Enhancing Physical Layer Security with RIS under Multi-Antenna Eavesdroppers and Spatially Correlated Channel Uncertainties

Zongze Li, Qingfeng Lin, Yik-Chung Wu, Derrick Wing Kwan Ng, and Arumugam Nallanathan

***Abstract*—Reconfigurable intelligent surface (RIS) has the capability to significantly enhance physical layer security by reconfiguring the propagation in wireless communications. However, due to the cascaded channel brought by the RIS and the hostile nature of potential eavesdroppers, acquiring perfect channel state information (CSI) of the eavesdroppers is challenging. Worse still, if the eavesdroppers are equipped with multiple antennas and there exists spatial correlation at the RIS due to closely spaced RIS elements, the random channel matrices are complicatedly coupled with the phase shift and other wireless resources in the outage probabilistic constraint, making their optimizations intractable. To date, there has been no systematic and feasible approach to address such a challenge. To fill this gap, this paper for the first time reveals an analytical transformation for handling the intractable outage probabilistic constraint. It is theoretically established that when the maximum tolerable outage probability is smaller than a threshold around 0.4, which generally holds in practice, the proposed transformation is exact and suffers no performance loss. As an illustrative example of the developed constraint transformation, the secure energy efficiency maximization is selected as the objecitve function and the resultant resource optimization is handled by the alternating maximization framework. Numerical results are presented to show the rapid convergence behavior of the proposed algorithm and unveil that the proposed probabilistic constraint transformation has superiority over the Bernstein-Type Inequality approximation. Compared with several baseline schemes (e.g., random phase-shift, fixed phase-shift, RIS ignoring CSI uncertainty, and secure transmission without RIS), the proposed scheme significantly boosts the performance, underscoring the significance of appropriately managing the probabilistic constraint outage and optimizing RIS phase shifts for secure transmission against multi-antenna eavesdroppers.**

***Index Terms*—Outage probability, physical layer security, reconfigurable intelligent surface, channel uncertainty, multi-antenna eavesdroppers.**

I. Introduction

Reconfigurable intelligent surface (RIS) has recently attracted tremendous attention from both industry and academia because of its abundant spatial degrees of freedom and revolutionary programmability. Compared to the traditional active nodes approach, which actively transmits the signals, a RIS shapes the impinging signal by altering the phase shift coefficients of the reflecting elements that could possibly establish virtual end-to-end line-of-sight (LoS) links between a base station (BS) and its desired mobile users even though the direct LoS path is blocked [1]. In addition, RIS could also provide a new means for effective physical layer security provisioning. To be specific, when the legitimate users and the eavesdroppers are in proximity, the traditional beamforming [2], which focuses the transmitted energy on legitimate receivers, may also benefit the decoding at eavesdroppers. In contrast, the employment of RIS can reduce the information leakage and improve transmission security by providing additional transmission links to the users while nulling the directions towards the eavesdroppers [3].

Previous works on RIS-aided secure transmission assume the availability of perfect channel state information (CSI) of the eavesdroppers' channels [4], [5]. Under this assumption, secure transmission with optimized RIS phase shift could achieve a better transmission performance than the scheme with random phase shift [6] or fixed phase shift [7]. While these results are promising, the perfect eavesdroppers' CSI assumption is generally invalid in practice due to inevitable estimation errors and hardware limitations. As such, RIS-aided secure transmission taking into account eavesdroppers' CSI uncertainty has been designed recently [8]–[10]. However, they only investigate the case of single-antenna eavesdroppers with limited application scenarios [6]. Since eavesdroppers in practice could be equipped with multiple antennas for effective wiretapping and those results obtained from the single-antenna cases are not applicable, investigating the secure transmission strategy under multi-antenna eavesdroppers in RIS-aided systems is paramount from the wireless communication security point of view [11].

Due to the imprecise knowledge of eavesdroppers' channels, practical RIS-aided secure transmission design should incorporate the notion of outage probability [12], which unluckily does not always admit tractable closed-form expressions. For instance, analyzing the outage probability for the situation of single-antenna eavesdroppers has been shown to be a nontrivial task [8]. On the other hand, for the generalized multi-antenna cases, the related outage analysis is undoubtedly more complex since the uncertain random channel matrices are non-trivially coupled with the optimization variables in the outage probability constraint. The situation is even more challenging if there exists spatial correlation in the uncertain channels due to

Zongze Li is with Peng Cheng Laboratory, Shenzhen 518038, China (e-mail: lizz@pcl.ac.cn). Qingfeng Lin and Yik-Chung Wu are with the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong (e-mail: qflin@eee.hku.hk; ycwu@eee.hku.hk). Derrick Wing Kwan Ng is with the School of Electrical Engineering and Telecommunications, the University of New South Wales, Australia (e-mail: w.k.ng@unsw.edu.au). A. Nallanathan is with the School of Electronic Engineering and Computer Science at Queen Mary University of London, UK (e-mail: a.nallanathan@qmul.ac.uk). (Corresponding Authors: Qingfeng Lin and Yik-Chung Wu).

the closely spaced RIS elements [13], [14]. Yet, a systematic and tractable approach for handling the complicated outage probabilistic constraint has not been studied before.

To overcome the above challenges and fill this gap, this paper for the first time reveals an efficient transformation to handle the outage probabilistic constraint taking into account the existence of multi-antenna eavesdroppers. In particular, the properties of the unitary matrix, matrix identities, and the Kronecker product [15] are non-trivially leveraged to compute the outage probability. Although this result manages to transform the probabilistic constraint into a deterministic form, it does not facilitate the design of a secure transmission system due to strongly coupled optimization variables. To this end, a constraint subset of the outage probability is further proposed based on a property of regularized gamma function [16]. It is shown that if the maximum tolerable outage probability is smaller than a threshold, which is determined by the number of antennas at the eavesdropper, adopting the subset constraint will not incur any performance loss. On the other hand, when the maximum tolerable outage probability is greater than the derived threshold, a guideline on minimizing the performance loss is also proposed based on the monotonic behaviors of the upper incomplete gamma function.

Compared with the conventional Monte Carlo sampling method [17] for tackling complicated probabilistic constraints, the proposed tight problem transformation provides an analytical expression that can be applied seamlessly to a wide class of wireless resources allocation optimization problems. Furthermore, compared to the widely used Bernstein-Type Inequality (BTI) safe approximation, the proposed approach does not lead to performance loss for a large range of maximum tolerable outage probability. As an illustration to demonstrate the strength of our proposed framework in handling the complex probabilistic constraint in secure transmission, this paper studies the secure energy efficiency (EE) maximization under multi-antenna eavesdroppers and spatially correlated channel uncertainties. Due to the proposed novel probabilistic constraint transformation, the resultant problem becomes tractable under the alternating maximization (AM) framework [18], where the closed-form optimal solution is obtained for the RIS phase shift, while the concave-convex procedure [19] and rank property of the positive semidefinite matrix are employed to handle the optimization of data covariance matrix. Simulation results are presented to show the convergence behavior of the proposed algorithm, the performance gains from the proposed tight problem transformation over the BTI safe approximation, and its superior secure EE over the baseline schemes of random phase shift (RPS), fixed phase shift (FPS), RIS ignoring CSI uncertainty, and secure transmission without RIS.

The rest of this paper is organized as follows. System model and the secure transmission problem are formulated in Section II. The outage probabilistic constraint in secure transmission system is handled in Section III. In Section IV, the optimization methods for solving secure EE maximization problem are detailed. Finally, simulation results are presented in Section V and conclusion is drawn in Section VI.

Notation: Column vectors and matrices are denoted by lowercase and uppercase boldface letters, respectively. Conjugate transpose, transpose, Frobenius norm, trace, the modulus of a scalar, the vectorization of matrix $\mathbf{X}$, the determinant of matrix $\mathbf{X}$, and the $(i,j)^{th}$ element of matrix $\mathbf{X}$ are denoted by $(\cdot)^H$, $(\cdot)^T$, $\|\cdot\|_F$, $\mathrm{Tr}(\cdot)$, $|\cdot|$, $\mathrm{vec}(\mathbf{X})$, $\det(\mathbf{X})$, and $\mathbf{X}_{i,j}$, respectively. $\mathbb{E}\{\cdot\}$ stands for the mathematical expectation, and $\mathrm{diag}\{x_1,\ldots,x_N\}$ represents a diagonal matrix with the diagonal components being $x_1,\ldots,x_N$. The notations $\Pr(\cdot)$ and $[x]^+$ stand for the probability of an event and $\max\{x,0\}$, respectively. The real part of a complex-valued variable, the Hadamard product between two matrices, and the Kronecker product are denoted by $\Re[\cdot]$, $\circ$, and $\otimes$, respectively. $\mathcal{N}(\cdot,\cdot)$ and $\mathcal{CN}(\cdot,\cdot)$ denote the normal distribution and the circularly symmetric complex normal distribution, respectively. $\mathrm{Exp}(\cdot)$ denotes the exponential distribution. The upper incomplete gamma function is defined as $\gamma(y,x)=\int_x^\infty t^{y-1}e^{-t}\mathrm{dt}$ [20].

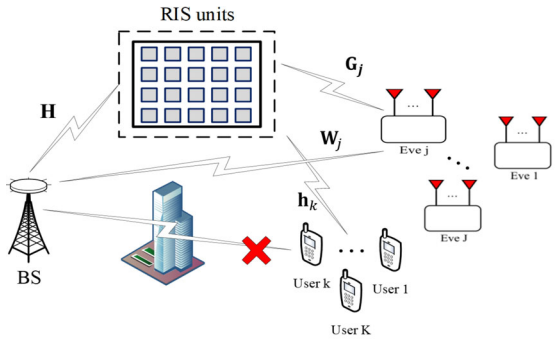


Fig. 1. RIS-aided secure MIMO network with multiple users and eavesdroppers.

II. System Model and Problem Formulation

We consider a downlink secure multicast system, as it is a spectrally and energy-efficient transmission, which supports efficient, reliable, and scalable group communication services [21]. As shown in Fig. 1, there are one N-antenna base station (BS), one RIS with M reflecting elements (controlled by the dedicated communication-oriented software), K single-antenna legitimate users, and J independent idle subscribed users who act as passive eavesdroppers (Eves) intercepting the muticasting of confidential messages to other users with Eve j equipped with N_j antennas, $\forall j\in\{1,\ldots,J\}$. All the users and eavesdroppers are located in a single-cell homogeneous environment. In particular, it is assumed that users are not moving in high speed such that the coherence time is sufficiently long compared with the transmission duration. Also, we consider an urban area with a lot of scatters in the environment but the direct links from the BS to the user are blocked by obstacles, e.g., buildings, and communications can only be established via the RIS. However, due to the malicious behaviour of eavesdroppers, it is assumed that there exist direct links from the BS to eavesdroppers. Considering a narrowband transmitted signal in such a rich scattering environment, all the wireless channels are modeled as quasi-static Rayleigh flat-fading [7].

Let the channels from the BS to the RIS, from the RIS to user k, from the BS to Eve j, and from the RIS to Eve j be denoted by $\mathbf{H}\in\mathbb{C}^{M\times N}$, $\mathbf{h}_k\in\mathbb{C}^{M\times 1},\forall k\in\mathcal{K}=\{1,\ldots,K\}$,

$\mathbf{W}_j \in \mathbb{C}^{N\times N_j}$ and $\mathbf{G}_j \in \mathbb{C}^{M\times N_j}, \forall j \in \mathcal{J} = \{1,\ldots,J\}$, respectively. Since the users and Eves are located in a single-cell homogeneous environment, they share the same channel and thermal noise statistics. Therefore, by observing the users' channels, the BS can acquire the statistical CSI of $\mathbf{W}_j$ and $\mathbf{G}_j$ with $\text{vec}(\mathbf{W}_j) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{NN_j})$ and $\text{vec}(\mathbf{G}_j) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_j} \otimes \mathbf{\Sigma}_{\text{RIS}})$, where $\mathbf{\Sigma}_{\text{RIS}} \in \mathbb{C}^{M\times M}$ is the spatial correlation matrices at the RIS.[1]Here, we include the correlation at the RIS as the elements of an RIS might be placed close to each other and the RIS spatial correlation is expressed as [14]

$$[\mathbf{\Sigma}_{\text{RIS}}]_{n_1,n_2} = \text{sinc}\left(\frac{2z_{n_1,n_2}}{d}\right), \ \forall n_1, n_2 \in \{1,\cdots,N\}, \quad (1)$$

where z_{n_1,n_2} denotes the distance between the n_1^{th} and the n_2^{th} RIS element, and d is the wavelength. On the other hand, the phase-shift coefficients[2]of the RIS are collected in a diagonal matrix $\mathbf{\Theta} = \text{diag}\{e^{i\theta_1},\ldots,e^{i\theta_M}\} \in \mathbb{C}^{M\times M}$, where $i^2 = -1$, and $\theta_m \in [0, 2\pi)$ with $m \in \{1,\ldots,M\}$.

Let the transmitted signal from the BS to all the users be denoted by $\mathbf{x}$ with the covariance matrix $\mathbf{Q} = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\} \in \mathbb{C}^{N\times N}$. With flat-fading channel, the received signals at user k and Eve j are respectively given by

$$y_k = \sqrt{\alpha_k}\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H}\mathbf{x} + n_k, \ \forall k, \quad (2)$$

$$\mathbf{y}_j = \sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H}\mathbf{x} + \sqrt{\beta_j}\mathbf{W}_j^H\mathbf{x} + \mathbf{n}_j, \ \forall j, \quad (3)$$

where α_k and $n_k \sim \mathcal{CN}(0,\sigma_k^2)$ are the path loss coefficient and the receiver noises at user k, respectively. Furthermore, α_j and β_j are the path loss coefficients for the links RIS-Eve j and the BS-Eve j, respectively. $\mathbf{n}_j$ is zero mean additive white Gaussian noises with the covariance matrix $\sigma_j^2\mathbf{I}$.

