Securing Intelligent Reflecting Surface Assisted Terahertz Systems

Jingping Qiao, *Member, IEEE*, Chuanting Zhang, *Member, IEEE*, Anming Dong, *Member, IEEE*, Ji Bian, *Member, IEEE*, and Mohamed-Slim Alouini, *Fellow, IEEE*

***Abstract*—This paper focuses on securing confidential communication in multiple intelligent reflecting surfaces (IRS) assisted terahertz (THz) systems, where a potential eavesdropper can intercept either the base station (BS)-IRS link or the IRS-user link. Notably, the secure transmission may be intercepted and blocked by the eavesdropper due to the blockage-prone nature in THz bands. To characterize the blocking effects of the eavesdropper, the blocking-based path loss is first investigated. With the imperfect eavesdropper channel state information (ECSI), the worst-case secrecy rate (WCSR) is derived, and a joint optimization problem of hybrid beamforming at the BS and reflecting beamforming at the IRS is formulated. For the BS-IRS link eavesdropping, the zero-forcing (ZF) principle-based hybrid beamforming and the closed-form phase shifts of multiple IRSs are respectively proposed. For the IRS-user link eavesdropping, an iterative algorithm is proposed to tackle the non-convex optimization problem with a given information leakage threshold. Finally, a robust secure transmission strategy for multi-eavesdropper systems is further investigated. Simulation results demonstrate that compared with blockage-unaware scenarios, our proposed scheme can resist the adverse effects of the blockage-prone nature of THz waves on information security, and significantly boost secrecy performance.**

***Index Terms*—Blocking eavesdropper, imperfect channel state information, multiple intelligent reflecting surfaces, physical layer security, terahertz communications.**

Manuscript received 20 September 2021; revised 1 March 2022; accepted 2 May 2022. Date of publication 5 May 2022; date of current version 15 August 2022. This work was supported in part by the National Natural Science Foundation of China under Grants 61901247, 61701269, and 62101311, in part by the Natural Science Foundation of Shandong Province of China under Grants ZR2019BF032 and ZR2020QF001, and in part by the KAUST Office of Sponsored Research . The review of this article was coordinated by Dr. Raghunandan M Rao. (*Corresponding authors: Jingping Qiao; Chuanting Zhang.*)

Jingping Qiao is with the Department of Electrical & Electronic Engineering, University of Bristol, Bristol BS8 1QU, UK, and also with the Computer, Electrical and Mathematical Science and Engineering Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia (e-mail: qiaojingping07@gmail.com).

Chuanting Zhang is with the Department of Electrical and Electronic Engineering, University of Bristol, Bristol, Bristol BS8 1QU, U.K. and was with the Computer, Electrical and Mathematical Science and Engineering Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia (e-mail: chuanting.zhang@bristol.ac.uk).

Anming Dong is with the Big Data Institute & School of Mathematics and Statistics, Qilu University of Technology, Jinan 250353, China (e-mail: anmingdong@qlu.edu.cn).

Ji Bian is with the School of Information Science and Engineering, Shandong Normal University, Jinan 250358, China (e-mail: jibian@sdnu.edu.cn).

Mohamed-Slim Alouini is with the Computer, Electrical and Mathematical Science and Engineering Division, King Abdullah University of Science and Technology, Thuwal 23955-6900, Saudi Arabia (e-mail: slim.alouini@kaust.edu.sa).

Digital Object Identifier 10.1109/TVT.2022.3172763

I. Introduction

With wide frequency band, terahertz (THz) transmission enables terabit/second (Tbps) data-rate communications, and is envisioned as a promising wireless technology for the future sixth-generation (6 G) networks [1]–[3]. Compared with microwave communications, THz waves can allow higher link directionality due to the shorter wavelengths, and they are less susceptible to free-space diffraction and inter-antenna interference [4], [5]. Moreover, the narrow beamwidth of THz signals presents a more challenging environment for eavesdropping attacks, thereby enhancing the information security [6]. Nevertheless, THz communications suffer from severe propagation losses and water-molecular absorption, which extremely restricts its transmission distance. The presence of random and dynamic obstacles in the propagation environment makes the situation worse since a highly directional and line-of-sight (LoS) dominated THz link is vulnerable to blockages [7]. Thus, new approaches to extend the coverage of THz communications and overcome the blockage issue are urgently needed.

