq. (46) is equivalent to constraint (9), and the optimal point, i.e., $\mathbf{q}^*$ is on the complex circle manifold $\mathcal{O}$. In this case, P5 with the given $\mathbf{\Phi}$ and $P = \rho$ can be equivalently transformed as

$$\text{P9: } \min_{\mathbf{q}\in\mathcal{O}} f(\mathbf{q}). \tag{47}$$

P9 can be solved by manifold optimization. Similar to traditional optimization methods, manifold optimization is also based on the gradient descent criterion, called the Riemannian gradient descent. However, the gradient of a point of the manifold is decided jointly by the Euclidean gradient and the tangent space on manifold $\mathcal{O}$ at this point. For instance, the tangent space for $\mathcal{O}$ at the point of the jth iteration, i.e., $\mathbf{q}_j \in \mathcal{O}$, is expressed as

$$T_{\mathbf{q}_j}\mathcal{O} = \left\{\mathbf{v} \in \mathbb{C}^{N_s} \middle| \mathbf{q}_j^{\mathrm{H}}\mathbf{v} = 0\right\}, \tag{48}$$

where $\mathbf{v}$ is the tangent vector at $\mathbf{q}_j$. Among all tangent vectors on $T_{\mathbf{q}_j}\mathcal{O}$, the one that yields the fastest increase of the objective function is defined as the Riemannian gradient [31], i.e., $\mathrm{grad}_{\mathbf{q}_j} f(\mathbf{q})$, where $f(\mathbf{q})$ is the objective function with respect to $\mathbf{q}$ as defined in Eq. (45). $\mathrm{grad}_{\mathbf{q}_j} f(\mathbf{q})$ is the projection from the Euclidean gradient, i.e.,

$$\nabla_{\mathbf{q}_j} f(\mathbf{q}) = -2k\boldsymbol{\Sigma}^{\mathrm{H}}\boldsymbol{\Sigma}\mathbf{q}_j - 2k\alpha\boldsymbol{\Sigma}^{\mathrm{H}}\mathbf{H}_b\mathbf{b}, \tag{49}$$

to the tangent space $\mathcal{O}$ as

$$\mathrm{grad}_{\mathbf{q}_j} f(\mathbf{q}) = \nabla_{\mathbf{q}_j} f(\mathbf{q}) - \Re(\nabla_{\mathbf{q}_j} f(\mathbf{q}) \circ \mathbf{q}_j^{\dagger}) \circ \mathbf{q}_j, \tag{50}$$

where $\circ$ is the Hadamard product, $\Re(\cdot)$ means the real part of a complex variable, and $(\cdot)^{\dagger}$ is the conjugate operation. The next point $\mathbf{q}_{j+1}$ should be with the direction of $\eta_j\mathbf{p}_j$ where η_j is the step size and $\mathbf{p}_i$ is the search direction vector. The initial direction $\mathbf{p}_0$ is $\mathrm{grad}_{\mathbf{q}_0} f(\mathbf{q})$ assuming that $\mathbf{q}_0$ is the beginning point. However, the movement can not guarantee that point $\mathbf{q}_{j+1}$ is on manifold $\mathcal{O}$. Hence, we introduce the retraction function to map a vector on $T_{\mathbf{q}_j}\mathcal{O}$ onto manifold $\mathcal{O}$, which is given as

$$\mathbf{q}_{j+1} = \mathrm{R}_{\mathbf{q}_j}(\eta_j\mathbf{p}_j), \tag{51}$$

where a typical retraction is the normalization function, i.e., $\mathrm{R}_{\mathbf{x}}(\mathbf{y}) = \frac{y_i}{|y_i|}, \forall i$. Based on the Riemannian gradient and retraction function, we use the conjugate-gradient descent method to find the optimal phase shifter matrix, which is shown in Algorithm 1. In conjugate-gradient descent algorithm, the update rule for the search direction on manifolds is given by

$$\mathbf{p}_{j+1} = -\mathrm{grad}_{\mathbf{q}_{j+1}} f(\mathbf{q}) + \varphi_j \mathcal{T}_{\mathbf{q}_j \to \mathbf{q}_{j+1}}(\mathbf{p}_j), \tag{52}$$

where $\mathcal{T}_{\mathbf{q}_j \to \mathbf{q}_{j+1}}(\mathbf{p}_j)$ is the mapping function of the tangent vector $\mathbf{p}_j$ from the tangent space $T_{\mathbf{q}_j}\mathcal{O}$ to the tangent space $T_{\mathbf{q}_{j+1}}\mathcal{O}$. The mapping function is given as

$$\mathcal{T}_{\mathbf{q}_j \to \mathbf{q}_{j+1}}(\mathbf{p}_j) = \mathbf{p}_j - \Re(\mathbf{p}_j \circ \mathbf{q}_{j+1}^{\dagger}) \circ \mathbf{q}_{j+1}. \tag{53}$$

Since the second derivative of $f(\mathbf{q})$, i.e., $\nabla^2_{\mathbf{q}} f(\mathbf{q}) = -k\boldsymbol{\Sigma}^{\mathrm{H}}\boldsymbol{\Sigma}$ and $\boldsymbol{\Sigma}^{\mathrm{H}}\boldsymbol{\Sigma}$ is positive semidefinite, so $f(\mathbf{q})$ is concave, such that Algorithm 1 based on conjugate-gradient descent can not be guaranteed to converge to the optimal point [30]. Hence, the output $\boldsymbol{\Phi}^*$ in Algorithm 1 is the local optimal result.

Algorithm 1: Conjugate-gradient Descent Algorithm for Phase Shifter Matrix based on Manifold.

Data: $\alpha, \beta, \rho, R_s, \sigma^2, \sigma_e^2, \mathbf{b}, \mathbf{H}_b, \mathbf{G}_r, \mathbf{H}, N_s$

Result: $\boldsymbol{\Phi}^*$

1 Initialize η_0 and φ_0;
2 Select beginning point $\mathbf{q}_0$, calculate $\mathrm{grad}_{\mathbf{q}_0} f(\mathbf{q})$;
3 **while** $|\mathrm{grad}_{\mathbf{q}_j} \mathrm{f}(\mathbf{q})| \leq \xi$ **do**
4 Calculate Riemannian gradient $\mathrm{grad}_{\mathbf{q}_j} f(\mathbf{q})$ via Eq. (50);
5 Compute conjugate search direction $\mathbf{p}_j$ via Eq. (52);
6 Find next point $\mathbf{q}_{j+1}$ via Eq. (51) ;
7 Determine step size η_j and φ_j proposed in [27] ;
8 Get $\mathbf{q}^* = \mathbf{q}_j$;
9 $\boldsymbol{\Phi}^* = \mathrm{diag}(\mathbf{q}^*)$;
10 **Procedure End**

The computational complexity analysis of Algorithm 1 is discussed here. The conjugate-gradient descent algorithm needs N_s^2 iterations for convergence [32], and each iteration needs the calculation of Eqs. (50), (51), (52), and a step size update, i.e., the steps 4-7. The steps 4, 5, 6, and 7 require $4N_s^2 + 2N_s$, $2N_s$, N_s, and $4N_s^2$ inner-iterations, respectively. In the step 9, $\boldsymbol{\Phi}^*$ generation needs N_s iterations. In this case, the number of iterations of Algorithm 1 is $8N_s^4 + 5N_s^3 + N_s$.