Based on (2) and (3), the channel capacities of user k and Eve j are respectively given by

$$R_b^k = \log_2\left(1 + \alpha_k(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})\mathbf{Q}(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})^H/\sigma_k^2\right), \ \forall k, \quad (4)$$

$$R_e^j = \log_2\det\left(\mathbf{I} + \left(\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H\right)\mathbf{Q} \times \left(\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H\right)^H/\sigma_j^2\right), \ \forall j. \quad (5)$$

For Eve j's channel, since the BS is unable to acquire its perfect estimate, the knowledge of the channel capacity of Eve j is generally uncertain [25]. Consequently, a secrecy outage event occurs at the BS when R_e^j exceeds the redundancy rate of user k. Denoting the redundancy rate as $D_{k,j}$, the secrecy outage probability (SOP) of user k due to Eve j is given by

$$p_{\text{so}}^{k,j} = \Pr\left\{D_{k,j} < \log_2\det\left(\mathbf{I} + (\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)\mathbf{Q} \times (\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)^H/\sigma_j^2\right)\right\}. \quad (6)$$

[1]Existing RIS-assisted physical layer security tasks are mainly based on the idealistic assumption of an independent and identically distributed (i.i.d.) channel model at the RIS [22], [23]. In this paper, we consider a spatially correlated Rayleigh fading model that is more practical when the elements of an RIS are placed close to each other [14], [24].

[2]This paper mainly considers the continuous phase shift model. For the discrete phase shift case, one possible approach is to first obtain the optimized phases from Algorithm 2 in Section IV and then quantize them to the nearest allowable discrete values.

Considering the non-colluding eavesdropping case, the instantaneous secrecy rate at user k achieved by the BS for all potential eavesdroppers is $\min_{j\in\mathcal{J}}[\log_2(1 + \alpha_k(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})\mathbf{Q}(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})^H/\sigma_k^2) - D_{k,j}]^+$. Since the achievable secrecy rate for multicast network is determined by the worst communication link [26], the multicast achievable secrecy rate is expressed as

$$\min_{k\in\mathcal{K},j\in\mathcal{J}} \left[\log_2\left(1 + \alpha_k\left(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H}\right)\mathbf{Q}\left(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H}\right)^H/\sigma_k^2\right) - D_{k,j}\right]^+, \quad (7)$$

which is the minimum achievable secrecy rate of all the users.

On the other hand, the total energy consumption of the RIS-assisted downlink system constitutes four major components: 1) the transmit power at the BS; 2) the hardware static power at BS and users; 3) the static power consumption of RIS arises from both the control circuits and impedance-adjusting semiconductor components, which are crucial for its operational functionality; 4) the dynamic power consumption of RIS arising from channel estimation. Then, the energy consumption model is given by [27], [28]

$$\frac{1}{\eta}\text{Tr}\left(\mathbf{Q}\right) + P_a + KP_c + M(P_s + P_e/T_f), \quad (8)$$

where $\eta \in (0,1)$ is the power amplifier efficiency and $\text{Tr}\left(\mathbf{Q}\right)$ is the transmit power at the BS. P_a and P_c are the hardware-dissipated power at the BS and the circuit power at each user, respectively. P_s is the static power consumption associated with a single reflecting element due to control circuits and impedance-adjusting. P_e is the dynamic energy consumption for channel estimation during a frame duration T_f [28].

Our objective is to optimize the secure EE subject to SOP constraint, phase shift constraint, and transmit power constraint. The secure EE is adopted to quantify the effective secrecy rate in the wireless system while considering the energy consumption. With the secure EE defined as the achievable secrecy rate (7) per unit of the total power consumption (8) [29], the corresponding optimization problem is formulated as

$$\textbf{(P1)} \ \max_{\mathbf{Q},\mathbf{\Theta},\{D_{k,j}\}} \frac{\min_{k\in\mathcal{K},j\in\mathcal{J}}\left[\log_2\left(1 + \alpha_k(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})\mathbf{Q}(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})^H/\sigma_k^2\right) - D_{k,j}\right]^+}{\frac{1}{\eta}\text{Tr}\left(\mathbf{Q}\right) + P_a + KP_c + M(P_s + P_e/T_f)} \quad (9a)$$

$$\text{s.t.} \ \ p_{\text{so}}^{k,j} \le \varepsilon, \ \forall k, j, \quad (9b)$$

$$|\mathbf{\Theta}_{m,m}| = 1, \ \forall m, \quad (9c)$$

$$\text{Tr}\left(\mathbf{Q}\right) \le P_{\max}, \ \mathbf{Q} \succeq \mathbf{0}, \ \text{rank}(\mathbf{Q}) = 1, \quad (9d)$$

where $\varepsilon \in (0,1)$ denotes the maximum tolerable SOP, and $P_{\max}$ is the maximum transmit power at the BS. The phase-shift coefficients constraint (9c) means that the amplitude of the reflecting elements of the RIS operates at 100% reflection efficiency.

In fact, problem **P1** provides a generalized formulation for evaluating the RIS-aided secure transmission performance via

the objective function defined in (9a). If we set $1/\eta = 0$, the denominator of the objective function becomes a constant and the fractional objective function reduces to a non-fractional form, which corresponds to secrecy rate maximization. It is important to note that all derivations and results remain valid in this case. Hence, **P1** can be employed to investigate not only secure EE maximization but also secrecy rate maximization. If **P1** can be solved, the corresponding objective function value is the achievable secure energy efficiency, while the corresponding solution for the transmit covariance matrix, phase shift design, and redundancy rate are the system parameters that lead to the secure energy efficiency[3] given by the optimized objective function value.

Notice that **P1** is a stochastic nonconcave optimization problem with a probabilistic constraint (9b). Even if we consider other objective functions rather than that in (9a), the probabilistic constraint still exists and remains an obstacle in solving the problem at hand. In general, the Monte Carlo simulation-based method [17] can be employed to tackle the probabilistic constraint. However, this approach requires solving **P1** numerous times, thus introducing prohibitively large computational load. To avoid the heavy computational burden, another widely used approach is to adopt the BTI to transform the probabilistic constraint (9b) into a more conservative but deterministic one [31]. To be specific, notice that since $\mathrm{vec}(\mathbf{G}_j) \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{I}_{N_j} \otimes \mathbf{\Sigma}_{\mathrm{RIS}}\right)$, it can be rewritten as $\mathrm{vec}(\mathbf{G}_j) = \left(\mathbf{I}_{N_j} \otimes \mathbf{\Sigma}_{\mathrm{RIS}}\right)^{\frac{1}{2}} \mathrm{vec}(\tilde{\mathbf{G}}_j)$, where $\mathrm{vec}(\tilde{\mathbf{G}}_j) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{MN_j})$. Then, the probabilistic constraint (9b) can be rewritten as

$$p_{so}^{k,j} = \Pr\Bigg\{(2^{D_{k,j}} - 1)\sigma_j^2 < \left[\mathrm{vec}(\tilde{\mathbf{G}}_j)^H, \mathrm{vec}(\mathbf{W}_j)^H\right](\mathbf{X} \otimes \mathbf{I}_{N_j}) \times \left[\mathrm{vec}(\tilde{\mathbf{G}}_j)^H, \mathrm{vec}(\mathbf{W}_j)^H\right]^H\Bigg\} \leq \varepsilon, \tag{10}$$

where matrix $\mathbf{X}$ is given by

$$\mathbf{X} = \begin{bmatrix} \alpha_j(\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H) & \sqrt{\alpha_j\beta_j}\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q} \\ \sqrt{\alpha_j\beta_j}\mathbf{Q}(\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H & \beta_j\mathbf{Q} \end{bmatrix}. \tag{11}$$

Since $\mathrm{vec}(\tilde{\mathbf{G}}_j)$ and $\mathrm{vec}(\mathbf{W}_j)$ are independent, $\left[\mathrm{vec}(\tilde{\mathbf{G}}_j)^H, \mathrm{vec}(\mathbf{W}_j)^H\right]^H \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{(N+M)N_j})$. Then, a smaller subset constraint to constraint (10) can be obtained by using the BTI [32]:

$$(2^{D_{k,j}} - 1)\sigma_j^2 \leq \mathrm{Tr}(\mathbf{X} \otimes \mathbf{I}_{N_j}) + \sqrt{2\ln(\varepsilon^{-1})}\|\mathbf{X} \otimes \mathbf{I}_{N_j}\|_F + \ln(\varepsilon^{-1})\left[\lambda_{\max}(\mathbf{X} \otimes \mathbf{I}_{N_j})\right]^+, \tag{12}$$

where $\lambda_{\max}(\cdot)$ denotes the largest eigenvalue of the input matrix. Although (12) is a deterministic constraint, it is generally a safe approximation, i.e., (12)⇒(10), which inevitably causes performance loss due to the restrictive feasible set. Worse still, since the optimization variables $\mathbf{\Theta}$ and $\mathbf{Q}$ are coupled in the Hermitian matrix $\mathbf{X}$, the deterministic constraint (12) does not facilitate the optimization of problem **P1** and transmission system design. To overcome the above challenges, in the next section, we provide a novel method to handle the probabilistic constraint (9b).

[3]Considering the multicast channel model, the dirty paper coding-based scheme [30] could be adopted to achieve the optimized secure energy efficiency, and the coding scheme depends implicitly on the channel uncertainties of Eves through the solution of **P1**.

Remark 1. *In general, there are two practical eavesdropping models: the colluding model and non-colluding model [4]. In the colluding model, eavesdroppers collaborate to process their received private information jointly. In contrast, the non-colluding model involves eavesdroppers acting independently, each with the ability to individually intercept private information. In this paper, since the eavesdroppers are regarded as the independent idle subscribed users who act as passive eavesdroppers, we adopt the non-collaborative eavesdropping model. For the colluding case, it is a promising topic for future research.*

III. Handling of the Probabilistic Constraint

The imperfect CSI of Eves is characterized by the outage probabilistic constraint $p_{\mathrm{so}}^{k,j} \leq \varepsilon$. For the single-antenna Eves, the exponentially distributed received signal power under Rayleigh fading channels has been employed to transform the probabilistic constraint into a deterministic one [8]. However, for the cases with multi-antenna Eves, the SOP constraint is more complicated and hence deriving a closed-form expression is nontrivial.

More specifically, using (6), the SOP constraint can be rewritten as

$$p_{\mathrm{so}}^{k,j} = \Pr\Bigg\{2^{D_{k,j}} < \det\left(\mathbf{I} + (\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)\mathbf{Q} \times (\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)^H/\sigma_j^2\right)\Bigg\} \leq \varepsilon, \forall k, j. \tag{13}$$

To handle the probabilistic constraint (13), we present the following lemma, which provides an equivalent deterministic form. The equivalence is leveraged on properties of unitary matrix, matrix identities, and the Kronecker product [15], and the detailed proof is presented in Appendix A.

Lemma 1. *Given* $\mathrm{vec}(\mathbf{W}_j) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{NN_j})$ *and* $\mathrm{vec}(\mathbf{G}_j) \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{I}_{N_j} \otimes \mathbf{\Sigma}_{\mathrm{RIS}}\right)$*, the SOP constraint of* (13) *can be equivalently expressed as:*

$$p_{\mathrm{so}}^{k,j} = \frac{\gamma\left(N_j, \frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1}\right)}{(N_j - 1)!} \leq \varepsilon, \ \forall k, j, \tag{14}$$

where $\lambda_1 = \mathrm{Tr}(\mathbf{X})$ *with* $\mathbf{X} = \begin{bmatrix} \alpha_j(\mathbf{\Sigma}_{RIS}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Sigma}_{RIS}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H) & \sqrt{\alpha_j\beta_j}\mathbf{\Sigma}_{RIS}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q} \\ \sqrt{\alpha_j\beta_j}\mathbf{Q}(\mathbf{\Sigma}_{RIS}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H & \beta_j\mathbf{Q} \end{bmatrix}$.

To visualize the equivalence between (13) and (14), $p_{\mathrm{so}}^{k,j}$ is plotted with respect to $D_{k,j}$ with $N = 64$, $M = 10$, $K = 2$, $J = 4$, $\{N_j = 4\}_{j=1}^4$ in Fig. 2 (other settings will be detailed at the beginning of Section V). It can be seen that the SOP from (13) and (14) perfectly coincide with each other even

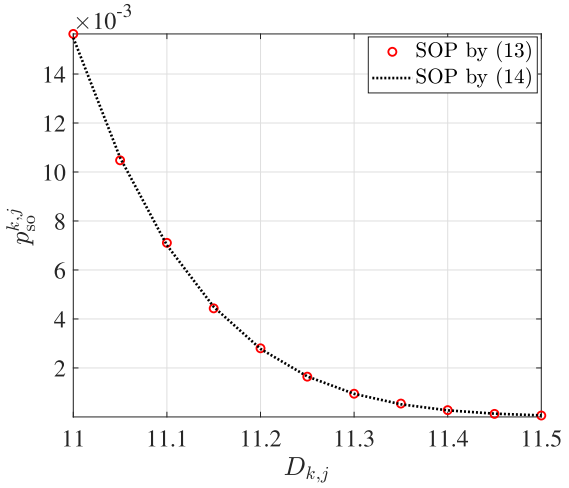


Fig. 2. SOP versus $D_{k,j}$ with $N = 64$, $M = 10$, $K = 2$, $J = 4$, $\{N_j = 4\}_{j=1}^{4}$.

when SOP is below 10^{-3}, which validates the accuracy of Lemma 1.

While we explicitly obtain an expression for the SOP in (14), the optimization variable $D_{k,j}$ appears inside the upper incomplete gamma function such that the constraint is still intractable from optimization perspective. By further leveraging the property of the incomplete gamma function, we provide the following theorem for handling the constraint (14).

Theorem 1. *If* $\varepsilon \in \left(0, \frac{\gamma(N_j,N_j)}{(N_j-1)!}\right]$, *constraint* (14) *is equivalent to*

$$D_{k,j} \geq \log_2\left(1 + \frac{N_j}{\sigma_j^2}\left(1 + \sqrt{2\ln(\mu_{k,j}^{-1})} + \ln(\mu_{k,j}^{-1})\right) \times \mathrm{Tr}\left(\alpha_j \boldsymbol{\Sigma}_{RIS}\boldsymbol{\Theta}\mathbf{H}\mathbf{Q}(\boldsymbol{\Theta}\mathbf{H})^H + \beta_j \mathbf{Q}\right)\right), \forall k, j, \tag{15}$$

with the tunable parameter $\mu_{k,j}$ *satisfying*

$$\frac{\gamma\left(N_j, N_j\left(1 + \sqrt{2\ln(\mu_{k,j}^{-1})} + \ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!} = \varepsilon. \tag{16}$$

On the other hand, if $\varepsilon \in (\frac{\gamma(N_j,N_j)}{(N_j-1)!}, 1]$, *constraint* (15) *is always tighter than the constraint* (14).