Recently, intelligent reflecting surfaces (IRS) [8], [9] have drawn increasing attention in millimeter wave (mmWave) and THz communications, because of their significant potentials in combating the transmission distance limitation and solving the non-line-of-sight (NLoS) transmission problems [10], [11]. In general, IRS is a uniform planar array consisting of a large number of composite material elements, and each element is able to reflect incident electromagnetic waves independently with an adjustable phase-shift [12]–[14]. Hence, by intelligently adjusting phase-shifts with a preprogrammed controller, the IRS can steer signals towards the desired receivers, thereby enhancing propagation performance [15]. Specifically, a cooperative channel estimation procedure for IRS-empowered THz systems was first developed in [16], and the achievable channel capacity for both IRS-assisted mmWave and THz systems were respectively investigated in [17]–[20]. It is proved that the IRS has a tremendous potential to realize high-frequency communications in the presence of high blockage densities. Based on the above discussion, IRS-assisted THz communication scenarios were further studied, and the active beamforming at the transmitter and passive reflecting beamforming at the IRS were jointly designed for the communication coverage extension [21]–[23]. In addition, [24] introduced the programmable IRS into multi-user THz communication systems, and achieved a great improvement in terms of the sum-rate.

On the other hand, information security is also a critical issue in the next generation networks [25], [26] since the broadcast nature of wireless medium presents a formidable challenge in ensuring simultaneously secure and reliable communications in the presence of adversaries [27], [28]. As the high-directional and narrow-angle broadcasts of THz waves bring inherent benefits to information security, the THz-enabled physical layer security scenarios have attracted considerable attention [29]. Specifically, to reduce the probability of data to be eavesdropped, the secure beamforming and intelligent reflecting beamforming were jointly designed [30]. To suppress blocking effects on secure communications, the IRS-assisted secure transmission schemes were proposed in mmWave and THz band communications [31], [32]. It is proved the secrecy performance can be significantly improved in both LoS and NLoS scenarios.

The above work on IRS-assisted secure THz communication schemes can intelligently use large-scale reflecting elements to achieve superior secrecy performance. However, the introduction of IRS also leads to additional eavesdropping challenges, since both the transmitter to IRS link and the IRS to user link can be attacked by eavesdroppers. Recent work in [30]–[32] either focuses on a single IRS assisted-secure transmission with perfect eavesdropper channel state information (ECSI) or only focuses on the IRS-user link eavesdropping attacks, ignoring simultaneous eavesdropping attacks on multiple links in IRS communication systems. In general, the ECSI is always challenging to be fully obtained due to the untrustworthy behaviors of eavesdroppers and feedback delay or channel estimation errors. Moreover, the extremely narrow beamwidth of THz waves makes the information leakage caused by the imperfect ECSI more intractable. Besides, the benefits of THz waves on physical layer security are limited by their blockage-prone nature. Different from microwave communications, THz waves are naturally prone to blockage by both stationary and mobile objects in the channel, including buildings, walls, or human bodies [33]. Therefore, eavesdroppers in THz systems can intercept confidential information transmission and block partial legitimate communication links, leading to severe secrecy performance loss. However, the impact of blocking eavesdroppers on secure THz communications has not yet been explored.