D. Alternating Optimization

The SDR-based or manifold-based optimization method is used to find the optimal phase shifter matrix with given beamforming vectors, and Eq. (33) provides the optimal beamforming vector for given phase shifter matrices. Here, we design an alternating optimization algorithm for the global results of the phase shifter matrix and beamforming vector, as shown in Algorithm 2. The alternating optimization algorithm is an iterative procedure for the global optimization over $\boldsymbol{\Phi}$ and $\mathbf{b}$ by alternating restricted optimization over individual $\boldsymbol{\Phi}$ and $\mathbf{b}$. It provides global

results that can converge with limited iterations [33]. The following theorem is used to show the convergence condition.

Algorithm 2: Alternating Optimization Algorithm for Phase Shifter Matrix and Beamforming Vector.

Data: $\alpha, \beta, \rho, R_s, \sigma^2, \sigma_e^2, \mathbf{H}_b, \mathbf{G}_r, \mathbf{H}, N_t, N_s, N_e$

Result: $\mathbf{\Phi}_o^*, \mathbf{w}_o^*$

1 Initialize $\mathrm{iter} = 1$ and the iterating limit is $\mathrm{iter}_{\max}$;

2 Initialize beamforming vector $\mathbf{b}_0 = \text{random\_unitary}(N_t, 1)$;

3 **while** $\mathrm{iter} \leq \mathrm{iter}_{\max} \&\& \{\mathrm{P}_{\mathrm{out}}(\Omega_{\mathrm{iter}+1}) - \mathrm{P}_{\mathrm{out}}(\Omega_{\mathrm{iter}}) \leq \xi\}$ **do**

4 Solve P8 via interior point method to obtain $\mathbf{Q}_{\mathrm{iter}}$;

5 Get $\hat{\mathbf{q}}_{\mathrm{iter}}$ via maximum eigenvalue method of $\mathbf{Q}_{\mathrm{iter}}$;

6 Get $\mathbf{q}_{\mathrm{iter}}$ via removing the last element of $\hat{\mathbf{q}}_{\mathrm{iter}}$ and calculate $\mathbf{\Phi}_{\mathrm{iter}} = \mathrm{diag}(\mathbf{q}_{\mathrm{iter}})$;

7 Calculate $P_{\text{out}}(\mathbf{\Omega}_{\mathrm{iter}})$ via Eq. (15);

8 Solve P4 via Eq. (33) to obtain $\mathbf{b}_{\mathrm{iter}+1}$;

9 $\mathbf{\Phi}_o^* = \mathbf{\Phi}_{\mathrm{iter}}, \mathbf{w}_o^* = \sqrt{\rho}\mathbf{b}_{\mathrm{iter}}$;

10 **Procedure End**

Theorem 2 (Convergence condition)**.** For given convex problems, i.e., P6 and P8 removing the rank-one constraint, there exists a global convergence point $\mathbf{\Omega}_{\mathrm{iter}} = (\mathbf{b}_{\mathrm{iter}}^*, \mathbf{Q}_{\mathrm{iter}}^*)$ that is the output of the iterth iteration, resulting that $P_{\text{out}}(\mathbf{\Omega}_{\mathrm{iter}})$ is equal to $P_{\text{out}}(\mathbf{\Omega}_{\mathrm{iter}+1})$, i.e., the secrecy outage probability P_{out} approaches to a constant, where $P_{\text{out}}(\mathbf{\Omega})$ is the secrecy outage probability function with parameters $\mathbf{\Omega} = (\mathbf{b}^*, \mathbf{Q}^*)$ that is calculated by steps 4-8 in Algorithm 2.

Proof: See [33, Th. 3]. In brief, if all sub-problems of the original problem are convex, there exists a global convergence point that can be found within the finite number of alternations. ■

The global convergence point $\mathbf{\Omega}_{\mathrm{iter}}$ is the output of the alternating algorithm, where $\mathbf{\Phi}_o^* = \mathbf{\Phi}_{\mathrm{iter}}, \mathbf{w}_o^* = \sqrt{\rho}\mathbf{b}_{\mathrm{iter}}$ are seen as the desired results of global optimization. According to the convergence condition in Theorem 2, we set an arbitrarily small value ξ, where the iteration process continues until $\{P_{\text{out}}(\mathbf{\Omega}_{\mathrm{iter}+1}) - P_{\text{out}}(\mathbf{\Omega}_{\mathrm{iter}}) \leq \xi\}$. To avoid the endless loop, we set $\mathrm{iter}_{\max}$ in Algorithm 2 as the maximum number of allowed loops. random_unitary$(N_t, 1)$ is to generate an $N_t \times 1$ unitary vector randomly in this algorithm.

It is worth noting that the manifold-based method can not provide a provable global-optimal phase shifter matrix. Hence, alternating optimization algorithm between P4 and P9 is not guaranteed to be convergent. Although the alternating optimization between P4 and P9 can be performed

via replacing $\mathbf{\Omega}_{\rm iter} = (\mathbf{b}^*_{\rm iter}, \mathbf{Q}^*_{\rm iter})$ with $\mathbf{\Omega}_{\rm iter} = (\mathbf{b}^*_{\rm iter}, \mathbf{\Phi}^*_{\rm iter})$ in Algorithm 2, the convergence performance should be examined by simulations in Section VII.

E. Computational Complexity Analysis

The computational complexity analysis of Algorithm 2 is discussed as follows. The steps 4, 5, and 6 need totally $\ln(1/\epsilon)[2(N_s+1)^{4.5}+(N_s+1)^{3.5}]+(N_s+1)^3+N_s$ iterations. According the Eq. (15), we know that the step 7 requires $N_s^2N_t+N_sN_t$ iterations. According the Eq. (33), we know that the step 8 requires $3N_t^3+2N_t^2$ iterations. In total, the computational complexity of Algorithm 2 in the worst condition is on the order of $O\{\text{iter}_{\max}[\ln(1/\epsilon)N_s^{4.5}+N_t^3+N_s^2N_t]\}$ where $\text{iter}_{\max}$ is the maximum number of allowed loops. If Algorithm 2 uses the manifold-based approach for the $\mathbf{\Phi}_{\rm iter}$ generation, the computational complexity is $O[\text{iter}_{\max}(N_s^4+N_t^3+N_s^2N_t)]$. It is concluded that the alternating optimization with manifold optimization has less computational complexity than that with the SDR approach.