Proof. Please see Appendix B. □

The importance of Theorem 1 is that when the maximum tolerable SOP ε is smaller than $\frac{\gamma(N_j,N_j)}{(N_j-1)!}$, the SOP admits an equivalent tractable form. In case the maximum tolerable SOP ε is greater than $\frac{\gamma(N_j,N_j)}{(N_j-1)!}$, (15) provides a more conservative constraint than (14). Notice that when $\{N_j = 1\}_{j=1}^{J}$, (15) reduces to the result of [8].

Since it is known that the objective function of problem (9) is a monotonic function on $D_{k,j}$, maximizing (9a) is equivalent to minimizing $D_{k,j}$. Exploiting Theorem 1, the maximizer $D_{k,j}^{\diamond}$ of (9) must activate (15), which yields

$$D_{k,j}^{\diamond} = \log_2\left(1 + \frac{N_j}{\sigma_j^2}\left(1 + \sqrt{2\ln(\mu_{k,j}^{-1})} + \ln(\mu_{k,j}^{-1})\right) \times \mathrm{Tr}\left(\alpha_j \boldsymbol{\Sigma}_{\mathrm{RIS}}\boldsymbol{\Theta}\mathbf{H}\mathbf{Q}(\boldsymbol{\Theta}\mathbf{H})^H + \beta_j \mathbf{Q}\right)\right), \forall k, j. \tag{17}$$

From Theorem 1, if $\varepsilon \in (0, \frac{\gamma(N_j,N_j)}{(N_j-1)!}]$, adopting (17) does not lead to any performance loss. However, if $\varepsilon > \frac{\gamma(N_j,N_j)}{(N_j-1)!}$, the obtained $D_{k,j}^{\diamond}$ of (17) serves as a conservative solution, and the choice of $\mu_{k,j}$ would affect the degree of conservatism. The following property is provided to minimize the conservatism.

Lemma 2. *To ensure* $D_{k,j}^{\diamond}$ *be the closest to that of the optimal solution of* (9) *when* $\varepsilon > \frac{\gamma(N_j,N_j)}{(N_j-1)!}$, *the tunable parameter* $\mu_{k,j}$ *in* (17) *should be chosen as* $\mu_{k,j} = 1$.

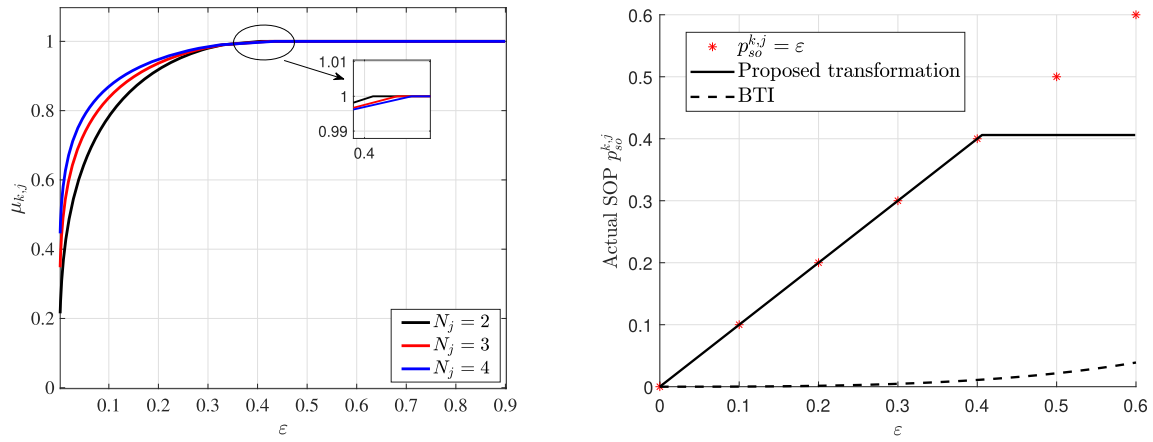
Proof. Please see Appendix C. □

The relationship between the tunable parameter $\mu_{k,j}$ and ε is determined by (16) and Lemma 2, and we illustrate the relationship in Fig. 3(a). It can be observed that the tunable parameter $\mu_{k,j}$ increases in $\varepsilon \in (0, \frac{\gamma(N_j,N_j)}{(N_j-1)!}]$ and reaches 1 when $\varepsilon = \frac{\gamma(N_j,N_j)}{(N_j-1)!}$. Moreover, it can be seen from the enlarged part of the figure that $\frac{\gamma(N_j,N_j)}{(N_j-1)!}$ takes value around 0.4 when $N_j = 2$ and the value of $\frac{\gamma(N_j,N_j)}{(N_j-1)!}$ is increasing in N_j, which means that $\frac{\gamma(N_j,N_j)}{(N_j-1)!}$ will generally larger than 0.4 even the eavesdropper employs more antennas. As we usually aim to control the outage to be a small value, there is a high chance that $\varepsilon < \frac{\gamma(N_j,N_j)}{(N_j-1)!}$ in practice and (17) does not lead to any loss. Since $\frac{\gamma(N_j,N_j)}{(N_j-1)!}$ does not depend on $\boldsymbol{\Sigma}_{\mathrm{RIS}}$, the threshold value 0.4 is independent of the spatial correlation. On the other hand, the maximizer $D_{k,j}^{\diamond}$ of (9) would be different in uncorrelated and correlated cases, as it depends on $\boldsymbol{\Sigma}_{\mathrm{RIS}}$ as shown in (17).

To show the tightness of the realized outage probability, we plot the realized outage probability for various ε in Fig. 3(b). The realized outage probability is obtained by first computing $\mu_{k,j}$ according to (16) and Lemma 2, then $D_{k,j}^{\diamond}$ in (17), and finally the left hand side of (14). Correspondingly, we also plot the obtained outage probability given by the BTI in (12). In particular, we can take the equality sign in (12), solve for $D_{k,j}$, and then put the resultant $D_{k,j}$ into the left hand side of (14). It can be seen that the realized outage probability of the proposed transformation match exactly ε from 0 to about 0.4. Although it becomes flat after ε is greater than 0.4, the achieved outage probability of the proposed method is still much tighter than that of the BTI method.

IV. Secure Energy Efficiency Maximization

To demonstrate the usage of the result in Section III, we focus on the secure energy efficiency maximization problem in **P1**. By virtue of (17), **P1** is transformed into (18), shown at the top of the next page, where the $\mu_{k,j}$ is chosen to satisfy (16) if $\varepsilon \in (0, \frac{\gamma(N_j,N_j)}{(N_j-1)!}]$ and $\mu_{k,j} = 1$ if $\varepsilon \in (\frac{\gamma(N_j,N_j)}{(N_j-1)!}, 1]$. Despite



(a) (b)

Fig. 3. The relationship between the tunable parameter $\mu_{k,j}$ and ε. (a) The tunable parameter $\mu_{k,j}$ versus ε under different values of N_j; (b) The realized outage for various ε with $N_j = 2$.

$$\textbf{(P2)} \quad \max_{\mathbf{Q},\boldsymbol{\Theta}} \ \frac{\min\limits_{k\in\mathcal{K},j\in\mathcal{J}} \left[\log_2\left(\frac{1+\alpha_k(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})\mathbf{Q}(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})^H/\sigma_k^2}{1+\frac{N_j}{\sigma_j^2}\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\mathrm{Tr}(\alpha_j\boldsymbol{\Sigma}_{\mathrm{RIS}}\boldsymbol{\Theta}\mathbf{H}\mathbf{Q}(\boldsymbol{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q})}\right)\right]^+}{\frac{1}{\eta}\mathrm{Tr}\left(\mathbf{Q}\right)+P_a+KP_c+M(P_s+P_e/T_f)} \tag{18a}$$

$$\text{s.t.} \quad |\boldsymbol{\Theta}_{m,m}| = 1, \ \forall m, \tag{18b}$$

$$\mathrm{Tr}\left(\mathbf{Q}\right) \le P_{\max}, \ \mathbf{Q} \succeq \mathbf{0}, \ \mathrm{rank}(\mathbf{Q}) = 1, \tag{18c}$$

the absence of a probabilistic constraint in **P2**, tackling it remains difficult because of the non-differentiable and non-convex nature of the objective function (18a), and the rank-one restriction.

For the non-smooth objective function, we notice that the denominator of (18a) does not depend on k and j. Hence, (18a) is equivalent to

$$\min_{k,j}\left\{\frac{\left[\log_2\left(\frac{1+\alpha_k(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})\mathbf{Q}(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})^H/\sigma_k^2}{1+\frac{N_j}{\sigma_j^2}\xi_{k,j}\mathrm{Tr}(\alpha_j\boldsymbol{\Sigma}_{\mathrm{RIS}}\boldsymbol{\Theta}\mathbf{H}\mathbf{Q}(\boldsymbol{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q})}\right)\right]^+}{\frac{1}{\eta}\mathrm{Tr}\left(\mathbf{Q}\right)+P_a+KP_c+M(P_s+P_e/T_f)}\right\}, \tag{19}$$

where $\xi_{k,j} = 1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})$. Therefore, **P2** is equivalently transformed into

$$\max_{\mathbf{Q},\boldsymbol{\Theta}}\min_{k,j}\left\{\frac{\left[\log_2\left(\frac{1+\alpha_k(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})\mathbf{Q}(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})^H/\sigma_k^2}{1+\frac{N_j}{\sigma_j^2}\xi_{k,j}\mathrm{Tr}(\alpha_j\boldsymbol{\Sigma}_{\mathrm{RIS}}\boldsymbol{\Theta}\mathbf{H}\mathbf{Q}(\boldsymbol{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q})}\right)\right]^+}{\frac{1}{\eta}\mathrm{Tr}\left(\mathbf{Q}\right)+P_a+KP_c+M(P_s+P_e/T_f)}\right\} \tag{20a}$$

$$\text{s.t.} \ |\boldsymbol{\Theta}_{m,m}| = 1, \quad \forall m, \tag{20b}$$

$$\mathrm{Tr}\left(\mathbf{Q}\right) \le P_{\max}, \ \mathbf{Q} \succeq \mathbf{0}, \ \mathrm{rank}(\mathbf{Q}) = 1. \tag{20c}$$

Since the inner objective function of (20) only depends on one k or j, and the parameters $\{\alpha_k, \alpha_j, \mu_{k,j}, \sigma_j, \sigma_k, N_j\}$ are independent of the optimization variables $\{\mathbf{Q}, \boldsymbol{\Theta}\}$, the operations of maximization and minimization in (20) are interchangeable. As a result, problem (20) can be solved by independently solving KJ maximization problems in a parallel manner under the modern multi-core computing architecture, and then choosing the minimum value. For the optimization subproblem for user k with Eve j, it is expressed as

$$\max_{\mathbf{Q},\boldsymbol{\Theta}} \ \frac{\left[\log_2\left(\frac{1+\alpha_k(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})\mathbf{Q}(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})^H/\sigma_k^2}{1+\frac{N_j}{\sigma_j^2}\xi_{k,j}\mathrm{Tr}(\alpha_j\boldsymbol{\Sigma}_{\mathrm{RIS}}\boldsymbol{\Theta}\mathbf{H}\mathbf{Q}(\boldsymbol{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q})}\right)\right]^+}{\frac{1}{\eta}\mathrm{Tr}\left(\mathbf{Q}\right)+P_a+KP_c+M(P_s+P_e/T_f)} \tag{21a}$$

$$\text{s.t.} \quad |\boldsymbol{\Theta}_{m,m}| = 1, \quad \forall m, \tag{21b}$$

$$\mathrm{Tr}\left(\mathbf{Q}\right) \le P_{\max}, \ \mathbf{Q} \succeq \mathbf{0}, \ \mathrm{rank}(\mathbf{Q}) = 1. \tag{21c}$$

Notice that constraints in (21) are not coupled when either $\mathbf{Q}$ or $\boldsymbol{\Theta}$ is fixed, the optimization problem can be solved under the alternating maximization (AM) framework [18]. To be specific, when variable $\mathbf{Q}$ is fixed, the closed-form optimal solution to the subproblem of (21) can be derived based on the rank property of the positive semidefinite matrix and trace property of symmetric matrices of $\boldsymbol{\Sigma}_{\mathrm{RIS}}$ and $\boldsymbol{\Theta}$. On the other hand, when variable $\boldsymbol{\Theta}$ is fixed, the subproblem of (21) can be solved by concave-convex procedure (CCP) and Dinkelbach algorithm, where a stationary solution is obtained.

A. Updating $\boldsymbol{\Theta}$

When $\mathbf{Q}$ is fixed, the optimization problem for updating $\boldsymbol{\Theta}$ becomes

$$\mathcal{Q}1: \max_{\boldsymbol{\Theta}} \log_2\left(\frac{1+\alpha_k(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})\mathbf{Q}(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})^H/\sigma_k^2}{1+\frac{N_j\xi_{k,j}}{\sigma_j^2}\mathrm{Tr}\left(\alpha_j\boldsymbol{\Sigma}_{\mathrm{RIS}}\boldsymbol{\Theta}\mathbf{H}\mathbf{Q}(\boldsymbol{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q}\right)}\right) \quad (22a)$$

$$\text{s.t.} \quad |\boldsymbol{\Theta}_{m,m}|=1, \ \forall m, \quad (22b)$$

where the pointwise operation $[\cdot]^+$ is removed since the objective function value of optimization problem (21) must be non-negative at the optimality. To handle the unit modulus constraint (22b), existing standard methods include: the semi-definite relaxation, the penalty method, the majorization minimization, the manifold optimization, the gradient descent, or the convex relaxation [33]. Not to mention these methods incur high computational complexity, none of them guarantee optimal solution of $\mathcal{Q}1$. In the following, we reveal that $\mathcal{Q}1$ has a special structure such that deriving the global optimal closed-form solution of $\boldsymbol{\Theta}$ is possible.