Motivated by the aforementioned problems, this paper investigates a multi-IRS-assisted secure transmission strategy in THz systems, in which an eavesdropper located within THz beams can both intercept and block confidential signal transmission among the base station (BS)-IRS link and the IRS-user link. To describe the impact of blockage-prone nature of THz waves on secure transmissions, the power loss caused by the eavesdropper's blockage is modeled and included to the confidential transmission channels. Under the imperfect ECSI assumption, the worst-case secrecy rate is defined to measure the secrecy transmission performance. The main objective of this work is to investigate the blocking effects of eavesdroppers on secure transmission in THz systems, and design robust hybrid beamforming and reflecting scheme to degrade the information leakage caused by imperfect ECSI, thereby enhancing secrecy performance for THz communications. Specifically, the main contributions of this paper can be summarized as follows.

- A multi-IRS-assisted secure transmission strategy for THz communications is investigated. Given the blockage-prone nature of THz waves, two types of blocking eavesdropping attacks are introduced and the blocking power loss is modeled.
- The worst-case secrecy rate performance is analyzed with partial ECSI, and a joint optimization problem of hybrid beamforming and reflecting phase shifts is formulated.
- For the BS-IRS link eavesdropping, to tackle the non-convex secrecy rate maximization problem with unit modulus constraints and coupled variables, an alternative method is proposed. The zero-forcing (ZF) principle-based hybrid beamforming and the closed-form phase shifts of multiple IRSs are respectively derived.
- For the IRS-user link eavesdropping, a semidefinite programming (SDP)-based iterative algorithm is proposed to obtain hybrid beamforming and reflecting beamforming solutions iteratively. The convergence of the proposed iterative algorithm is also proved theoretically.
- The robust IRS-empowered secure transmission strategy is extended into multi-eavesdropper systems to resist concurrent BS-IRS link-eavesdropping and IRS-user link-eavesdropping attacks.

The rest of this paper is organized as follows. Section II introduces the system model and formulates the optimization problem. In Section III and Section IV, we respectively propose an alternative method and an iterative algorithm to maximize the secrecy rate performance for BS-IRS link and IRS-user link eavesdropping activities. In Section V, a robust secure transmission strategy is further investigated for IRS-empowered THz systems with multiple eavesdroppers. The simulation results are presented and analyzed in Section VI. Finally, Section VII concludes the paper.

Notations: The bold upper (lower) letters denote matrices (column vectors), and $(\cdot)^H$ denotes the conjugate transpose. $\|\cdot\|$ indicates the L_2 norm of a vector and the $|\cdot|$ means the absolute value. $[a]^+$ denotes $\max(a,0)$, $\angle\mathbf{a}$ denotes the component-wise phase of a complex vector, and diag$\{\mathbf{a}\}$ means a diagonal matrix with its diagonal elements given in the vector $\mathbf{a}$. $\mathcal{CN}(0,\sigma^2)$ represents a circularly symmetric complex Gaussian distribution with zero mean and variance σ^2. $\mathbf{I}_M$ is the identity matrix of size $M\times M$, and $\mathbb{C}^{M\times N}$ represents the space of $M\times N$ complex matrices.

II. System Model and Problem Formulation

Secure transmission for a multi-IRS-assisted THz system is considered in this paper. As shown in Fig. 1, the THz-empowered BS transmits confidential information to its desired user Bob with the assistance of K IRSs, while the direct THz link between them is blocked by the surrounding buildings, trees, or other infrastructures. Here, we assume that the BS and user Bob wish to keep their communication secret from other users. Thus, the idle legitimate user Eve in the same network is regarded as a potential eavesdropper. Considering the blockage-prone nature of THz waves, we assume that Eve located within THz beams

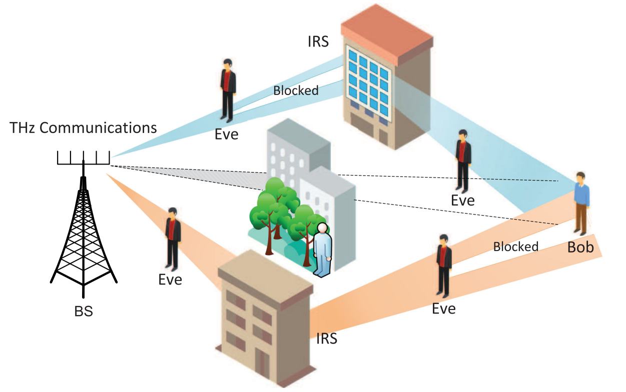


Fig. 1. System model for multi-IRS-assisted THz systems, where BS communicates with user Bob, in the presence of multiple eavesdroppers Eve.

can intercept confidential communications and block a portion of confidential signals.