VI. Lower Computational Complexity Algorithms For Single-Antenna Cases

In the single-antenna cases, we present beamforming and phase shifter matrix optimization algorithms that have lower computational complexity.

A. Single-Antenna Alice

Corollary 2 provides the expression of secrecy outage probability when Alice has one antenna. According to Eq. (20) in Corollary 2 and the monotonicity of the secrecy outage probability function, the minimization of secrecy outage probability, i.e., P2, can be expressed as

$$\text{P10: } \max_{\mathbf{\Phi}} \frac{\phi_2}{\beta^2+|\mathbf{\Phi}\mathbf{h}_0|^2}, \qquad \text{s.t. Eq. (9)}, \tag{54}$$

where $\phi_2 = \sigma_e^2(2^{C'_m-R_s}-1)/P$. The minus of the objective function in P10 can be transformed as a function with respect to $\mathbf{q}$, i.e.,

$$\begin{aligned} f_0(\mathbf{q}) = \frac{-\phi_2}{\beta^2+|\mathbf{\Phi}\mathbf{h}_0|^2} &= -k[|\alpha\mathbf{h}_b+\mathbf{G}_r\mathbf{\Phi}\mathbf{h}_0|^2+t] \\ &= -k(\mathbf{q}^{\rm H}\mathbf{\Sigma}_0^{\rm H}\mathbf{\Sigma}_0\mathbf{q}+\alpha^2|\mathbf{h}_b|^2+\alpha\mathbf{h}_b^{\rm H}\mathbf{\Sigma}_0\mathbf{q}+\alpha\mathbf{q}^{\rm H}\mathbf{\Sigma}_0^{\rm H}\mathbf{h}_b+t), \end{aligned} \tag{55}$$

where $\mathbf{\Sigma}_0 = \mathbf{G}_r\text{diag}(\mathbf{h}_0)$, $k = c/(\beta^2+|\mathbf{h}_0|^2)$, $c = \sigma_e^2/(\sigma^2 2^{R_s})$, and $t = \sigma^2(1-2^{R_s})/\rho$. With Eq. (55), P10 can be transformed as a problem of manifold optimization, i.e.,

$$\text{P11: } \min_{\mathbf{q}\in\mathcal{O}} f_0(\mathbf{q}), \tag{56}$$

where $\mathbf{q}$ is defined as a complex circle manifold as shown in Eq. (46). Refer to the multiple-antenna case, this paper also uses the conjugate-gradient descent algorithm to solve P11, whose procedure is similar with Algorithm 1, so we will not repeat it. Note that the beamforming optimization is not available in the single-antenna Alice case, thus alternating optimization is not required, and the computational complexity is reduced significantly. The computational complexity to solve P11 with the conjugate-gradient descent algorithm is on the order of $O(N_s^4)$.

B. Single-Antenna Bob

When Bob has one antenna, with given beamforming vector $\mathbf{b}$ and $P = \rho$, the minimization of secrecy outage probability, i.e., P2, can be expressed as

$$\text{P12: } \max_{\mathbf{\Phi}} \frac{\phi_1}{\beta^2 + |\mathbf{\Phi H b}|^2}, \qquad \text{s.t.} \quad \text{Eq. } (9), \tag{57}$$

where $\phi_1 = \sigma_e^2(2^{C_m''-R_s} - 1)/\rho$ and C_m'' is defined in Eq. (22). The objective function of P12 can be transformed as follows,

$$\frac{\phi_1}{\beta^2 + |\mathbf{\Phi H b}|^2} = k[|(\alpha \mathbf{h}_b^{\mathrm{H}} + \mathbf{h}^{\mathrm{H}}\mathbf{\Phi H})\mathbf{b}|^2 + t]. \tag{58}$$

With Eq. (58), P12 can be transformed as

$$\text{P13: } \max_{\mathbf{\Phi}} |(\alpha \mathbf{h}_b^{\mathrm{H}} + \mathbf{h}^{\mathrm{H}}\mathbf{\Phi H})\mathbf{b}|^2, \qquad \text{s.t.} \quad \text{Eq. } (9). \tag{59}$$

We use the method in [3] to find the closed-form solution for the optimal phase shifter matrix $\mathbf{\Phi}$. At first, we have the following inequality:

$$|(\alpha \mathbf{h}_b^{\mathrm{H}} + \mathbf{h}^{\mathrm{H}}\mathbf{\Phi H})\mathbf{b}| \leq |\alpha \mathbf{h}_b^{\mathrm{H}}\mathbf{b}| + |\mathbf{h}^{\mathrm{H}}\mathbf{\Phi H b}|. \tag{60}$$

The equation holds if and only if $\arg(\mathbf{h}_b^{\mathrm{H}}\mathbf{b}) = \arg(\mathbf{h}^{\mathrm{H}}\mathbf{\Phi H b}) = \arg[\mathbf{q}^{\mathrm{H}}\mathrm{diag}(\mathbf{h}^{\mathrm{H}})\mathbf{m}] = \theta_0$, where $\mathbf{m} = \mathbf{H b}$ and $\arg(x)$ is the angle of the complex number x. Thus, with a fixed $\mathbf{b}$ and θ_0, the nth phase shifter at the IRS has the closed-form solution, i.e.,

$$\theta_n^* = \theta_0 - \arg(h_n^{\mathrm{H}}) - \arg(m_n), i = 1, ..., N_s, \tag{61}$$

where h_n^{H} and m_n are the nth elements of $\mathbf{h}^{\mathrm{H}}$ and $\mathbf{m}$, respectively. According to Eq. (61), we have $\mathbf{\Phi}^* = \mathrm{diag}[\exp(j\theta_1^*), ..., \exp(j\theta_{N_s}^*)]$. If $\mathbf{\Phi}$ is fixed, we can get the optimal beamforming vector $\mathbf{b}^*$ via Eq. (33) replacing $\mathbf{A}_1$ with $\mathbf{A}_3$, where $\mathbf{A}_3 = (\alpha \mathbf{h}_b^{\mathrm{H}} + \mathbf{h}^{\mathrm{H}}\mathbf{\Phi H})^{\mathrm{H}}(\alpha \mathbf{h}_b^{\mathrm{H}} + \mathbf{h}^{\mathrm{H}}\mathbf{\Phi H})$. Note that both $\mathbf{b}^*$ and $\mathbf{\Phi}^*$ have the closed-form solution, so the alternating optimization between beamforming and phase shifter matrix in the single-antenna Bob case has lower computational

complexity compared to the multiple-antenna case. In detail, Eq. (61) requires $N_s N_t + N_s$ iterations and the calculation of θ_0 requires N_t iterations, so the computational complexity of alternating optimization in the single-antenna Bob case is on the order of $O[\text{iter}_{\max}(N_t^3 + N_s^2 N_t)]$.