Firstly, we rewrite $\mathrm{Tr}\left(\alpha_j\boldsymbol{\Sigma}_{\mathrm{RIS}}\boldsymbol{\Theta}\mathbf{H}\mathbf{Q}(\boldsymbol{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q}\right)$ as

$$\begin{aligned}&\mathrm{Tr}\left(\alpha_j\boldsymbol{\Sigma}_{\mathrm{RIS}}\boldsymbol{\Theta}\mathbf{H}\mathbf{Q}(\boldsymbol{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q}\right)\\ &=\mathrm{Tr}\left(\alpha_j\mathbf{H}\mathbf{Q}\mathbf{H}^H\boldsymbol{\Theta}^H\boldsymbol{\Sigma}_{\mathrm{RIS}}\boldsymbol{\Theta}\right)+\mathrm{Tr}(\beta_j\mathbf{Q}) \quad (23)\\ &=\mathrm{Tr}\left(\alpha_j\mathbf{H}\mathbf{Q}\mathbf{H}^H\boldsymbol{\Theta}^H\boldsymbol{\Theta}\boldsymbol{\Sigma}_{\mathrm{RIS}}\right)+\mathrm{Tr}(\beta_j\mathbf{Q}) \quad (24)\\ &=\mathrm{Tr}\left(\alpha_j\mathbf{H}\mathbf{Q}\mathbf{H}^H\boldsymbol{\Sigma}_{\mathrm{RIS}}\right)+\mathrm{Tr}(\beta_j\mathbf{Q}), \quad (25)\end{aligned}$$

where (23) follows from cyclic permutations property of trace operation, (24) is obtained due to the symmetric matrices of $\boldsymbol{\Sigma}_{\mathrm{RIS}}$ and $\boldsymbol{\Theta}$, and (25) follows from $\boldsymbol{\Theta}^H\boldsymbol{\Theta}=\mathbf{I}_M$. Based on (25) and denoting $\mathbf{e}=[e^{i\theta_1},\ldots,e^{i\theta_M}]^H$ as the diagonal elements of $\boldsymbol{\Theta}$, $\mathcal{Q}1$ is equivalently rewritten as

$$\max_{\mathbf{e}} \log_2\left(\frac{1+\alpha_k\mathbf{e}^H\boldsymbol{\Upsilon}_k\mathbf{e}/\sigma_k^2}{1+\frac{N_j\xi_{k,j}}{\sigma_j^2}\mathrm{Tr}\left(\alpha_j\mathbf{H}\mathbf{Q}\mathbf{H}^H\boldsymbol{\Sigma}_{\mathrm{RIS}}+\beta_j\mathbf{Q}\right)}\right), \quad (26)$$

where $\boldsymbol{\Upsilon}_k=\mathrm{diag}(\mathbf{h}_k^H)\mathbf{H}\mathbf{Q}(\mathrm{diag}(\mathbf{h}_k^H)\mathbf{H})^H$. Since $\mathrm{rank}\left(\boldsymbol{\Upsilon}_k\right)\le\mathrm{rank}(\mathbf{Q})$ always holds [34, Lemma 4] and it is known that $\mathrm{rank}(\mathbf{Q})=1$, $\boldsymbol{\Upsilon}_k$ is a rank-one positive semidefinite matrix. As a result, $\boldsymbol{\Upsilon}_k$ can be decomposed as $\boldsymbol{\Upsilon}_k=\boldsymbol{\kappa}_k\boldsymbol{\kappa}_k^H$ with $\boldsymbol{\kappa}_k=[\kappa_{k,1},\ldots,\kappa_{k,M}]^H\in\mathbb{C}^{M\times1}$. Then, problem (26) can be equivalently expressed as

$$\max_{\mathbf{e}} \log_2\left(\frac{1+\alpha_k|\mathbf{e}^H\boldsymbol{\kappa}_k|^2/\sigma_k^2}{1+\frac{N_j\xi_{k,j}}{\sigma_j^2}\mathrm{Tr}\left(\alpha_j\mathbf{H}\mathbf{Q}\mathbf{H}^H\boldsymbol{\Sigma}_{\mathrm{RIS}}+\beta_j\mathbf{Q}\right)}\right). \quad (27)$$

Notice that maximizing (27) is equivalent to maximizing the quadratic function $|\mathbf{e}^H\boldsymbol{\kappa}_k|^2$, which can be expressed as

$$|\mathbf{e}^H\boldsymbol{\kappa}_k|^2=\left|\sum_{m=1}^{M}|\kappa_{k,m}|e^{i\angle\kappa_{k,m}}e^{-i\theta_m}\right|^2. \quad (28)$$

Since $|\mathbf{e}^H\boldsymbol{\kappa}_k|^2$ reaches its maximum value $|\sum_{m=1}^{M}|\kappa_{k,m}||^2$ when $\theta_m=\angle\kappa_{k,m},\forall m$, the maximizer $\mathbf{e}^*$ of problem (27) is given by $\mathbf{e}^*=[e_1^*,\ldots,e_M^*]$ with $e_m^*=e^{i\angle\kappa_{k,m}}$. Since $\mathcal{Q}1$ is equivalently transformed into (26) and then (27) without any approximation, the solution

$$\boldsymbol{\Theta}^*=\mathrm{diag}\{e^{i\angle\kappa_{k,1}},\ldots,e^{i\angle\kappa_{k,M}}\} \quad (29)$$

is the optimal solution for $\mathcal{Q}1$. With $\boldsymbol{\Theta}^*$ being a closed-form solution, the corresponding algorithm is convenient for efficient hardware implementation.

B. Updating $\mathbf{Q}$

When $\boldsymbol{\Theta}$ is fixed, the optimization problem for updating $\mathbf{Q}$ is

$$\mathcal{D}1: \max_{\mathbf{Q}} \frac{[\Gamma(\mathbf{Q})]^+}{\frac{1}{\eta}\mathrm{Tr}(\mathbf{Q})+P_a+KP_c+M(P_s+P_e/T_f)} \quad (30a)$$

$$\text{s.t.} \quad \mathrm{Tr}(\mathbf{Q})\le P_{\max}, \ \mathbf{Q}\succeq\mathbf{0}, \ \mathrm{rank}(\mathbf{Q})=1, \quad (30b)$$

where $\Gamma(\mathbf{Q})$ is given by

$$\Gamma(\mathbf{Q})=\log_2\left(\frac{1+\alpha_k(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})\mathbf{Q}(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})^H/\sigma_k^2}{1+\frac{N_j\xi_{k,j}}{\sigma_j^2}\mathrm{Tr}\left(\alpha_j\mathbf{H}\mathbf{Q}\mathbf{H}^H\boldsymbol{\Sigma}_{\mathrm{RIS}}+\beta_j\mathbf{Q}\right)}\right). \quad (31)$$

Due to the fractional form inside the logarithm function $\Gamma(\mathbf{Q})$, the objective function of $\mathcal{D}1$ is non-concave. Fortunately, since $\Gamma(\mathbf{Q})$ can be rewritten as a difference of two concave functions, the concave-convex procedure (CCP) [35] can be employed to locally concavify $\Gamma(\mathbf{Q})$ at a feasible point $\mathbf{Q}^{(n)}$ as $\hat{\Gamma}(\mathbf{Q};\mathbf{Q}^{(n)})$. This results in a lower bound at the point $\mathbf{Q}^{(n)}$ as

$$\begin{aligned}&\hat{\Gamma}(\mathbf{Q};\mathbf{Q}^{(n)})\\ &=\log_2\left(1+\alpha_k(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})\mathbf{Q}(\mathbf{h}_k^H\boldsymbol{\Theta}\mathbf{H})^H/\sigma_k^2\right)\\ &-\log_2\left(1+\frac{N_j\xi_{k,j}}{\sigma_j^2}\mathrm{Tr}\left(\alpha_j\mathbf{H}\mathbf{Q}^{(n)}\mathbf{H}^H\boldsymbol{\Sigma}_{\mathrm{RIS}}+\beta_j\mathbf{Q}^{(n)}\right)\right)\\ &-\frac{\frac{N_j\xi_{k,j}}{\sigma_j^2}\mathrm{Tr}\left(\alpha_j\mathbf{H}(\mathbf{Q}-\mathbf{Q}^{(n)})\mathbf{H}^H\boldsymbol{\Sigma}_{\mathrm{RIS}}+\beta_j(\mathbf{Q}-\mathbf{Q}^{(n)})\right)}{\left(1+\frac{N_j\xi_{k,j}}{\sigma_j^2}\mathrm{Tr}\left(\alpha_j\mathbf{H}\mathbf{Q}^{(n)}\mathbf{H}^H\boldsymbol{\Sigma}_{\mathrm{RIS}}+\beta_j\mathbf{Q}^{(n)}\right)\right)\ln 2}.\end{aligned} \quad (32)$$

By virtue of $\hat{\Gamma}(\mathbf{Q};\mathbf{Q}^{(n)})$, $\mathcal{D}1$ can be iteratively handled by solving a subproblem at the $(n+1)^{th}$ iteration being[4]

$$\max_{\mathbf{Q}\succeq\mathbf{0}} \frac{\hat{\Gamma}(\mathbf{Q};\mathbf{Q}^{(n)})}{\frac{1}{\eta}\mathrm{Tr}(\mathbf{Q})+P_a+KP_c+M(P_s+P_e/T_f)}, \quad (33a)$$

$$\text{s.t.} \quad \mathrm{Tr}(\mathbf{Q})\le P_{\max}, \ \mathrm{rank}(\mathbf{Q})=1. \quad (33b)$$

Since $\hat{\Gamma}(\mathbf{Q};\mathbf{Q}^{(n)})$ is concave on $\mathbf{Q}$, the objective function (33a) is in a concave-convex form. Accordingly, the Dinkelbach algorithm [36] can be employed to transform (33) into a sequence of subproblems, with the l^{th} subproblem given

[4]The operation of pointwise maximum $[\cdot]^+$ is omitted without loss of optimality, since the objective function value of $\mathcal{D}1$ must be non-negative at the optimality.

Algorithm 1 CCP and Dinkelbach Method for Solving $\mathcal{D}1$

1: Initialize $\mathbf{Q}^{(0)}$ and set $n := 0$.
2: **repeat**
3: Initialize ψ_0 and set $l := 0$.
4: **repeat**
5: Solve problem (35) with $\mathbf{Q}^{(n)}$ and denote the optimal value of (35) as $\mathbf{Q}^{\diamond}$.
6: Update $\mathbf{Q} = \mathbf{Q}^{\diamond}$ and ψ_l with the objective function value of (33a).
7: Update iteration: $l := l + 1$.
8: **until** Stopping criterion is satisfied.
9: Update $\mathbf{Q}^{(n+1)} = \mathbf{Q}$ and iteration $n := n + 1$.
10: **until** Stopping criterion is satisfied.

by

$$\max_{\mathbf{Q}\succeq\mathbf{0}} \quad \hat{\Gamma}(\mathbf{Q};\mathbf{Q}^{(n)}) - \psi_l\left(\frac{1}{\eta}\mathrm{Tr}\left(\mathbf{Q}\right) + P_a + KP_c + M(P_s + P_e/T_f)\right) \tag{34a}$$

$$\text{s.t.} \quad \mathrm{Tr}\left(\mathbf{Q}\right) \le P_{\max},\ \mathrm{rank}(\mathbf{Q}) = 1, \tag{34b}$$

where ψ_l is the objective function value of (33a) with $\mathbf{Q}$ substituted by the optimal solution of (34) at the $(l-1)^{th}$ iteration. To tackle the rank one constraint in (34b), (34) can be relaxed by dropping constraint $\mathrm{rank}(\mathbf{Q}) = 1$, and the relaxed problem is given by

$$\max_{\mathbf{Q}\succeq\mathbf{0}} \quad \hat{\Gamma}(\mathbf{Q};\mathbf{Q}^{(n)}) - \psi_l\left(\frac{1}{\eta}\mathrm{Tr}\left(\mathbf{Q}\right) + P_a + KP_c + M(P_s + P_e/T_f)\right) \tag{35a}$$

$$\text{s.t.} \quad \mathrm{Tr}\left(\mathbf{Q}\right) \le P_{\max}, \tag{35b}$$

which is a strongly concave optimization problem and can be efficiently solved via the interior-point method [37] to obtain the optimal solution. The property of the solution to (35) is revealed by the following theorem.

Theorem 2. *The optimal solution of* (35) *is always rank-one.*

Proof. Please see Appendix D. □

The entire procedure for solving $\mathcal{D}1$ is summarized in Algorithm 1, which includes the outer iterations over n with the CCP method and the inner iterations over l with the Dinkelbach method. Theorem 2 states that the rank relaxation does not cause any performance loss. Hence, the optimal solution to (35) is also the optimal solution to (34). Since (34) is the Dinkelbach's reformulation of (33), the iteration with respect to l is guaranteed to converge to the global optimal solution to (33) [36]. Furthermore, with linearized $\hat{\Gamma}(\mathbf{Q};\mathbf{Q}^{(n)})$, the iteration over n with CCP method is guaranteed to converge to a stationary solution of $\mathcal{D}1$ [35]. On the other hand, the computational complexity order of Algorithm 1 is $\mathcal{O}\left(\mathcal{I}_1\mathcal{I}_2N^{3.5}\right)$ [38, Theorem 3.12], where $\mathcal{I}_1$ and $\mathcal{I}_2$ are the required iteration numbers for the Dinkelbach method and the CCP method to converge, respectively.

Algorithm 2 The Overall Algorithm for Handling **P2**

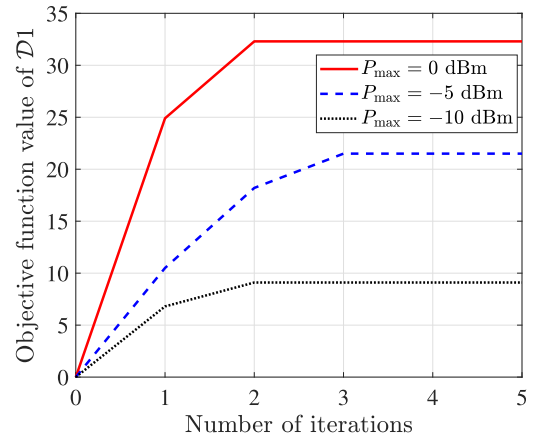
1: The feasible point of $(\mathbf{Q}, \boldsymbol{\Theta})$ is initialized based on (18b) and (18c).
2: For each $k \in \mathcal{K}$ and $j \in \mathcal{J}$, compute the objective function (21a).
3: **repeat**
4: Update $\boldsymbol{\Theta}$ based on (29).
5: Update $\mathbf{Q}$ by exploiting Algorithm 1.
6: **until** Stopping criterion is satisfied.
7: Select the minimum among KJ objective function values of (21).