A. Channel Model

Here we assume that both BS and IRSs are equipped with half-wavelength spaced uniform square planar arrays (USPAs) [34], which respectively consist of M antennas and N reflecting elements. Then, the THz multiple-input and multiple-output (MIMO) channel between the BS and the k-th IRS can be modeled as [35],

$$\mathbf{H}_{BI,k}^{H} = \sqrt{\frac{MN}{L}}\sum_{l=0}^{L}\alpha_{BI}^{l,k}G_r^kG_t^k\mathbf{a}_r(\vartheta_{a,r}^{l,k},\vartheta_{e,r}^{l,k})\mathbf{a}_t(\vartheta_{a,t}^{l,k},\vartheta_{e,t}^{l,k})^H,\forall k, \tag{1}$$

where $k\in\mathcal{K}$, $\mathcal{K}=\{1,2,\ldots,K\}$, and L denotes the number of paths from the BS to the IRS and l indexes the paths. Note that when $l=0$, the corresponding component represents the LoS path. Besides, $\alpha_{BI}^{l,k}$ represents the channel gain of the l-th path for the communication link between the BS and the kth IRS, which simultaneously captures the transmission loss, molecular absorption, and the path loss caused by the blocking eavesdropper. G_r^k and G_t^k are antenna gains at the transceiver. $\mathbf{a}_r(\vartheta_{a,r}^{l,k},\vartheta_{e,r}^{l,k})$ and $\mathbf{a}_t(\vartheta_{a,t}^{l,k},\vartheta_{e,t}^{l,k})$ denote the array steering vector at the transceiver. $\vartheta_{a,r}^{l}(\vartheta_{a,t}^{l,k})$ and $\vartheta_{e,r}^{l,k}(\vartheta_{e,t}^{l,k})$ are the azimuth and elevation angles of arrival and departure (AoA and AoD), respectively.

Due to the space limitation at Bob and Eve, both of them are assumed to be equipped with a single antenna. Thus the IRS-user/Eve channel can be modeled as a multiple-input and single-output (MISO) channel, i.e.,

$$\mathbf{h} = \sqrt{\frac{N}{L}}\sum_{l=0}^{L}\alpha_{IU}^{l,k}G_r^kG_t^k\mathbf{a}_{I,t}(\vartheta_a^{l,k},\vartheta_e^{l,k}),\forall k, \tag{2}$$

where $\mathbf{h}\in\{\mathbf{h}_{D,k},\bar{\mathbf{g}}_{IE}\}$, and $\mathbf{h}=\mathbf{h}_{D,k}$ denotes the IRS-user channel, while $\mathbf{h}=\bar{\mathbf{g}}_{IE}$ denotes the IRS-Eve channel. $\alpha_{IU}^{l,k}$ is the complex gain of the l-th path, $\mathbf{a}_{I,t}(\vartheta_a^{l,k},\vartheta_e^{l,k})$ denotes the array steering vector at the IRS. $\vartheta_a^{l,k}$ and $\vartheta_e^{l,k}$ are the azimuth- and elevation-AoD of the IRS-user/Eve channel.

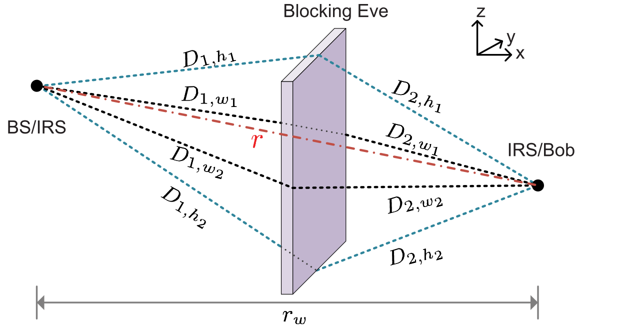


Fig. 2. METIS-based shadowing screen model for blocking Eve.