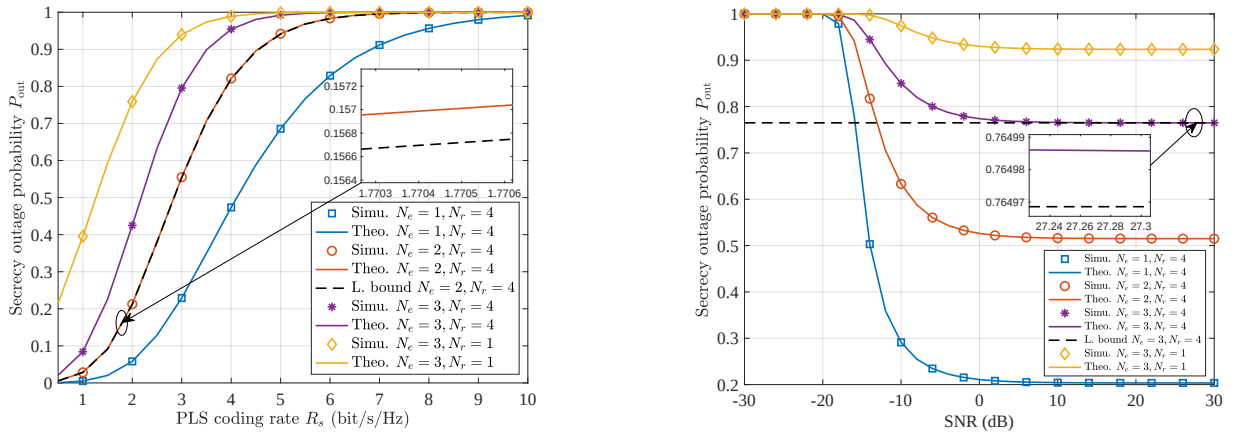
VII. Simulations

The simulation results are provided to investigate joint impacts of SNR, PLS coding rate, the number of antennas, and the number of IRS elements on the secrecy outage probability of the proposed schemes. Here, the AWGN floor parameters σ^2 and σ_e^2 are calculated by $174 + 10\log 2(W) + 10$ dBm, where W is the carrier bandwidth and selected as 20 MHz. The path loss can be uniformly calculated by $\frac{c}{\sqrt{d_i}}, i = \{1, 2\}$, where c is the path loss constant, d_1 and d_2 are the distances between Alice to Bob and Eve, respectively.

A. Numerical Test for Secrecy Outage Probability

Here, we examine Theorem 1 in terms of PLS coding rate and SNR in Figs. 3a and 3b, respectively. These figures show the good agreements between theoretical results (Theo.) and Monte Carlo simulation results (Simu.) from 10^5 independent runs. The simulation adopts the parameters as $N_s = 16$, $N_t = 10$, $\mathbf{\Phi}$ is arbitrary, and $\mathbf{w}$ is the MRT vector of main channels, i.e., $\mathbf{w} = \sqrt{\rho}(\alpha \mathbf{h}_b^{\mathrm{H}} + \mathbf{h}^{\mathrm{H}} \mathbf{\Phi} \mathbf{H})^{\mathrm{H}} / |\alpha \mathbf{h}_b^{\mathrm{H}} + \mathbf{h}^{\mathrm{H}} \mathbf{\Phi} \mathbf{H}|$ in the single-antenna Bob case, and $\mathbf{w}/\sqrt{\rho} = \text{eigvec}_{\lambda_{\max}}[(\alpha \mathbf{H}_b + \mathbf{G}_r \mathbf{\Phi} \mathbf{H})^{\mathrm{H}} (\alpha \mathbf{H}_b + \mathbf{G}_r \mathbf{\Phi} \mathbf{H})]$ in the multiple-antenna Bob case [19], where $\text{eigvec}_{\lambda_{\max}}(\mathbf{X})$ means the corresponding eigenvector of the largest eigenvalue of matrix $\mathbf{X}$, and $\lambda_{\max}$ is the largest eigenvalue of $\mathbf{X}$.

From Fig. 3a, we can find that the secrecy outage probability increases with an increasing PLS coding rate. It is also shown that the increasing number of Eve's antennas enlarges the secrecy outage probability, and adding Bob's antennas can reduce secrecy outage probability, which are consistent with the conclusions [21]. Without loss of generality, the simulations of $\{N_e = 2, N_r = 4\}$ are selected for the tight test between the theoretical results of secrecy outage probability and their lower bound. It is demonstrated that the lower bound from Corollary 1 is very tight for secrecy outage probability. In Fig. 3b, we can find that the secrecy outage probability decreases fast with an increasing SNR at lower SNR regions, then decreases slow and has a nearly constant in higher SNR regions, which is consistent with the conclusion in Corollary 1 of this paper. The simulations of $\{N_e = 3, N_r = 4\}$ are selected for the tight test and shows the lower bound is tightness. Throughout Figs. 3a and 3b, we find the secrecy outage



(a) PLS coding rate effect when SNR is 9 dB.

(b) SNR effect when PLS coding rate is 3 bit/s/Hz

Fig. 3: Theoretical results and Monte Carlo simulations of secrecy outage probability, where $N_s = 16$, $N_t = 10$, $\alpha = \beta = 0.8$, $\mathbf{\Phi}$ is randomly generated, and $\mathbf{w}$ is the MRT vector.

probability with arbitrary phase shifter matrices is very large when the PLS coding rate is larger than 1 bit/s/Hz, meaning that the optimization of the phase shifter matrix is necessary.

B. Single-Antenna Alice

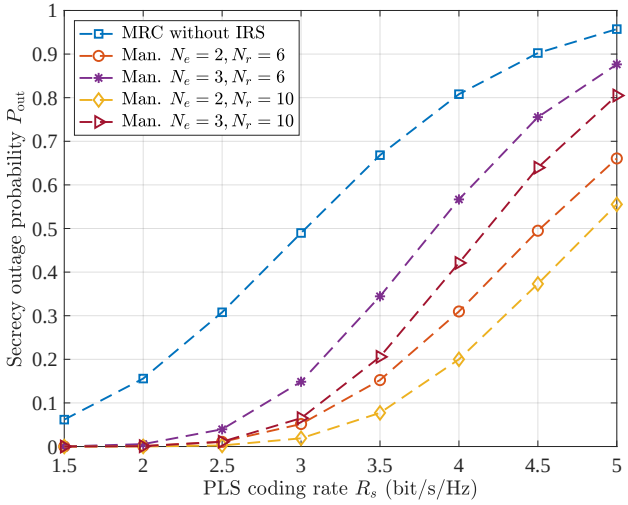


Fig. 4: Secrecy outage probability in the IRS-assisted SIMOME case, where $N_t = 10$, $N_s = 32$, $\alpha = \beta = 0.8$, and SNR is 9 dB.

The secrecy outage probability in the case of single-antenna Alice, also called IRS-assisted single-input multiple-output multiple-antenna-eavesdropper (SIMOME) case, is examined in Fig.