C. Overall Algorithm and Discussions

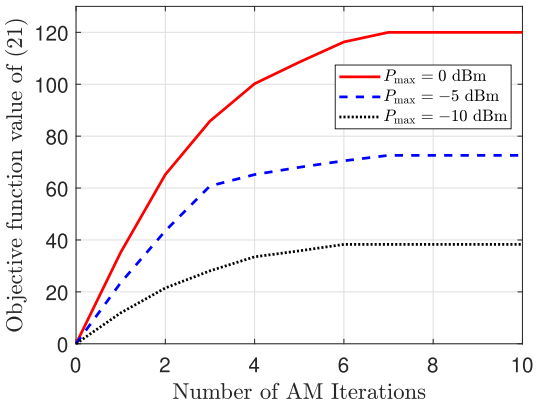
With the alternative update of $\mathbf{Q}$ and $\boldsymbol{\Theta}$, the optimization problem (21) can be effectively handled under the proposed AM framework. Since **P2** is equivalent to problem (20) and the latter comprises KJ parallel subproblems each in the form of problem (21), the overall algorithm for solving **P2** reduces to solving subproblems (21) in parallel for all k and j, and is summarized in Algorithm 2. Notice that the computational complexity is dominated by the alternating updates of variables $\boldsymbol{\Theta}$ and $\mathbf{Q}$. Specifically, the obtained $\boldsymbol{\Theta}$ is derived in a closed-form expression based on the decomposition of matrix $\boldsymbol{\Upsilon}_k$, which entails the complexity order of $\mathcal{O}\left(M^3\right)$. On the other hand, the complexity of updating $\mathbf{Q}$ is $\mathcal{O}\left(\mathcal{I}_1\mathcal{I}_2N^{3.5}\right)$. Hence, the computational complexity of the Algorithm 2 is $\mathcal{O}\left(\mathcal{T}(M^3 + \mathcal{I}_1\mathcal{I}_2N^{3.5})\right)$, where $\mathcal{T}$ is the required iteration number for the AM framework to converge.

V. Performance Evaluation and Discussions

In this section, we evaluate the secure transmission performance of the proposed algorithms through simulations. The simulation results are performed on MATLAB R2021b on a Windows x64 desktop with 3.2 GHz CPU and 16 GB RAM. For each point in the figure, it is obtained by averaging over 100 random simulation trials, with independent Eves' locations, channels, and noise realizations in each trial. Unless otherwise specified, the simulation set-up is as follows and kept throughout this section. There are 2 legitimate users and 4 Eves in the whole system. We adopt the carrier frequency of 3.3 GHz according to the 3GPP Rel-15 specification [39]. Then, the wavelength d is 0.09 m. The distance from the BS to the RIS is fixed at 20 m, and the distance from the RIS to the user is fixed at 10 m. The distance from each eavesdropper to the RIS is randomly generated between 5 m and 50 m, and the path-loss exponent is set to 3.76 [27]. As a result, the path loss coefficients of user k and Eve j can be respectively obtained based on the signal propagation model [40]. The RIS is equipped with a uniform rectangular array with the distance between the adjacent elements being $d/3$. The spatial correlation matrix is computed according to (1). The small-scale fading vectors from the RIS to all Eves and the user are generated according to $\mathcal{CN}(\mathbf{0}, \boldsymbol{\Sigma}_{\text{RIS}})$. $\mathrm{vec}(\mathbf{W}_j)$ is generated from $\mathcal{CN}(\mathbf{0}, \mathbf{I}_{NN_j})$, and $\mathrm{vec}(\mathbf{H})$ is generated from $\mathcal{CN}(\mathbf{0}, \boldsymbol{\Sigma}_{\text{RIS}} \otimes \mathbf{I}_N)$. Since the users and Eves are located in a single-cell homogeneous environment, the



(a)



(b)

Fig. 4. Convergence behavior of the proposed algorithms with $N = 64$, $M = 10$, $\{N_j = 4\}_{j=1}^{4}$, $K = 2$, $J = 4$, $\varepsilon = 0.3$. (a) The iteration of Algorithm 1; (b) The AM iterations in Algorithm 2.

noise power spectral density of Eves is identical to the users, i.e., $\sigma_u^2 = \sigma_j^2 = -99$ dBm/Hz [39]. The power amplifier efficiency is set to be $\eta = 0.3$, and the hardware-dissipated power at the BS and each user are $P_a = 39$ dBm, $P_c = 20$ dBm [7], respectively. The static power consumption associated at single reflecting element is $P_s = 10$ dBm [7]. The dynamic energy consumption for channel estimation is $P_e = 20$ dBm during $T_f = 244$ ms duration of a frame [28]. To avoid repeating descriptions of figures, the settings for $(\varepsilon, M, N, \{N_j\}, K, J, P_{\max})$ are provided in the caption of each figure.

First, to demonstrate the convergence behaviour of the proposed algorithms, we provide the simulation results as shown in Fig. 4. The initial value of $\mathbf{Q}$ is chosen as $\mathbf{Q} = \mathbf{q}\mathbf{q}^H$, where $\mathbf{q} = [\sqrt{P_{\max}/N}, \ldots, \sqrt{P_{\max}/N}]^T \in \mathbb{R}^{N\times 1}$. The stopping standard for each layer of Algorithm 1 is the relative change of the two consecutive objective function values being less than 10^{-4}. The convergence results for Algorithm 1 for solving $\mathcal{D}1$ are shown in Fig. 4(a). It is observed that the proposed algorithm achieves fast convergence under different values of $P_{\max}$. To verify the convergence of AM iteration for solving problem (21) in Algorithm 2, Fig. 4(b) shows the objective function value (21a) versus the AM iteration. It can be seen that the proposed AM algorithm converges rapidly within 10 iterations under different values of $P_{\max}$.

Next, we provide the numerical results to demonstrate the performance gains of the proposed probabilistic constraint transformation over the BTI safe approximation. It can be seen from Fig. 5 that the performance gaps between the proposed transformation and BTI method are significant, with around 50% improvement from the proposed method under various M and K as shown in Fig. 5(a) and Fig. 5(b). This is due to the tight probabilistic constraint realization from the proposed transformation in Section III. Furthermore, from Fig. 5(a), it can be seen that the average secure EEs increase in M due to more degrees of freedom provided by the increases of the RIS elements. On the other hand, as shown in Fig. 5(b), since the multicast secure EE is determined by the worst-case users' channel conditions, the performance deteriorates with an increase in the number of users K.

To show the effect of the direct link between the BS and the eavesdroppers on secure transmission performance, we compare the average secure EEs with that of secure transmission without the direct link, which is a special case of the proposed formulation if we set $\beta_j = 0$ in problem (18) and all the derivations remain unchanged. Fig. 6 shows the average secure EEs when there are two eavesdroppers. It can be observed that the performances with or without direct links are close to each other under different values of ε and $P_{\max}$. This indicates that although the existence of a direct link from the BS to the eavesdroppers would degrade the system performance to a certain extent, the proposed method can effectively mitigate this loss.

To demonstrate that the proposed solution can also address the special case of secrecy rate maximization (i.e., by setting $1/\eta = 0$ in problem (9)), the simulation results of the average secrecy rate with respect to $P_{\max}$ and M are provided and shown in Fig. 7. Compared to the RIS-aided secure transmission that ignores the channel uncertainty of single-antenna eavesdroppers [5], the proposed method significantly increases the average secrecy rates, especially under high transmit power. Furthermore, it should be emphasized that the proposed algorithm is capable of handling the more general scenarios where the eavesdroppers possess multiple antennas. In fact, the performance metrics of the proposed framework cover both the more general energy efficiency and the special case of secrecy rate maximization.

Finally, the proposed RIS scheme is compared with several baseline schemes under the same security requirement. To be specific, the simulation results of the following competing schemes are provided:

1) Random phase shift (RPS): In this scheme, the coefficients of phase shift are randomly generated with equal probability, having a complexity order of $\mathcal{O}\left(\mathcal{T}(1 + \mathcal{I}_1\mathcal{I}_2 N^{3.5})\right)$;
2) Fixed phase-shift (FPS): In this scheme, the coefficients of phase shift are fixed. Hence, $\mathbf{\Theta}$ is fixed as $\mathbf{\Theta} = \mathbf{I}_M$ with a complexity order of $\mathcal{O}\left(\mathcal{T}(1 + \mathcal{I}_1\mathcal{I}_2 N^{3.5})\right)$;
3) Ignoring CSI uncertainty: This scheme ignores the uncertain CSI for RIS-aided secure transmission with a

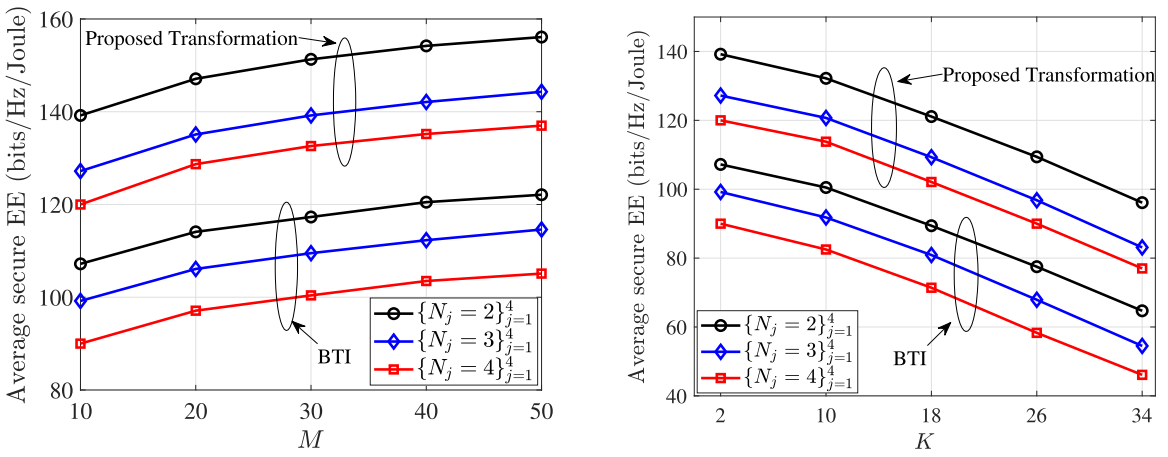


Fig. 5. Performance of the proposed algorithm under different values of tunable parameter $\mu_{k,j}$ with $N = 64$, $J = 4$, $P_{\max} = 0$ dBm, $\varepsilon = 0.3$. (a) Average secure EE versus M with $K = 2$; (b) Average secure EE versus K with $M = 10$.

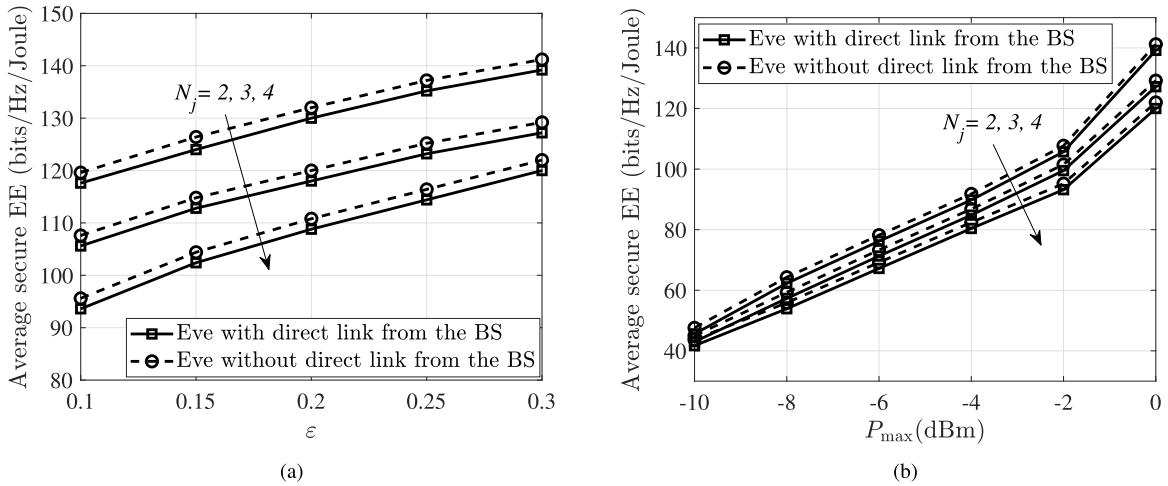


Fig. 6. Performance comparison of the proposed algorithm with transmission without the direct link, with $N = 64$, $M = 10$, $K = 2$, $J = 2$. (a) Average secure EE versus ε with $P_{\max} = 0$ dBm; (b) Average secure EE versus $P_{\max}$ and $\varepsilon = 0.3$.

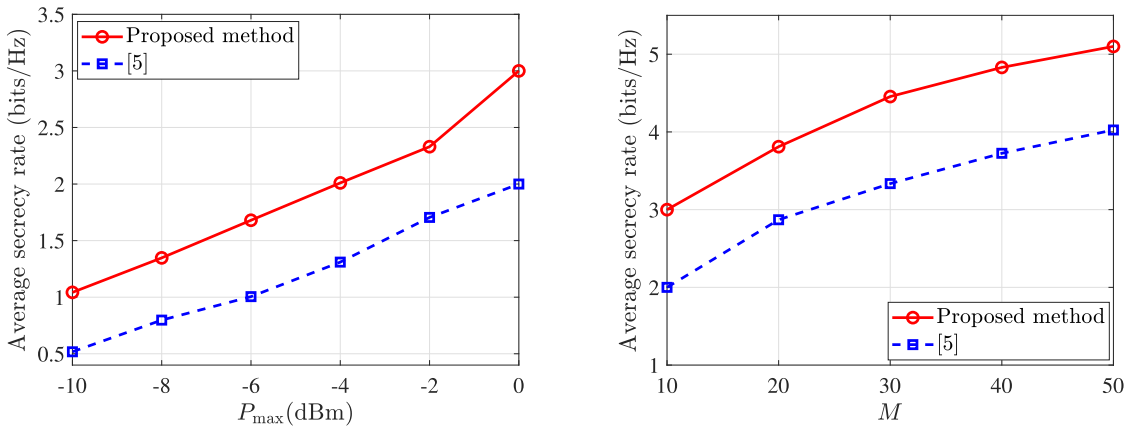


Fig. 7. Performance comparison with single-antenna eavesdropper transmission [5] with $N = 64$, $K = 2$, $J = 4$, $\{N_j = 1\}_{j=1}^4$, $\varepsilon = 0.3$. (a) Average secrecy rate versus $P_{\max}$ with $M = 10$; (b) Average secrecy rate versus M with $P_{\max} = 0$ dBm.