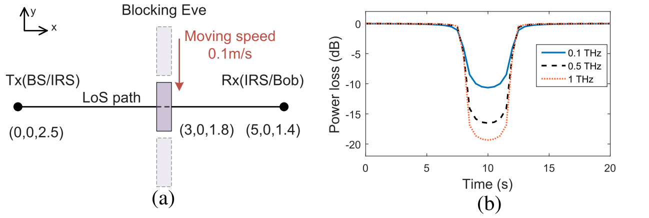


Fig. 3. The power loss versus the moving Eve, in which Eve moves in a direction orthogonal to the Tx/Rx link with a speed of 0.1 m/s. The locations of (Tx, Rx, Eve) are (0,0,2.5), (5,0,1.4), and (3,0,1.8) in meter (m). (a) Location map. (b) Power loss.

1) Blocking-Based Power Loss: Since THz waves are vulnerable to blockage events, eavesdroppers may block confidential communications when located within THz beams. To determine the power loss caused by the blocking eavesdropper, the METIS-based shadowing screen model [36] is adopted. As shown in Fig. 2, treating the blocking eavesdropper as a shadowing screen with the height h and width w, the power loss due to blockage can be modeled as

$$L_b = 1-(F_{h_1}+F_{h_2})(F_{w_1}+F_{w_2}), \tag{3}$$

where F_{h_1}, F_{h_2} and F_{w_1}, F_{w_2} account for knife edge diffraction at the four edges (h_1, h_2, w_1, w_2). The shadowing for a single edge is

$$F_x = \frac{\arctan\left(\frac{\pi}{2}\sqrt{\frac{\pi}{\lambda}(D_{1,x}+D_{2,x}-r)}\right)}{\pi}, \tag{4}$$

in which $x\in\{h_1,h_2,w_1,w_2\}$, and λ denotes the wave length, $D_{1,x}$ and $D_{2,x}$ are the projected distances between the x edge of the screen and communication users, i.e., the projected distance between BS/IRS and blocking eavesdropper or the projected distance between IRS/Bob and blocking eavesdropper. In addition, r is the projected distance between the transceivers (e.g., the BS-to-IRS distance or the IRS-to-user distance).

Aiming to clearly demonstrate the influence of blocking eavesdroppers on signal transmission, we show the power loss L_b in Fig. 3 as the eavesdropper moves orthogonal to the LoS link. From Fig. 3 we can notice that the LoS link suffers from severe power loss when the eavesdropper blocks it. Thus, it is necessary to take into account the blockage of the eavesdropper for secure transmission in high-frequency bands.

2) Path Gain: It is known that THz signals not only suffer severe molecular absorption and propagation loss, but also are highly sensitive to blockage due to high penetration loss. Hence, when the blocking eavesdropper is located within the THz beam, we formulate the LoS path loss as[1]

$$\alpha_{LoS}(f) = L_b \frac{c}{4\pi f r} \exp\left(-j2\pi f \frac{r}{c}\right) \exp\left(-\frac{1}{2}\mathcal{K}(f) r\right), \quad (5)$$

in which L_b is the power loss caused by blocking eavesdropper, f is the frequency of operation. Particularly, $\mathcal{K}(f)$ is the molecular absorption coefficient and can be written as [19], [37]

$$\mathcal{K}(f) = \sum_g \frac{p}{p_0} \frac{T_0}{T} \sigma^g(f), \quad (6)$$

in which p and p_0 denote the system pressure and the reference pressure, while T and T_0 represent the system temperature and the standard temperature. $\sigma^g(f)$ is the absorption cross section.