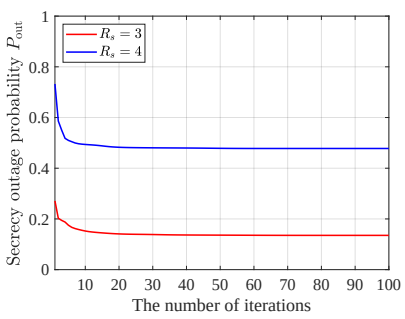
4. The comparison simulation is conducted between the proposed scheme in Section VI. A and the maximal-ratio combining (MRC) technology without IRS. The MRC vector is $\mathbf{h}_b^{\mathrm{H}}/|\mathbf{h}_b|$. We can find that an increasing PLS coding rate will enlarge the secrecy outage probability, and the proposed manifold (Man.) method has a lower secrecy outage probability compared to the MRC method. In addition, the increasing number of Eve's antennas causes a large secrecy outage probability due to the wiretap channel capacity increases with the number of Eve's antennas. It is also demonstrated that adding Bob's antennas will reduce secrecy outage probability.

C. Single-Antenna Bob

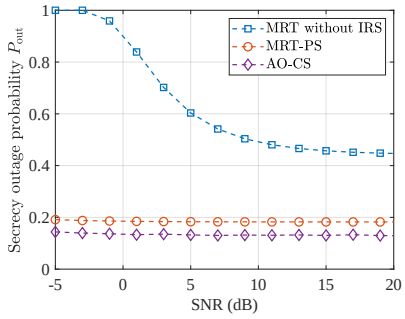
In single-antenna Bob case, three different schemes, i.e., MRT-based beamforming without IRS (MRT without IRS), joint MRT-based beamforming and phase shift optimization (MRT-PS), and the proposed alternating optimization (AO) scheme based on closed-form solutions (AO-CS), are compared, which are described detailedly as follows.

1) MRT without IRS: Alice performs MRT-based beamforming, i.e., $\mathbf{w} = \sqrt{\rho}\mathbf{h}_b^{\mathrm{H}}/|\mathbf{h}_b|$ where $\mathbf{h}_b^{\mathrm{H}}$ represent the channel between Alice and Bob in the scenarios without IRS, and phase shift control is not considered in this case. The secrecy outage probability of MRT-based beamforming is calculated as $P_{\text{out,MRT}}(R_s) = \Gamma(N_e, \phi_m)/\Gamma(N_e)$, where $\phi_m = \sigma_e^2(2^{C_m - R_s} - 1)/\rho$ and $C_m = \log_2(1 + \rho/\sigma^2|\alpha\mathbf{h}_b^{\mathrm{H}}|^2)$. The computational complexity of MRT-based beamforming is $O(N_b)$.
2) MRT-PS: Alice performs joint MRT-based beamforming and SDR-based or manifold-based phase shifter optimization scheme as proposed in [3], [8], [11], [34], which achieves an optimal channel capacity without the instantaneous CSIs of eavesdroppers. The secrecy outage probability of this scheme can be measured by Eq. (15). The computational complexity of MRT-PS is $O(N_s^4 + N_sN_t + N_t)$ (using manifold optimization) or $O[\ln(1/\epsilon)(N_s^{4.5} + N_sN_t + N_t)]$ (using SDR optimization).
3) AO-CS: Alice performs alternating optimization between beamforming and phase shift as described in Section VI. B. Both beamforming vectors and phase shifter matrices are closed-form in the alternating process. The secrecy outage probability of the proposed AO-CS scheme can be measured by Eq. (15). The computational complexity is $O\{\text{iter}_{\max}[N_t^3 + N_s^2N_t]\}$ as discussed in Section VI. E.

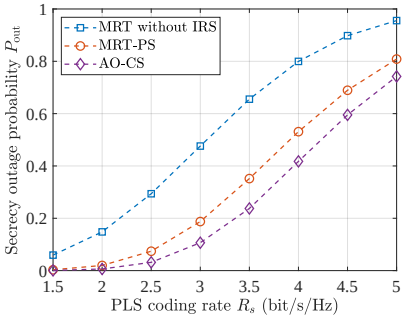
Before the comparison simulations, we first verify the convergence performance of the alternating optimization scheme in Fig. 5a. As can be seen in this figure, P_{out} converges as the



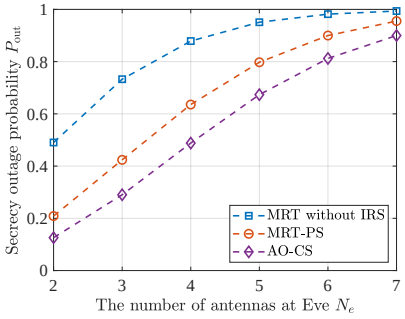
(a) $N_t = 10$, $N_e = 2$, $N_s = 32$, $\alpha = \beta = 0.8$, and SNR is 7 dB.



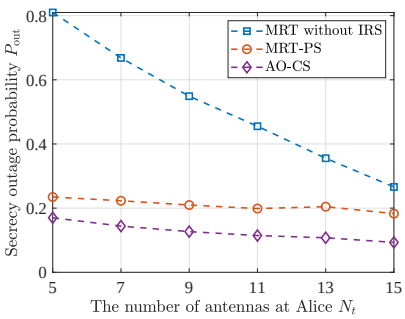
(b) $N_t = 10$, $N_e = 2$, $N_s = 32$, $\alpha = \beta = 0.8$, and R_s is 3 bit/s/Hz.



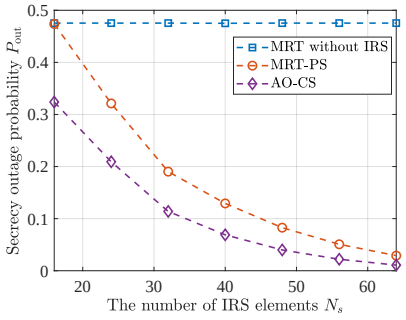
(c) $N_t = 10$, $N_e = 2$, $N_s = 32$, $\alpha = \beta = 0.8$, and SNR is 9 dB.



(d) $N_t = 10$, $N_s = 32$, $\alpha = \beta = 0.8$, SNR is 9 dB, and $R_s = 3$ bit/s/Hz.



(e) $N_e = 3$, $N_s = 32$, $\alpha = \beta = 0.8$, SNR is 9 dB, and $R_s = 3$ bit/s/Hz.



(f) $N_t = 10$, $N_e = 2$, $\alpha = \beta = 0.8$, SNR is 9 dB, and $R_s = 3$ bit/s/Hz.

Fig. 5: Secrecy outage probability in IRS-assisted MISOME scenarios.

number of iterations increases in the AO-CS scheme. The curve shows a good performance of algorithm convergence as the convergence point appears before 10 iterations.