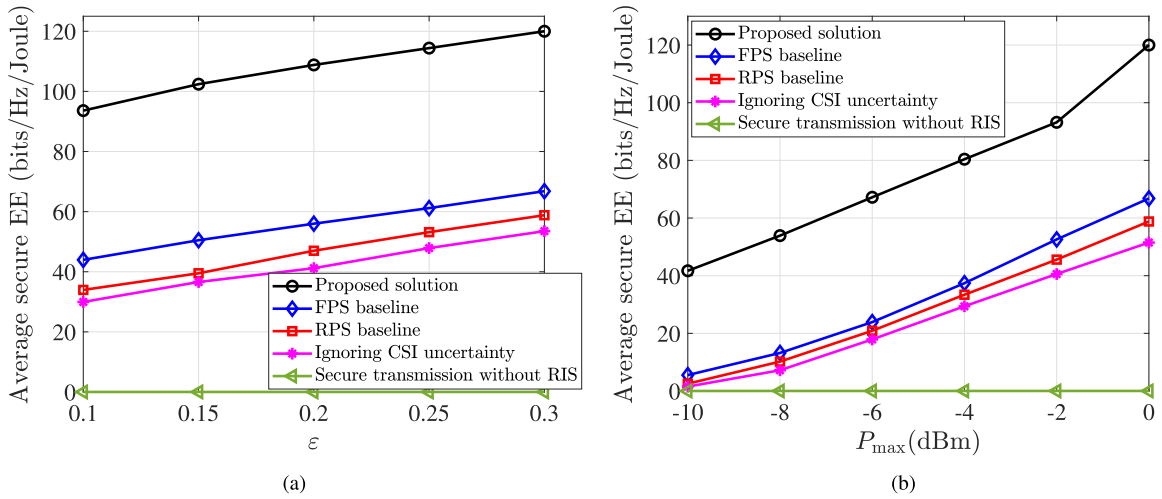


Fig. 8. Comparison with other RIS schemes with $N = 64$, $M = 10$, $K = 2$, $J = 4$, $\{N_j = 4\}_{j=1}^{4}$. (a) Average secure EE versus ε with $P_{\max} = 0$ dBm; (b) Average secure EE versus $P_{\max}$ with $\varepsilon = 0.3$.

complexity order of $\mathcal{O}\left(\mathcal{T}(M^3 + \mathcal{I}_1\mathcal{I}_2N^{3.5})\right)$;

4) Secure transmission without RIS: This scheme has a complexity order of $\mathcal{O}\left(\mathcal{I}_1\mathcal{I}_2N^{3.5}\right)$.

In Fig. 8(a), we demonstrate the impact of the maximum tolerable SOP parameter ε on the secure transmission performance. It can be seen that all average secure EEs increase with ε, but the proposed solution always achieves a significantly higher average secure EE than other baseline schemes. In particular, the FPS scheme enjoys a better performance than the RPS scheme since some optimized phase shift coefficients are quite close to 1. Moreover, for transmission without RIS, due to the strong capability of multi-antenna eavesdroppers, the average secure EEs are almost zero. The simulation results validate that an RIS can significantly improve the secure transmission performance against strong eavesdroppers and even if the outage requirement is stringent (i.e., small ε). Furthermore, it can be seen from Fig. 8(b) that the proposed scheme improves the transmission performance compared to the other RIS schemes under different values of $P_{\max}$, with the performance gaps between the proposed solution and other baseline solutions increasing in $P_{\max}$, indicating that the strategically designed phase shift of RIS can efficiently utilize the transmit power. The results from Fig. 8 show that both the proper handling of uncertain CSI and optimization of phase shift are indispensable in secure transmission.

VI. Conclusion

This paper studied the RIS aided secure networks with multi-antenna Eves and spatially correlated channel uncertainties, and proposed efficient numerical optimization algorithms to maximize the secure EE. To tackle the complicated probabilistic constraint incurred by imperfect CSI and multi-antenna Eves, a novel transformation was established for the first time to transform the probabilistic constraint into a deterministic one and a guideline was established to guarantee no or minimal performance loss. An optimization algorithm was further proposed to determine the transmit covariance matrix, phase-shift design, and redundancy rate. Simulation results demonstrated that due to the tight outage control, the proposed probabilistic constraint transformation leads to substantially higher secure EE than that provided by the conventional BTI safe approximation. Furthermore, compared with other baseline schemes, the resultant scheme can improve the secure transmission performance, showing the importance of proper handling of the outage probabilistic constraint and optimization of RIS phase shifts in secure transmission against multi-antenna eavesdroppers.

Appendix A
Proof of Lemma 1

From [34, Lemma 4], we have

$$\operatorname{rank}\Big((\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)\mathbf{Q} \times (\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)^H/\sigma_j^2\Big) \le \operatorname{rank}(\mathbf{Q}) \tag{36}$$

always holds. Moreover, from constraint (9d), it is known that $\operatorname{rank}(\mathbf{Q}) = 1$. Hence, we have the following equality:

$$\operatorname{rank}\Big((\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)\mathbf{Q} \times (\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)^H/\sigma_j^2\Big) = 1. \tag{37}$$

On the other hand, for the identity matrix $\mathbf{I}_{N_j}$ and a matrix $\mathbf{X} \in \mathbb{C}^{N_j \times N_j}$, it is known that

$$\det\left(\mathbf{I}_{N_j} + \mathbf{X}\right) \ge 1 + \operatorname{Tr}(\mathbf{X}) \tag{38}$$

with the equality holds when $\mathrm{rank}(\mathbf{X}) = 1$. Together with (37), we have

$$\begin{aligned}\det\Bigg(&\mathbf{I}_{N_j} + (\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)\mathbf{Q} \\ &\times (\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)^H/\sigma_j^2\Bigg) \\ &= 1 + \mathrm{Tr}\Bigg(\left(\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H\right)\mathbf{Q} \\ &\times \left(\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H\right)^H/\sigma_j^2\Bigg). \end{aligned} \tag{39}$$

Then, the SOP constraint in (13) can be equivalently transformed into

$$\begin{aligned}p_{so}^{k,j} &= \Pr\Bigg\{(2^{D_{k,j}}-1)\sigma_j^2 < \mathrm{Tr}\Big((\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)\mathbf{Q} \\ &\quad\times (\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H} + \sqrt{\beta_j}\mathbf{W}_j^H)^H\Big)\Bigg\} \\ &= \Pr\left\{(2^{D_{k,j}}-1)\sigma_j^2 < \mathrm{Tr}\left(\mathbf{X}_1+\mathbf{X}_2+\mathbf{X}_3+\mathbf{X}_4\right)\right\} \le \varepsilon, \end{aligned} \tag{40}$$

where $\mathbf{X}_1 = \alpha_j\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Theta}\mathbf{H})^H\mathbf{G}_j$, $\mathbf{X}_2 = \sqrt{\alpha_j\beta_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H}\mathbf{Q}\mathbf{W}_j$, $\mathbf{X}_3 = \sqrt{\alpha_j\beta_j}\mathbf{W}_j^H\mathbf{Q}(\mathbf{\Theta}\mathbf{H})^H\mathbf{G}_j$ and $\mathbf{X}_4 = \beta_j\mathbf{W}_j^H\mathbf{Q}\mathbf{W}_j$. Given $\mathrm{vec}(\mathbf{G}_j) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_j}\otimes\mathbf{\Sigma}_{\mathrm{RIS}})$, we have

$$\mathrm{vec}(\mathbf{G}_j) = \left(\mathbf{I}_{N_j}\otimes\mathbf{\Sigma}_{\mathrm{RIS}}\right)^{\frac{1}{2}}\mathrm{vec}(\tilde{\mathbf{G}}_j), \tag{41}$$

where $\mathrm{vec}(\tilde{\mathbf{G}}_j) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{MN_j})$. By leveraging the matrix identities and (41), $\mathrm{Tr}(\mathbf{X}_1)$, $\mathrm{Tr}(\mathbf{X}_2)$, $\mathrm{Tr}(\mathbf{X}_3)$ and $\mathrm{Tr}(\mathbf{X}_4)$ in (40) can be respectively given by

$$\begin{aligned}\mathrm{Tr}(\mathbf{X}_1) &= \mathrm{vec}(\tilde{\mathbf{G}}_j)^H(\alpha_j\mathbf{I}_{N_j}\otimes(\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H)) \\ &\quad\times\mathrm{vec}(\tilde{\mathbf{G}}_j), \end{aligned} \tag{42}$$

$$\mathrm{Tr}(\mathbf{X}_2) = \mathrm{vec}(\tilde{\mathbf{G}}_j)^H(\sqrt{\alpha_j\beta_j}\mathbf{I}_{N_j}\otimes\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q})\mathrm{vec}(\mathbf{W}_j), \tag{43}$$

$$\mathrm{Tr}(\mathbf{X}_3) = \mathrm{vec}(\mathbf{W}_j)^H(\sqrt{\alpha_j\beta_j}\mathbf{I}_{N_j}\otimes\mathbf{Q}(\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H)\mathrm{vec}(\tilde{\mathbf{G}}_j), \tag{44}$$

$$\mathrm{Tr}(\mathbf{X}_4) = \mathrm{vec}(\mathbf{W}_j)^H(\beta_j\mathbf{I}_{N_j}\otimes\mathbf{Q})\mathrm{vec}(\mathbf{W}_j). \tag{45}$$

Based on (42)-(45), we can rewrite (40) as

$$\begin{aligned}p_{so}^{k,j} = \Pr\Bigg\{&(2^{D_{k,j}}-1)\sigma_j^2 < \left[\mathrm{vec}(\tilde{\mathbf{G}}_j)^H, \mathrm{vec}(\mathbf{W}_j)^H\right] \\ &\times\mathbf{\Omega}_j\left[\mathrm{vec}(\tilde{\mathbf{G}}_j)^H, \mathrm{vec}(\mathbf{W}_j)^H\right]^H\Bigg\} \le \varepsilon, \end{aligned} \tag{46}$$

where matrix $\mathbf{\Omega}_j$ is given by (47), shown at the top of the next page. To derive a closed-form expression of (46), we first reveal the following properties.

Lemma 3. *$\mathrm{rank}(\mathbf{\Omega}_j) = N_j$ with all N_j non-zero eigenvalues being λ_1, where $\lambda_1 = \mathrm{Tr}(\mathbf{X})$ with $\mathbf{X} = \begin{bmatrix}\alpha_j(\mathbf{\Sigma}_{RIS}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Sigma}_{RIS}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H) & \sqrt{\alpha_j\beta_j}\mathbf{\Sigma}_{RIS}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q} \\ \sqrt{\alpha_j\beta_j}\mathbf{Q}(\mathbf{\Sigma}_{RIS}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H & \beta_j\mathbf{Q}\end{bmatrix}_{(M+N)\times(M+N)}$.*

Proof. First, we decompose $\mathbf{X} = \begin{bmatrix}\sqrt{\alpha_j}\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{q} \\ \sqrt{\beta_j}\mathbf{q}\end{bmatrix}\begin{bmatrix}\sqrt{\alpha_j}\mathbf{q}^H(\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H & \sqrt{\beta_j}\mathbf{q}^H\end{bmatrix}$ with $\mathbf{Q} = \mathbf{q}\mathbf{q}^H$. Since $\mathbf{q} \in \mathbb{C}^{N\times 1}$ is a column vector and $\mathbf{X}$ is the outer product of two vectors, $\mathrm{rank}(\mathbf{X}) = 1$ always holds. Therefore, we have $\mathrm{Tr}(\mathbf{X}) = \lambda_1$ with the non-zero eigenvalue of $\mathbf{X}$ being λ_1.