The NLoS path loss is a combination of the Fresnel reflection coefficient $R(f)$, spreading loss, and molecular absorption loss and can be written as

$$\alpha_{Ref}(f) = \frac{c}{4\pi f (r_1 + r_2)} \cdot \exp\left(-j2\pi f \frac{r_1 + r_2}{c}\right) \cdot R(f) \cdot \exp\left(-\frac{1}{2}\mathcal{K}(f)(r_1 + r_2)\right). \quad (7)$$

where r_1 denotes the transmitter-to-reflector distance, and r_2 is the reflector-to-receiver distance.

3) Array Steering Vector: For the $N_x \times N_z$-element USPA on the xz-plane, the array steering vector corresponding to the l-path can be expressed as

$$\mathbf{a}(\vartheta_a^l, \vartheta_e^l) = \frac{1}{\sqrt{NxN_z}} \left[1, \ldots, e^{j\frac{2\pi}{\lambda} d(p\cos(\vartheta_a^l)\sin(\vartheta_e^l) + q\cos(\vartheta_e^l)}, \ldots, e^{j\frac{2\pi}{\lambda} d\left((N_x - 1)\cos(\vartheta_a^l)\sin(\vartheta_e^l) + (N_z - 1)\cos(\vartheta_e^l)\right)}\right]^T, \quad (8)$$

where $\lambda = c/f_c$ is the wavelength, and $d = \lambda/2$ is the element spacing at the BS or IRSs. $0 \le p < N_x$, $0 \le q < N_z$ are the element indices in the xz-plane.

B. Signal Model

In the multi-IRS-assisted secure THz communication system, a THz-empowered BS transmits signal s with power P_s to multiple IRSs, then IRSs reflect the confidential signal to the desired user Bob through reflecting phase shifters.

To reduce the power consumption and hardware cost, a partial-connected hybrid beamforming structure [7], [38] is adopted at the BS. As shown in Fig. 4, there are N_{RF} RF chains equipped at the BS with M antennas, and each RF chain is connected to $\frac{M}{N_{RF}}$ antennas via analog phase shifters[2]. Hence, the digital beamformer is $\mathbf{f}_{BB} \in \mathbb{C}^{N_{RF} \times 1}$, and the analog beamformer can be expressed as $\mathbf{F}_{RF} = \text{diag}\{\mathbf{f}_{RF,1}, \ldots, \mathbf{f}_{RF,N_{RF}}\} \in \mathbb{C}^{M \times N_{RF}}$, where $\mathbf{f}_{RF,n} \in \mathbb{C}^{\frac{M}{N_{RF}} \times 1}$ denotes the analog beamformer for each antenna subarray. Then the received signal at Bob is denoted as[3]

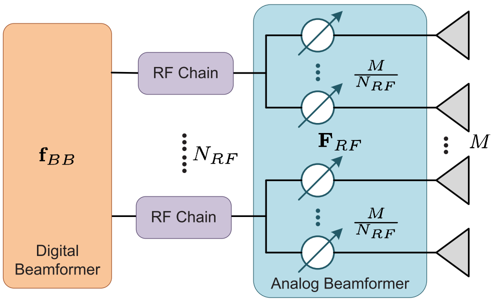


Fig. 4. Partial-connected hybrid analog-digital beamforming structure.

$$y_D = \sum_{k=1}^{K} \mathbf{h}_{D,k}^H \mathbf{\Theta}_k \mathbf{H}_{BI,k}^H \mathbf{F}_{RF} \mathbf{f}_{BB} s + n_D, \quad (9)$$

where $\mathbb{E}\{|s|^2\} = 1$ and $\mathbb{E}\{\|\mathbf{F}_{RF}\mathbf{f}_{BB}\|^2\} \le P_s$. The matrix $\mathbf{\Theta}_k = \text{diag}\{\hat{\boldsymbol{\theta}}_k\}$ is the reflecting matrix at the k-th IRS, in which $\hat{\boldsymbol{\theta}}_k = [e^{j\theta_{k,1}}, e^{j\theta_{k,2}}, \ldots, e^{j\theta_{k,N}}]^T$, and $\theta_{k,i} \in [0, 2\pi), \forall k, i$ is the phase shift of each reflecting element. In addition, $\mathbf{H}_{BI,k} \in \mathbb{C}^{M \times N}$ and $\mathbf{h}_{D,k} \in \mathbb{C}^{N \times 1}$ are respectively the BS-to-k-th IRS channel and the k-th IRS-to-Bob channel, which are assumed perfectly known at the BS.[4] $n_D \sim \mathcal{CN}(0, \sigma_D^2)$ is the additive white Gaussian noise (AWGN) at Bob.