The secrecy outage probability in terms of SNR is evaluated in Fig. 5b. Several observations can be made as follows. Firstly, we can find that the secrecy outage probability decreases with an increasing SNR then nearly approaches to a constant in higher SNR regions, and transmission power provides a less gain for IRS-assisted PLS compared to IRS-free cases. Secondly, the IRS-assisted schemes outperform the scheme without IRS as IRS can provide more randomness in wireless channels. Lastly, the proposed AO-CS scheme has a better performance than others.

Next, we want to show the impact of the PLS coding rate on secrecy outage probability in Fig. 5c, where an increasing PLS coding rate can enlarge the secrecy outage probability in all schemes. The proposed AO-CS outperforms these schemes and the advantage is obvious in the higher rate region. The effects of the number of Eve's antennas on secrecy outage probability are examined Fig. 5d, where these curves show an increasing trend in secrecy outage probability

when Eve has more antennas, but the lines rise slowly in the AO-CS scheme. It means the eavesdropping antenna effect used to be an important consideration and does much harm on traditional PLS schemes, but is relieved by IRS. The proposed scheme absolutely outperforms others a lot when the number of Eve's antennas is large, e.g., the secrecy outage probability of the proposed scheme is reduced by almost 20% compared to the MRT-PS scheme when $N_e = 5$.

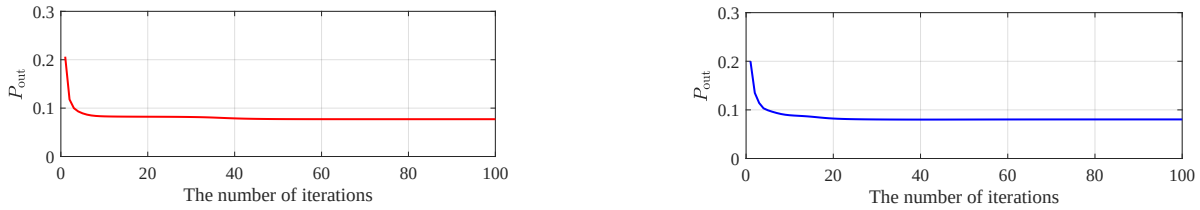
Finally, Figs. 5e and 5f illustrate the impacts of the number of Alice's antennas and IRS elements on secrecy outage probability, respectively. From Fig. 5e, we can observe that a large number of Alice's antennas will decrease secrecy outage probability in all schemes. With phase shifter optimization, the secrecy outage probability decreases quickly as the optimal phase shifter matrix provides a larger gain for the main channel compared to the individual direct channel. A similar trend is seen in Fig. 5f, it shows that the secrecy outage probability is reduced with the increasing number of IRS elements. As the cost of IRS elements is less than that of antenna radio frequency modules, a huge number of elements are available in wireless communications. Throughout all simulations, the AO-CS is the best choice for PLS as it significantly reduce the secrecy outage probability with acceptable computational cost.

D. Multiple-Antenna Alice and Bob

In the IRS-assisted MIMOME scenarios, we consider three different schemes, i.e., MRT without IRS, the proposed alternating optimization (AO) scheme based on SDR (AO-SDR), and the proposed AO scheme based on manifold optimization (AO-Man). They are described as follows.

1) MRT without IRS: Alice performs MRT-based beamforming, i.e., $\mathbf{w}/\sqrt{\rho} = \text{eigvec}_{\lambda_{\max}}(\mathbf{H}_b^{\mathrm{H}}\mathbf{H}_b)$ where $\mathbf{H}_b$ represent the channel between Alice and Bob in the scenarios without IRS [19], and phase shift control is not considered in this case. Meanwhile, Bob use $\mathbf{w}^{\mathrm{H}}$ as the receiving vector. The secrecy outage probability of MRT-based beamforming is calculated as $P_{\text{out,MRT}}(R_s) = \Gamma(N_e, \phi_m)/\Gamma(N_e)$, where $\phi_m = \sigma_e^2(2^{C_m - R_s} - 1)/\rho$ and $C_m = \log_2(1 + \rho\alpha^2\lambda_{\max}/\sigma^2)$. The computational complexity of MRT-based beamforming is $O(N_b^3)$.
2) AO-SDR: Alice performs alternating optimization between beamforming and SDR-based phase shifter optimization as described in Section V. B. The secrecy outage probability of the proposed AO-SDR scheme can be measured by Eq. (15). The computational complexity is $O\{\text{iter}_{\max}[\ln(1/\epsilon)N_s^{4.5} + N_t^3 + N_s^2 N_t]\}$ as discussed in Section V. E.

3) AO-Man: Alice performs alternating optimization between beamforming and manifold-based phase shifter optimization as described in Section V. C. The secrecy outage probability of the proposed AO-Man scheme can be measured by Eq. (15). The computational complexity is $O[\text{iter}_{\max}(N_s^4 + N_t^3 + N_s^2 N_t)]$ as discussed in Section V. E.



(a) AO-Man convergence.

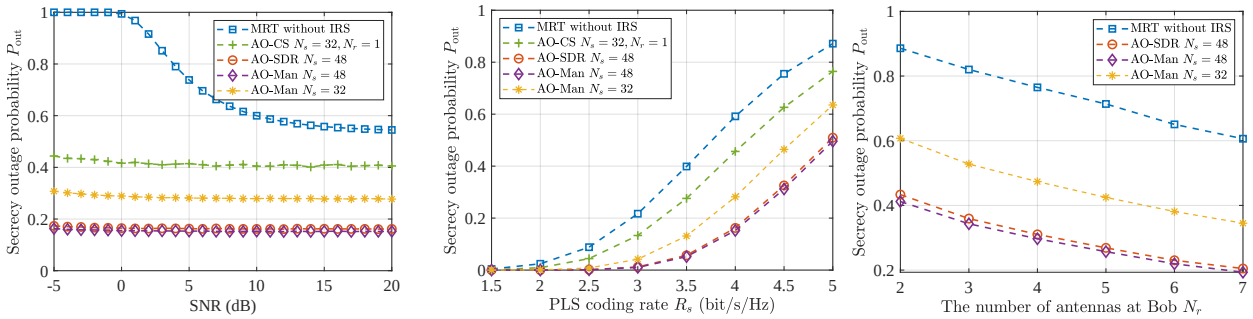
(b) AO-SDR convergence.

Fig. 6: Convergence tests in IRS-assisted MIMOME scenarios, where $N_s = 32$, $N_e = 2$, $N_t = 10$, $N_r = 3$, $\alpha = \beta = 0.8$, SNR is 7 dB, and PLS coding rate is 3 bit/s/Hz.

Firstly, we also verify the convergence performance of the AO-Man and AO-SDR schemes in Fig. 6. It is shown that P_{out} converges as the number of iterations increases in both AO-Man and AO-SDR schemes. The curve shows a good performance of algorithm convergence as the convergence point appears before 10 iterations. We also find that AO-Man converge faster than AO-SDR because the conjugate-gradient descent method of manifold optimization executes faster than the Newton method in the SDR approach.