On the other hand, notice that matrix $\mathbf{\Omega}_j$ can be rewritten as

$$\begin{aligned}\mathbf{\Omega}_j &= \\ &\begin{bmatrix}\alpha_j(\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H) & \sqrt{\alpha_j\beta_j}\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q} \\ \sqrt{\alpha_j\beta_j}\mathbf{Q}(\mathbf{\Sigma}_{\mathrm{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H & \beta_j\mathbf{Q}\end{bmatrix}\otimes\mathbf{I}_{N_j} \\ &= \mathbf{X}\otimes\mathbf{I}_{N_j}. \end{aligned} \tag{48}$$

Based on the property of Kronecker product [15], we have $\mathrm{rank}(\mathbf{\Omega}_j) = N_j$ with all N_j non-zero eigenvalues being λ_1. □

Based on Lemma 3, $\mathbf{\Omega}_j$ can be diagonalized with a unitary matrix $\mathbf{P} \in \mathbb{C}^{(N+M)N_j\times(N+M)N_j}$ and expressed as

$$\mathbf{P}^H\mathbf{\Omega}_j\mathbf{P} = \begin{bmatrix}\lambda_1\mathbf{I}_{N_j} & \mathbf{0} \\ \mathbf{0} & \mathbf{0}\end{bmatrix}_{(N+M)N_j\times(N+M)N_j}. \tag{49}$$

Based on (49), we have

$$\begin{aligned}&\left[\mathrm{vec}(\tilde{\mathbf{G}}_j)^H, \mathrm{vec}(\mathbf{W}_j)^H\right]\mathbf{\Omega}_j\left[\mathrm{vec}(\tilde{\mathbf{G}}_j)^H, \mathrm{vec}(\mathbf{W}_j)^H\right]^H \\ &= \mathbf{v}^H\begin{bmatrix}\lambda_1\mathbf{I}_{N_j} & \mathbf{0} \\ \mathbf{0} & \mathbf{0}\end{bmatrix}\mathbf{v} = \lambda_1\sum_{i=1}^{N_j}{v_i}^2, \end{aligned} \tag{50}$$

where $\mathbf{v} = \mathbf{P}^H\left[\mathrm{vec}(\tilde{\mathbf{G}}_j)^H, \mathrm{vec}(\mathbf{W}_j)^H\right]^H$, and v_i is the i^{th} element of $\mathbf{v}$. By putting (50) into the inner part of (46), we have

$$p_{so}^{k,j} = \Pr\left\{\frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1} < \sum_{i=1}^{N_j}{v_i}^2\right\} \le \varepsilon. \tag{51}$$

Due to the fact that $\mathbf{P}$ is a unitary matrix, and $\left[\mathrm{vec}(\tilde{\mathbf{G}}_j)^H, \mathrm{vec}(\mathbf{W}_j)^H\right]^H \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{(N+M)N_j})$, $\mathbf{v} = \mathbf{P}^H\left[\mathrm{vec}(\tilde{\mathbf{G}}_j)^H, \mathrm{vec}(\mathbf{W}_j)^H\right]^H \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{(N+M)N_j})$ too. Therefore, $v_i \sim \mathcal{CN}(0,1)$ such that $v_i^2 \sim \mathrm{Exp}(1)$, and $\sum_{i=1}^{N_j}{v_i}^2 \sim \mathcal{G}(N_j, 1)$, which is the gamma distribution with shape N_j and scale 1. Notice that $p_{so}^{k,j}$ is expressed in the cumulative distribution function (CDF) of $\sum_{i=1}^{N_j}{v_i}^2$. A closed-form deterministic constraint of (51) can be derived as

$$\begin{aligned}p_{so}^{k,j} &= \Pr\left\{\frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1} < \sum_{i=1}^{N_j}{v_i}^2\right\} \\ &= 1 - \frac{1}{(N_j-1)!}\int_0^{\frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1}} t^{N_j-1}e^{-t}\mathrm{d}t \\ &= \frac{\gamma\left(N_j, \frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1}\right)}{(N_j-1)!} \le \varepsilon. \end{aligned} \tag{52}$$

$$\mathbf{\Omega}_j = \begin{bmatrix} \alpha_j \mathbf{I}_{N_j} \otimes (\mathbf{\Sigma}_{\text{RIS}}^{\frac{1}{2}} \mathbf{\Theta} \mathbf{H} \mathbf{Q} (\mathbf{\Sigma}_{\text{RIS}}^{\frac{1}{2}} \mathbf{\Theta} \mathbf{H})^H) & \sqrt{\alpha_j \beta_j} \mathbf{I}_{N_j} \otimes \mathbf{\Sigma}_{\text{RIS}}^{\frac{1}{2}} \mathbf{\Theta} \mathbf{H} \mathbf{Q} \\ \sqrt{\alpha_j \beta_j} \mathbf{I}_{N_j} \otimes \mathbf{Q} (\mathbf{\Sigma}_{\text{RIS}}^{\frac{1}{2}} \mathbf{\Theta} \mathbf{H})^H & \beta_j \mathbf{I}_{N_j} \otimes \mathbf{Q} \end{bmatrix} \tag{47}$$

Appendix B
Proof of Theorem 1

At the beginning, we provide the following property with respect to constraint (14).

Lemma 4. *If* $\varepsilon \leq \frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!}$ *with* $\mu_{k,j} \in (0,1]$, *the constraint in* (14) *is a tighter constraint than* (15).

Proof. Since $\varepsilon \leq \frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!}$, together with the constraint (14), we have

$$\frac{\gamma\left(N_j, \frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1}\right)}{(N_j-1)!} \leq \frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!}. \tag{53}$$

It is known that the upper incomplete gamma function $\gamma(y,x) = \int_x^\infty t^{y-1}e^{-t}\text{dt}$ is decreasing in x [41]. Hence, we can obtain the following inequality based on (53):

$$\frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1} \geq N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right). \tag{54}$$

Furthermore, from [34, Lemma 4], we have

$$\text{rank}\left((\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H}+\sqrt{\beta_j}\mathbf{W}_j^H)\mathbf{Q} \times (\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H}+\sqrt{\beta_j}\mathbf{W}_j^H)^H/\sigma_j^2\right) \leq \text{rank}(\mathbf{Q}) \tag{55}$$

always holds. Since it is known that $\text{rank}(\mathbf{Q}) = 1$ from the constraint (9d), we have

$$\text{rank}\left((\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H}+\sqrt{\beta_j}\mathbf{W}_j^H)\mathbf{Q} \times (\sqrt{\alpha_j}\mathbf{G}_j^H\mathbf{\Theta}\mathbf{H}+\sqrt{\beta_j}\mathbf{W}_j^H)^H/\sigma_j^2\right) = 1. \tag{56}$$

From Lemma 1, it is known that λ_1 is the largest eigenvalue of matrix $\mathbf{\Omega}_j = \mathbf{X} \otimes \mathbf{I}_{N_j}$ and $\lambda_1 = \text{Tr}(\mathbf{X})$ with $\mathbf{X} = \begin{bmatrix} \alpha_j(\mathbf{\Sigma}_{\text{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Sigma}_{\text{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H) & \sqrt{\alpha_j\beta_j}\mathbf{\Sigma}_{\text{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q} \\ \sqrt{\alpha_j\beta_j}\mathbf{Q}(\mathbf{\Sigma}_{\text{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H & \beta_j\mathbf{Q} \end{bmatrix}$. Hence, we have

$$\text{Tr}\left(\alpha_j\mathbf{\Sigma}_{\text{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Sigma}_{\text{RIS}}^{\frac{1}{2}}\mathbf{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q}\right) = \text{Tr}\left(\alpha_j\mathbf{\Sigma}_{\text{RIS}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q}\right) = \lambda_1. \tag{57}$$

Applying (57) into (54), we can obtain

$$\frac{(2^{D_{k,j}}-1)\sigma_j^2}{\text{Tr}\left(\alpha_j\mathbf{\Sigma}_{\text{RIS}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q}\right)} \geq N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right). \tag{58}$$

By re-arranging (58), we can obtain the following inequality:

$$D_{k,j} \geq \log_2\left(1+\frac{N_j}{\sigma_j^2}\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right) \times \text{Tr}\left(\alpha_j\mathbf{\Sigma}_{\text{RIS}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q}\right)\right), \tag{59}$$

which is identical to (15). Hence, the constraint (14) is a tighter constraint than the one in (15). □

Then, we provide the following property with respect to the constraint in (15).

Lemma 5. *If* $\varepsilon \geq \frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!}$ *with* $\mu_{k,j} \in (0,1]$, *the constraint* (15) *is a tighter constraint than* (14).

Proof. By re-arranging (15), we can obtain the following inequality:

$$(2^{D_{k,j}}-1)\sigma_j^2 \geq N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right) \times \text{Tr}\left(\alpha_j\mathbf{\Sigma}_{\text{RIS}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q}\right). \tag{60}$$

By substituting $\text{Tr}\left(\alpha_j\mathbf{\Sigma}_{\text{RIS}}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q}\right)$ of (57) into (60), we obtain

$$\frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1} \geq N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right). \tag{61}$$

It is known that the upper incomplete gamma function $\gamma(y,x) = \int_x^\infty t^{y-1}e^{-t}\text{dt}$ is decreasing in x [41]. Hence, we can obtain the following inequality based on (61):

$$\frac{\gamma\left(N_j, \frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1}\right)}{(N_j-1)!} \leq \frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!}. \tag{62}$$

Since it is known that $\frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!} \leq \varepsilon$, together with (62), we can conclude that

$$\frac{\gamma\left(N_j, \frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1}\right)}{(N_j-1)!} \leq \varepsilon, \tag{63}$$

which is identical to (14). Therefore, (15) is a tighter constraint than constraint (14). □

Based on Lemma 4 and Lemma 5, we can conclude that constraint (15) is equivalent to constraint (14) if and only if $\varepsilon = \frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!}$ with $\mu_{k,j} \in (0,1]$. Since $\gamma(y,x) = \int_x^{\infty} t^{y-1}e^{-t}\mathrm{d}t$ is decreasing in x [41], and $N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)$ is decreasing in $\mu_{k,j}$, the composite function $\frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!}$ is increasing in $\mu_{k,j} \in (0,1]$. As a result, we have

$$0 < \frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!} \leq \frac{\gamma(N_j,N_j)}{(N_j-1)!}. \tag{64}$$

Since $\varepsilon = \frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!}$, we can conclude that $\varepsilon \in (0, \frac{\gamma(N_j,N_j)}{(N_j-1)!}]$ and the constraint (15) is equivalent to constraint (14) if $\varepsilon \in (0, \frac{\gamma(N_j,N_j)}{(N_j-1)!}]$.

On the other hand, if $\varepsilon \in (\frac{\gamma(N_j,N_j)}{(N_j-1)!}, 1]$, together with (64), $\varepsilon \geq \frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!}$ always holds. According to Lemma 5, constraint (15) is a tighter constraint than the one in (14).

Appendix C
Proof of Lemma 2

By substituting $D_{k,j}^{\diamond}$ of (17) into (14), $p_{so}^{k,j}$ is rewritten as (65), shown at the top of the next page, where (66) is obtained by substituting (57) into (65). Since the upper incomplete gamma function $\gamma(y,x) = \int_x^{\infty} t^{y-1}e^{-t}\mathrm{d}t$ is decreasing in x [41], and $N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)$ is decreasing in $\mu_{k,j}$, $p_{\mathrm{so}}^{k,j}(\mu_{k,j})$ is increasing in $\mu_{k,j} \in (0,1]$. Since it is known that $p_{\mathrm{so}}^{k,j}(0) = 0$ and $p_{\mathrm{so}}^{k,j}(1) = \frac{\gamma(N_j,N_j)}{(N_j-1)!}$, $p_{\mathrm{so}}^{k,j}(\mu_{k,j}) \in (0, \frac{\gamma(N_j,N_j)}{(N_j-1)!}]$. If $\varepsilon > \frac{\gamma(N_j,N_j)}{(N_j-1)!}$, we have $p_{\mathrm{so}}^{k,j}(\mu_{k,j}) < \varepsilon$, and setting $\mu_{k,j} = 1$ could make $p_{\mathrm{so}}^{k,j}(\mu_{k,j})$ be closest to ε.

On the other hand, it is known that the objective function of (9) is a monotonic function with respect to $D_{k,j}$ and hence maximizing (9) is equivalent to minimizing $D_{k,j}$. Since the upper incomplete Gamma function $\gamma(y,x) = \int_x^{\infty} t^{y-1}e^{-t}\mathrm{d}t$ decreases in x [41] and $\frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1}$ increases in $D_{k,j}$, the composite function $\frac{\gamma\left(N_j, \frac{(2^{D_{k,j}}-1)\sigma_j^2}{\lambda_1}\right)}{(N_j-1)!}$ decreases in $D_{k,j}$. Together with constraint (14), the optimal $D_{k,j}^*$ of optimization problem (9) satisfies

$$p_{\mathrm{so}}^{k,j} = \frac{\gamma\left(N_j, \frac{(2^{D_{k,j}^*}-1)\sigma_j^2}{\lambda_1}\right)}{(N_j-1)!} = \varepsilon. \tag{67}$$

Hence, to make $D_{k,j}^{\diamond}$ be the closest to $D_{k,j}^*$, we should select proper $\mu_{k,j}$ such that $p_{\mathrm{so}}^{k,j}(\mu_{k,j})$ be closest to ε. This happens when $\mu_{k,j} = 1$, and the corresponding $D_{k,j}^{\diamond}$ would be the closest solution to the optimal solution of (9).

Appendix D
Proof of Theorem 2

The Lagrangian function of problem (35) is given by

$$\mathcal{L}(\mathbf{Q},\mathbf{\Lambda},\zeta) = -\Phi^{(n)}(\mathbf{Q}) + \zeta(\mathrm{Tr}(\mathbf{Q}) - P_{\max}) - \mathrm{Tr}(\mathbf{\Lambda Q}), \tag{68}$$

where $\Phi^{(n)}(\mathbf{Q})$ is given by

$$\Phi^{(n)}(\mathbf{Q}) = \hat{\Gamma}(\mathbf{Q};\mathbf{Q}^{(n)}) - \psi_l\left(\frac{1}{\eta}\mathrm{Tr}(\mathbf{Q}) + P_a + KP_c + M(P_s + P_e/T_f)\right). \tag{69}$$

$\mathbf{\Lambda} \in \mathbb{C}_+^{N\times N}$ and $\zeta \geq 0$ are the dual variables for constraints in problem (35). Then, the optimal solutions of (35) must satisfy the following KKT conditions:

$$\begin{cases} \nabla\Phi^{(n)}(\mathbf{Q}) + \mathbf{\Lambda} = \zeta\mathbf{I}_N, \\ \mathbf{\Lambda Q} = \mathbf{0}, \quad \mathbf{\Lambda} \succeq \mathbf{0}, \\ \mathrm{Tr}(\mathbf{Q}) - P_{\max} \leq 0, \ \zeta \geq 0, \end{cases} \tag{70}$$

where the gradient of $\Phi^{(n)}(\mathbf{Q})$ is derived as

$$\nabla\Phi^{(n)} = \frac{(\mathbf{h}_k^H\mathbf{\Theta H})^H(\mathbf{h}_k^H\mathbf{\Theta H})}{(\sigma_k^2/\alpha_k + (\mathbf{h}_k^H\mathbf{\Theta H})\mathbf{Q}(\mathbf{h}_k^H\mathbf{\Theta H})^H)\ln 2} - \frac{\frac{N_j\xi_{k,j}}{\sigma_j^2}(\alpha_j\mathbf{H}^H\mathbf{\Sigma}_{\mathrm{RIS}}\mathbf{H} + \beta_j\mathbf{I}_N)}{\left(1+\frac{N_j\xi_{k,j}}{\sigma_j^2}\mathrm{Tr}\left(\alpha_j\mathbf{HQ}^{(n)}\mathbf{H}^H\mathbf{\Sigma}_{\mathrm{RIS}} + \beta_j\mathbf{Q}^{(n)}\right)\right)\ln 2} - \frac{\psi_l}{\eta}\mathbf{I}_N. \tag{71}$$