For the IRS-assisted communication, since the confidential signals are transmitted among the BS-to-IRS link and the IRS-to-Bob link, the eavesdropping attacks may occur in both links, namely BS-IRS link eavesdropping and IRS-user link eavesdropping.

1) BS-IRS Link Eavesdropping: When the eavesdropper Eve is located between the BS and the m-th IRS, it is assumed that Eve attempts to intercept signals from BS, then the BS-IRS link eavesdropping occurs. The received signal at Eve is written as[5]

$$y_E^B = \mathbf{g}_{BE}^H \mathbf{F}_{RF} \mathbf{f}_{BB} s + n_E, \quad (10)$$

where $\mathbf{g}_{BE} \in \mathbb{C}^{M \times 1}$ denotes the channel coefficient from the BS and Eve, and $n_E \sim \mathcal{CN}(0, \sigma_E^2)$ is the AWGN noise at Eve. Note that considering the blocking effects of Eve and narrow THz beams, we assume that the link from the BS to the m-th IRS $\mathbf{H}_{BI,m}$ surfers blocking-based power loss L_b.

2) IRS-User Link Eavesdropping: When Eve is located between IRS and Bob links, it may attempt to intercept the reflecting beam from IRS. In this case, Eve can also cause an additional power loss L_b in the IRS-Bob link due to the narrow

[1] If the eavesdropper does not block the THz beam, $L_b = 1$.

[2] Note that to facilitate the partial connected hybrid beamforming structure at the BS, we assume that $N_{RF} < M$ and $\frac{M}{N_{RF}}$ is an integer.

[3] The channel between IRSs is ignored due to sufficiently large distance between buildings where IRSs are integrated.

[4] Note that the perfect CSI at legal users is obtained by making full use of all available resources.

[5] Note that in this case there is no IRS-Eve link due to narrow THz beams.

beam and the blocking sensitivity of THz waves. Without of loss generality, we assume that the m-th IRS-Bob link is intercepted and blocked, then the received signal at Eve can be written as[6]

$$y_E^I = \mathbf{g}_{IE}^H \mathbf{\Theta}_m \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB} s + n_E, \tag{11}$$

in which $\mathbf{g}_{IE} \in \mathbb{C}^{N\times 1}$ denotes the m-th IRS-to-eavesdropper channel coefficient.

Note that as Eve is an idle user, its interactions with the dedicated system are less frequent. Thus, the ECSI is assumed to be imperfectly known at the BS. Taking into account the feedback delay and untrustworthy of feedback information caused by the malicious behaviors of eavesdroppers, an additive uncertainty channel model with error bound is adopted to account for the imperfect ECSI, i.e.,

$$\mathbf{g} = \bar{\mathbf{g}} + \Delta\mathbf{g}, \ \Omega = \{\|\Delta\mathbf{g}\| \le \epsilon\}, \tag{12}$$

where $\mathbf{g} \in \{\mathbf{g}_{BE}, \mathbf{g}_{IE}\}$, and $\bar{\mathbf{g}} \in \{\bar{\mathbf{g}}_{BE}, \bar{\mathbf{g}}_{IE}\}$ is the estimated channel vector. In particular, the continuous set Ω contains all possible CSI uncertainties with their norms bounded by $\epsilon > 0$.