The SNR impact on the secrecy outage probability of IRS-assisted MIMOME models is evaluated in Fig. 7a. Similar to the single-antenna Bob case, the transmission power provides a lower gain in IRS-assisted PLS as we can find that the secrecy outage probability slowly decreases with an increasing SNR. It is also shown that the proposed AO-SDR and AO-Man schemes have a better performance than others, and the AO-man is better than the AO-SDR as the maximum eigenvalue method in AO-SDR can not guarantee to provide the optimal phase shifter matrix, as discussed in Section V. B. Last but no least, by comparing the green line with the violet one, we can find the secrecy performance is improved when the multiple antennas are used at Bob. It means that our schemes applied to the IRS-assisted MIMOME case outperforms the state-of-the-art researches [3], [8], [11] as they focus on the IRS-assisted MISOME case.

Then, we want to show the effect of the PLS coding rate on secrecy outage probability in Fig. 7b. We find that an increasing PLS coding rate results in the rise of secrecy outage probability in all schemes, and the proposed AO-SDR and AO-Man outperform much of these schemes. It is



(a) $N_t = 10$, $N_e = 2$, $N_r = 3$, $\alpha = \beta = 0.8$, and R_s is 4 bit/s/Hz.

(b) $N_t = 10$, $N_e = 2$, $N_r = 3$, $\alpha = \beta = 0.8$, and SNR is 9 dB.

(c) $N_t = 10$, $N_e = 2$, $\alpha = \beta = 0.8$, SNR is 9 dB, and R_s is 4 bit/s/Hz.

Fig. 7: Secrecy outage probability in IRS-assisted MIMOME scenarios.

also demonstrated that the low computational complexity scheme, i.e., the MRT without IRS, has the similar performance with others when the preset PLS coding rate is small, so it is a possible plan if computational resources are scarce although it has the worst security performance. Lastly, the impact of the number of Bob's antennas is checked in Fig. 7c. Although we have known the increasing number of Bob's antennas can reduce the secrecy outage probability through the simulations above, Fig. 7c shows a fast linear descent on the secrecy outage probability. It is because MIMO provides a larger diversity gain than the MISO case, and more randomness that contributes to PLS will be produced among antennas when more antennas are used at Bob.

VIII. Conclusions

In this paper, we focus on the PLS scenario without the instantaneous CSI of eavesdropper in IRS-assisted MIMOME channels, in which the expression of secrecy outage probability for any beamforming vector and phase shifter matrix is deduced by Gamma distribution. Following that, we design an alternating optimization scheme between the beamforming vector and phase shifter matrix to reduce the secrecy outage probability. Also, lower computational complexity schemes are found in the single antenna cases. Simulation results have shown that the proposed optimization scheme can reduce secrecy outage probability significantly in comparison with state-of-the-art schemes. As one of our future works, we will integrate multi-IRS-assisted PLS, in which multiple IRSs will cooperate with each other to improve the secrecy performance.

APPENDIX

A. Proof of Lemma 1

Recalling the random variable $x = |\beta\mathbf{a} + \mathbf{C}\mathbf{u}|^2$ as shown in Eq. (11). We begin to calculate the mean and variance of $x \sim X(\beta, m, n, \mathbf{u})$ as follows. At first, the mean of x is expressed as

$$\mathbb{E}(x) = \mathbb{E}(\beta^2|\mathbf{a}|^2) + \mathbb{E}(|\mathbf{C}\mathbf{u}|^2) = m(\beta^2 + |\mathbf{u}|^2). \tag{62}$$

Then, we will deduce the variance of x, i.e., $\text{Var}(x)$, which is given as

$$\text{Var}(x) = \mathbb{E}(|x|^2) - |\mathbb{E}(x)|^2, \tag{63}$$

where $\mathbb{E}(|x|^2)$ can be transformed as

$$\begin{aligned}
\mathbb{E}(|x|^2) &= \mathbb{E}(\big||\beta\mathbf{a} + \mathbf{C}\mathbf{u}|^2\big|^2) \\
&= \mathbb{E}\big(\big||\beta\mathbf{a}|^2 + |\mathbf{C}\mathbf{u}|^2 + \beta\mathbf{u}^{\mathrm{H}}\mathbf{C}^{\mathrm{H}}\mathbf{a} + \beta\mathbf{a}^{\mathrm{H}}\mathbf{C}\mathbf{u}\big|^2\big) \\
&= \mathbb{E}\big(\big||\beta\mathbf{a}|^2\big|^2\big) + \mathbb{E}\big(\big||\mathbf{C}\mathbf{u}|^2\big|^2\big) + \mathbb{E}\big(|\beta\mathbf{u}^{\mathrm{H}}\mathbf{C}^{\mathrm{H}}\mathbf{a}|^2\big) \\
&\quad + \mathbb{E}(|\beta\mathbf{a}^{\mathrm{H}}\mathbf{C}\mathbf{u}|^2) + 2\mathbb{E}(|\beta\mathbf{a}|^2|\mathbf{C}\mathbf{u}|^2),
\end{aligned} \tag{64}$$

$\mathbb{E}\big(|\beta\mathbf{u}^{\mathrm{H}}\mathbf{C}^{\mathrm{H}}\mathbf{a}|^2\big) = \mathbb{E}(|\beta\mathbf{a}^{\mathrm{H}}\mathbf{C}\mathbf{u}|^2) = \beta^2 m|\mathbf{u}|^2$, and $\mathbb{E}(|\beta\mathbf{a}|^2|\mathbf{C}\mathbf{u}|^2) = \beta^2 m^2|\mathbf{u}|^2$. According to the property of noncentral chi-square distribution, the mean and variance of $|\beta\mathbf{a}|^2$ is $\beta^2 m$ and $\beta^4 m$, respectively. Hence, $\mathbb{E}(\big||\beta\mathbf{a}|^2\big|^2)$ can be expressed as

$$\mathbb{E}(\big||\beta\mathbf{a}|^2\big|^2) = \text{Var}(|\beta\mathbf{a}|^2) + [\mathbb{E}(|\beta\mathbf{a}|^2)]^2 = \beta^4(m + m^2). \tag{65}$$

We introduce an auxiliary random variable $\mathbf{z}_1 = \mathbf{C}\mathbf{u}/|\mathbf{u}|$ such that $\mathbf{z}_1 \sim \mathcal{CN}_{m,1}(\mathbf{0}, \mathbf{I}_m)$. We change the form of $\mathbb{E}(\big||\mathbf{C}\mathbf{u}|^2\big|^2)$ as

$$\mathbb{E}(\big||\mathbf{C}\mathbf{u}|^2\big|^2) = \mathbb{E}(|\mathbf{u}|^4|\mathbf{z}_1|^4) = (m^2 + m)|\mathbf{u}|^4. \tag{66}$$