Based on the KKT conditions, the optimal primal variable $\mathbf{Q}^{\diamond}$, and dual variables $\{\mathbf{\Lambda}^{\diamond}, \zeta^{\diamond}\}$ should satisfy

$$\mathbf{\Lambda}^{\diamond} = \left(\zeta^{\diamond} + \frac{\psi_l}{\eta}\right)\mathbf{I}_N - \frac{(\mathbf{h}_k^H\mathbf{\Theta H})^H(\mathbf{h}_k^H\mathbf{\Theta H})}{\left(\frac{\sigma_k^2}{\alpha_k} + (\mathbf{h}_k^H\mathbf{\Theta H})\mathbf{Q}^{\diamond}(\mathbf{h}_k^H\mathbf{\Theta H})^H\right)\ln 2} + \frac{\frac{N_j\xi_{k,j}}{\sigma_j^2}(\alpha_j\mathbf{H}^H\mathbf{\Sigma}_{\mathrm{RIS}}\mathbf{H} + \beta_j\mathbf{I}_N)}{\left(1+\frac{N_j\xi_{k,j}}{\sigma_j^2}\mathrm{Tr}\left(\alpha_j\mathbf{HQ}^{(n)}\mathbf{H}^H\mathbf{\Sigma}_{\mathrm{RIS}} + \beta_j\mathbf{Q}^{(n)}\right)\right)\ln 2}. \tag{72}$$

By putting $\mathbf{\Lambda}^{\diamond}$ into condition $\mathbf{\Lambda Q} = \mathbf{0}$ of (70), the optimal $\mathbf{Q}^{\diamond}$ must satisfy

$$\frac{(\mathbf{h}_k^H\mathbf{\Theta H})^H(\mathbf{h}_k^H\mathbf{\Theta H})}{(\sigma_k^2/\alpha_k + (\mathbf{h}_k^H\mathbf{\Theta H})\mathbf{Q}^{\diamond}(\mathbf{h}_k^H\mathbf{\Theta H})^H)\ln 2}\mathbf{Q}^{\diamond} = \mathbf{B}\mathbf{Q}^{\diamond}, \tag{73}$$

where $\mathbf{B}$ is given by

$$\mathbf{B} = \left(\zeta^{\diamond} + \frac{\psi_l}{\eta}\right)\mathbf{I}_N + \frac{\frac{N_j\xi_{k,j}}{\sigma_j^2}(\alpha_j\mathbf{H}^H\mathbf{\Sigma}_{\mathrm{RIS}}\mathbf{H} + \beta_j\mathbf{I}_N)}{\left(1+\frac{N_j\xi_{k,j}}{\sigma_j^2}\mathrm{Tr}\left(\alpha_j\mathbf{HQ}^{(n)}\mathbf{H}^H\mathbf{\Sigma}_{\mathrm{RIS}} + \beta_j\mathbf{Q}^{(n)}\right)\right)\ln 2}. \tag{74}$$

Notice that matrix $\mathbf{B}$ of (74) is invertible. As a result, (73) can be rewritten as

$$\mathbf{Q}^{\diamond} = \mathbf{B}^{-1}\frac{(\mathbf{h}_k^H\mathbf{\Theta H})^H(\mathbf{h}_k^H\mathbf{\Theta H})}{(\sigma_k^2/\alpha_k + (\mathbf{h}_k^H\mathbf{\Theta H})\mathbf{Q}^{\diamond}(\mathbf{h}_k^H\mathbf{\Theta H})^H)\ln 2}\mathbf{Q}^{\diamond}, \tag{75}$$

$$p_{\rm so}^{k,j}(\mu_{k,j}) = \frac{1}{(N_j-1)!}\gamma\left(N_j, \frac{N_j}{\lambda_1}\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\mathrm{Tr}\left(\alpha_j\mathbf{\Sigma}_{\rm RIS}\mathbf{\Theta}\mathbf{H}\mathbf{Q}(\mathbf{\Theta}\mathbf{H})^H+\beta_j\mathbf{Q}\right)\right) \tag{65}$$

$$= \frac{\gamma\left(N_j, N_j\left(1+\sqrt{2\ln(\mu_{k,j}^{-1})}+\ln(\mu_{k,j}^{-1})\right)\right)}{(N_j-1)!} \tag{66}$$

Then, taking the rank of a matrix on the both sides of (75), we have the following rank relation

$$\begin{aligned}
&\mathrm{rank}(\mathbf{Q}^\diamond)\\
&= \mathrm{rank}\left(\mathbf{B}^{-1}\frac{(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})^H(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})}{(\sigma_k^2/\alpha_k+(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})\mathbf{Q}^\diamond(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})^H)\ln 2}\mathbf{Q}^\diamond\right)\\
&\le \mathrm{rank}\left(\frac{(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})^H(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})}{(\sigma_k^2/\alpha_k+(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})\mathbf{Q}^\diamond(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})^H)\ln 2}\right) \qquad (76)\\
&= \mathrm{rank}\left((\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})^H(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})\right), \qquad (77)
\end{aligned}$$

where (76) follows from [34, Lemma 4].

On the other hand, it is known that $\mathrm{rank}(\mathbf{q}) = \mathrm{rank}(\mathbf{q}\mathbf{q}^H) \le 1$ always holds for $\mathbf{q}\in\mathbb{C}^{N\times 1}$ [42]. By substituting $(\mathbf{h}_k^H\mathbf{\Theta}\mathbf{H})^H = \mathbf{q}$ into (77), we can obtain $\mathrm{rank}(\mathbf{Q}^\diamond)\le 1$. By excluding the trivial solution of $\mathbf{Q}^\diamond = \mathbf{0}$, we can conclude that $\mathrm{rank}(\mathbf{Q}^\diamond) = 1$ holds and then the optimal solution of (35) is always rank-one.

References

[1] X. Yuan, Y.-J. A. Zhang, Y. Shi, W. Yan, and H. Liu, "Reconfigurable-intelligent-surface empowered wireless communications: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 136–143, 2021.

[2] Y. Cao, N. Zhao, Y. Chen, M. Jin, Z. Ding, Y. Li, and F. R. Yu, "Secure transmission via beamforming optimization for NOMA networks," *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 193–199, 2020.

[3] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan, "Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack," *IEEE Wireless Commun.*, vol. 29, no. 3, pp. 131–138, 2022.

[4] X. Lu, W. Yang, X. Guan, Q. Wu, and Y. Cai, "Robust and secure beamforming for intelligent reflecting surface aided mmWave MISO systems," *IEEE Wireless Commun. Lett.*, vol. 9, no. 12, pp. 2068–2071, Dec. 2020.

[5] S. Asaad, Y. Wu, A. Bereyhi, R. R. Müller, R. F. Schaefer, and H. V. Poor, "Secure active and passive beamforming in IRS-aided MIMO systems," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 1300–1315, 2022.

[6] S. Hong, C. Pan, H. Ren, K. Wang, K. K. Chai, and A. Nallanathan, "Robust transmission design for intelligent reflecting surface-aided secure communication systems with imperfect cascaded CSI," *IEEE Trans. Wireless Commun.*, vol. 20, no. 4, pp. 2487–2501, 2021.

[7] L. You, J. Xiong, Y. Huang, D. W. K. Ng, C. Pan, W. Wang, and X. Gao, "Reconfigurable intelligent surfaces-assisted multiuser MIMO uplink transmission with partial CSI," *IEEE Trans. Wireless Commun.*, vol. 20, no. 9, pp. 5613–5627, Sep. 2021.

[8] Z. Li, S. Wang, M. Wen, and Y.-C. Wu, "Secure multicast energy-efficiency maximization with massive RISs and uncertain CSI: First-order algorithms and convergence analysis," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 6818–6833, Sep. 2022.

[9] S. Hu, Z. Wei, Y. Cai, C. Liu, D. W. K. Ng, and J. Yuan, "Robust and secure sum-rate maximization for multiuser MISO downlink systems with self-sustainable IRS," *IEEE Trans. Commun.*, vol. 69, no. 10, pp. 7032–7049, 2021.

[10] W. Hao, J. Li, G. Sun, C. Huang, M. Zeng, O. A. Dobre, and C. Yuen, "Robust security energy efficiency optimization for RIS-aided cell-free networks with multiple eavesdroppers," *arXiv: 2211.05562*, Nov. 2022.

[11] L. Dong and H.-M. Wang, "Enhancing secure MIMO transmission via intelligent reflecting surface," *IEEE Trans. Wireless Commun.*, vol. 19, no. 11, pp. 7543–7556, 2020.

[12] 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," *Digital Communications and Networks*, 2022.

[13] A. Bereyhi, S. Asaad, C. Ouyang, R. R. Müller, R. F. Schaefer, and H. V. Poor, "Channel hardening of IRS-aided multi-antenna systems: How should IRSs scale?" *IEEE J. Sel. Areas Commun.*, vol. 41, no. 8, pp. 2321–2335, 2023.

[14] E. Björnson and L. Sanguinetti, "Rayleigh fading modeling and channel hardening for reconfigurable intelligent surfaces," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 830–834, Apr. 2021.

[15] M. Taboga, "Properties of the kronecker product," *Lectures on matrix algebra*, 2021.

[16] A. Jeffrey and D. Zwillinger, *Table of Integrals, Series, and Products (6th ed.)*. San Diego, USA: Academic Press, 2000.

[17] J. Luedtke and S. Ahmed, "A sample approximation approach for optimization with probabilistic constraints," *SIAM J. Optim.*, vol. 19, no. 2, pp. 674–26, 2008.

[18] A. Beck and M. Teboulle, *Gradient-based Algorithms with Applications to Signal Recovery Problems*. Cambridge University Press, 2009, pp. 42–88.

[19] L. An and P. Tao, "The DC (difference of convex functions) programming and DCA revisited with DC models of real world nonconvex optimization problems," *Ann. Oper. Res.*, vol. 133, no. 1-4, pp. 23–46, 2005.

[20] W. Gautschi, "A computational procedure for incomplete Gamma functions," *ACM Transactions on Mathematical Software*, vol. 5, no. 4, pp. 466–481, 1979.

[21] E. Garro, M. Fuentes, J. L. Carcel, H. Chen, D. Mi, F. Tesema, J. J. Gimenez, and D. Gomez-Barquero, "5G mixed mode: Nr multicast-broadcast services," *IEEE Trans. Broadcast.*, vol. 66, no. 2, pp. 390–403, 2020.

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

[23] 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.

[24] L. Hu, G. Li, X. Qian, A. Hu, and D. W. K. Ng, "Reconfigurable intelligent surface-assisted secret key generation in spatially correlated channels," *arXiv:2211.03132*, 2022.

[25] Z. Li, S. Wang, P. Mu, and Y. Wu, "Probabilistic constrained secure transmissions: Variable-rate design and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2543–2557, Apr. 2020.

[26] X. Liu, F. Gao, G. Wang, and X. Wang, "Joint beamforming and user selection in multicast downlink channel under secrecy-outage constraint," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 82–85, Jan. 2014.

[27] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.

[28] K. Ntontin, A. A. Boulogeorgos, E. Björnson, W. A. Martins, S. Kisseleff, S. Abadal, E. Alarcón, A. Papazafeiropoulos, F. I. Lazarakis, and S. Chatzinotas, "Wireless energy harvesting for autonomous reconfigurable intelligent surfaces," *IEEE Trans. Green Commun. Netw.*, vol. 7, no. 1, pp. 114–129, 2023.

[29] T. Zheng, H. Wang, and J. Yuan, "Secure and energy-efficient transmissions in cache-enabled heterogeneous cellular networks: Performance analysis and optimization," *IEEE Trans. Commun.*, vol. 66, no. 11, pp. 5554–5567, Nov. 2018.

[30] M. El-Halabi, T. Liu, C. N. Georghiades, and S. Shamai, "Secret writing

on dirty paper: A deterministic view," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3419–3429, 2012.

[31] I. Bechar, "A Bernstein-type inequality for stochastic processes of quadratic forms of Gaussian variables," *2009 [Online]. Available: http://arxiv.org/abs/0909.3595*, 2009.

[32] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Robust outage secrecy rate optimizations for a MIMO secrecy channel," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 86–89, 2015.

[33] Z. Li, S. Wang, Q. Lin, Y. Li, M. Wen, Y.-C. Wu, and H. V. Poor, "Phase shift design in RIS empowered wireless networks: From optimization to AI-based methods," *Network*, vol. 2, no. 3, pp. 398–418, 2022.

[34] Y. Tian, "Equalities and inequalities for ranks of products of generalized inverses of two matrices and their applications," *Journal of Inequalities and Applications*, vol. 2016, no. 1, pp. 1–51, 2016.

[35] T. Lipp and S. Boyd, "Variations and extension of the convex–concave procedure," *Optim. Eng.*, vol. 17, no. 2, pp. 263–287, Jun. 2016.

[36] W. Dinkelbach, "On nonlinear fractional programming," *Manage. Sci.*, vol. 13, no. 7, pp. 492–498, 1967.

[37] A. Ben-Tal and A. Nemirovski, *Lectures on Modern Convex Optimization: Analysis, Algorithms, and Engineering Applications*. Philadelphia, PA, USA: SIAM, 2001.

[38] I. Polik and T. Terlaky, *Interior Point Methods for Nonlinear Optimization*. Springer, 2010.

[39] 3GPP, "Evolved universal terrestrial radio access (E-UTRA): User equipment (UE) radio transmission and reception," 3rd Generation Partnership Project (3GPP), TS 36.101, Apr. 2023.

[40] J. B. Andersen, T. S. Rappaport, and S. Yoshida, "Propagation measurements and models for wireless communications channels," *IEEE Commun. Mag.*, vol. 33, no. 1, pp. 42–49, 1995.

[41] G. J. O. Jameson, "The incomplete Gamma functions," *The Mathematical Gazette*, vol. 100, no. 548, pp. 298–306, 2016.

[42] S. Banerjee and A. Roy, *Linear Algebra and Matrix Analysis for Statistics*. New York: Chapman and Hall/CRC, 2014.