Following that, we have

$$\mathbb{E}(|x|^2) = (\beta^4 + |\mathbf{u}|^4 + 2\beta^2|\mathbf{u}|^2)(m^2 + m). \tag{67}$$

Then, according to Eq. (63), $\text{Var}(x)$ can be expressed as

$$\text{Var}(x) = (\beta^4 + |\mathbf{u}|^4 + 2\beta^2|\mathbf{u}|^2)m. \tag{68}$$

Hence, the shape and scale of the Gamma distribution can be expressed as [25]

$$k = \frac{[\mathbb{E}(x)]^2}{\text{Var}(x)} = m, \quad w = \frac{\text{Var}(x)}{\mathbb{E}(x)} = \beta^2 + |\mathbf{u}|^2. \tag{69}$$

At last, on the basis of the definition of the Gamma distribution [25], we get the PDF and CDF of X as follows.

$$f_X(x) = \frac{1}{\Gamma(k_1)w^k}x^{k-1}\exp(-x/w) = \frac{1}{\Gamma(m)(\beta^2+|\mathbf{u}|^2)^m}x^{m-1}\exp(-\frac{x}{\beta^2+|\mathbf{u}|^2}),$$
$$F_X(x) = 1 - \frac{1}{\Gamma(k)}\Gamma(k,\frac{x}{w}) = 1 - \frac{1}{\Gamma(m)}\Gamma(m,\frac{x}{\beta^2+|\mathbf{u}|^2}), \tag{70}$$

where $\Gamma(x)$ is the Gamma function of variable x, and $\Gamma(\epsilon,\eta)$ is the upper incomplete Gamma function defined in Eq. (13). The proof is completed. ■

REFERENCES

[1] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, Fourthquarter 2019.

[2] 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.

[3] 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.

[4] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. D. Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12 296–12 300, Oct. 2020.

[5] 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.

[6] J. Zhang, H. Du, Q. Sun, B. Ai, and D. W. K. Ng, "Physical layer security enhancement with reconfigurable intelligent surface-aided networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3480–3495, May 2021.

[7] 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.

[8] 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.

[9] J. Qiao and M. S. Alouini, "Secure transmission for intelligent reflecting surface-assisted mmwave and terahertz systems," *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1743–1747, Oct. 2020.

[10] Z. Chu, W. Hao, P. Xiao, D. Mi, Z. Liu, M. Khalily, J. R. Kelly, and A. P. Feresidis, "Secrecy rate optimization for intelligent reflecting surface assisted MIMO system," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1655–1669, Nov. 2021.

[11] L. Dong and H.-M. Wang, "Secure MIMO transmission via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 787–790, Jun. 2020.

[12] H. Niu, Z. Chu, F. Zhou, Z. Zhu, M. Zhang, and K.-K. Wong, "Weighted sum secrecy rate maximization using intelligent reflecting surface," *Early Access in IEEE Trans. Commun., DOI: 10.1109/TCOMM.2021.3085780.*

[13] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE J. Selected Areas in Commun.*, vol. 38, no. 11, pp. 2637–2652, Jul. 2020.

[14] B. Feng, Y. Wu, M. Zheng, X.-G. Xia, Y. Wang, and C. Xiao, "Large intelligent surface aided physical layer security transmission," *IEEE Trans. Signal Process.*, vol. 68, pp. 5276–5291, Sep. 2020.

[15] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Proces. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[16] Y. Liu, W. Wang, H.-H. Chen, F. Lyu, L. Wang, W. Meng, and X. Shen, "Physical layer security assisted computation offloading in intelligently connected vehicle networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, pp. 3555–3570, Jun. 2021.

[17] T. Hou, Y. Liu, Z. Song, X. Sun, Y. Chen, and L. Hanzo, "MIMO assisted networks relying on large intelligent surfaces: A stochastic geometry model," *arXiv preprint arXiv:1910.00959, Online: https://arxiv.org/pdf/1910.00959.pdf*.

[18] N. Bhargav, C. R. N. da Silva, Y. J. Chun, E. J. Leonardo, S. L. Cotton, and M. D. Yacoub, "On the product of two $\kappa - \mu$ random variables and its application to double and composite fading channels," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2457–2470, Apr. 2018.

[19] M. Kang and M.-S. Alouini, "Largest eigenvalue of complex Wishart matrices and performance analysis of MIMO MRC systems," *IEEE J. Selected Areas in Commun.*, vol. 21, no. 3, pp. 418–426, Apr. 2003.

[20] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, Firstquarter 2017.

[21] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[22] T. Van Chien, L. T. Tu, S. Chatzinotas, and B. Ottersten, "Coverage probability and ergodic capacity of intelligent reflecting surface-enhanced communication systems," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 69–73, Jan. 2021.

[23] Z. Cui, K. Guan, J. Zhang, and Z. Zhong, "SNR coverage probability analysis of RIS-aided communication systems," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3914–3919, Apr. 2021.

[24] A. M. Salhab and M. H. Samuh, "Accurate performance analysis of reconfigurable intelligent surfaces over Rician fading channels," *IEEE Wireless Commun. Lett.*, vol. 10, no. 5, pp. 1051–1055, May 2021.

[25] E. W. Weisstein, *CRC concise encyclopedia of mathematics*. Boca Raton, Florida, USA: CRC press, 2002.

[26] Y. Liu, H. H. Chen, and L. Wang, "Secrecy capacity analysis of artificial noisy MIMO channels–An approach based on ordered eigenvalues of Wishart matrices," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 617–630, Mar. 2017.

[27] P.-A. Absil, R. Mahony, and R. Sepulchre, *Optimization algorithms on matrix manifolds*. Princeton, New Jersey, US: Princeton University Press, 2009.

[28] Z. Luo, W. Ma, A. M. 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.

[29] K.-Y. Wang, A. M.-C. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 21, pp. 5690–5705, Nov. 2014.

[30] N. Boumal, B. Mishra, P.-A. Absil, and R. Sepulchre, "Manopt, a Matlab toolbox for optimization on manifolds," *Journal of Machine Learning Research*, vol. 15, no. 42, pp. 1455–1459, Apr. 2014.

[31] X. Yu, D. Xu, and R. Schober, "MISO wireless communication systems via intelligent reflecting surfaces : (invited paper)," in *2019 IEEE/CIC International Conference on Communications in China (ICCC)*, 2019, pp. 735–740.

[32] J. R. Shewchuk *et al.*, "An introduction to the conjugate gradient method without the agonizing pain," 1994.

[33] J. C. Bezdek and R. J. Hathaway, "Convergence of alternating optimization," *Neural, Parallel & Scientific Computations*, vol. 11, no. 4, pp. 351–368, Dec. 2003.

[34] H.-M. Wang, J. Bai, and L. Dong, "Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 27, pp. 1300–1304, Jul. 2020.