To guarantee the information security for any admissible ECSI conditions, the nominal worst-case secrecy rate (WCSR) between the BS and legal user Bob is defined to measure the minimum secrecy rate with partial ECSI, i.e.,

$$\begin{aligned} R_s^{wc} &= \min_{\|\Delta\mathbf{g}\|\le\epsilon} [\log_2(1+\gamma_D) - \log_2(1+\gamma_E)]^+ \\ &= [\log_2(1+\gamma_D) - \log_2(1+\gamma_{ewc})]^+, \end{aligned} \tag{13}$$

where γ_D is the received SNR at Bob [39],

$$\gamma_D = \frac{1}{\sigma_D^2} \left| \sum_{k=1}^{K} \mathbf{h}_{D,k}^H \mathbf{\Theta}_k \mathbf{H}_{BI,k}^H \mathbf{F}_{RF} \mathbf{f}_{BB} \right|^2, \tag{14}$$

and γ_{ewc} denotes the maximum SNR which can be received at the eavesdropper under any channel realization.

Before obtaining the expression of γ_{ewc}, the following two inequalities are first derived based on the triangle inequality and Cauchy-Schwarz inequality[7], i.e.,

$$|(\bar{\mathbf{g}}_{BE} + \Delta\mathbf{g}_{BE})^H \mathbf{F}_{RF}\mathbf{f}_{BB}| \le |\bar{\mathbf{g}}_{BE}^H \mathbf{F}_{RF}\mathbf{f}_{BB}| + \epsilon\|\mathbf{F}_{RF}\mathbf{f}_{BB}\|, \tag{15}$$

$$\begin{aligned} &|(\bar{\mathbf{g}}_{IE} + \Delta\mathbf{g}_{IE})^H \mathbf{\Theta}_m \mathbf{H}_{BI,m}^H \mathbf{F}_{RF}\mathbf{f}_{BB}| \\ &\quad \le |\bar{\mathbf{g}}_{IE}^H \mathbf{\Theta}_m \mathbf{H}_{BI,m}^H \mathbf{F}_{RF}\mathbf{f}_{BB}| \\ &\quad + \epsilon\|\mathbf{\Theta}_m \mathbf{H}_{BI,m}^H \mathbf{F}_{RF}\mathbf{f}_{BB}\|. \end{aligned} \tag{16}$$

According to the equation (15), the maximum SNR at Eve for the BS-IRS link eavesdropping can be expressed as

$$\begin{aligned} \gamma_{ewc}^B &= \max_{\|\Delta\mathbf{g}_{BE}\|\le\epsilon} \frac{1}{\sigma_E^2} |\mathbf{g}_{BE}^H \mathbf{F}_{RF}\mathbf{f}_{BB}|^2 \\ &= \frac{1}{\sigma_E^2} \left(|\bar{\mathbf{g}}_{BE}^H \mathbf{F}_{RF}\mathbf{f}_{BB}| + \epsilon\|\mathbf{F}_{RF}\mathbf{f}_{BB}\|\right)^2. \end{aligned} \tag{17}$$

Similarly, for the IRS-user link eavesdropping, the maximum received SNR at Eve can be obtained based on (16)

$$\begin{aligned} \gamma_{ewc}^I &= \max_{\|\Delta\mathbf{g}_{IE}\|\le\epsilon} \frac{1}{\sigma_E^2} |\mathbf{g}_{IE}^H \mathbf{\Theta}_m \mathbf{H}_{BI,m}^H \mathbf{F}_{RF}\mathbf{f}_{BB}|^2 \\ &= \frac{1}{\sigma_E^2} \big(|\bar{\mathbf{g}}_{IE}^H \mathbf{\Theta}_m \mathbf{H}_{BI,m}^H \mathbf{F}_{RF}\mathbf{f}_{BB}| \\ &\quad + \epsilon\|\mathbf{\Theta}_m \mathbf{H}_{BI,m}^H \mathbf{F}_{RF}\mathbf{f}_{BB}\|\big)^2. \end{aligned} \tag{18}$$

To maximize the secrecy performance with partial ECSI, the joint optimization problem with respect to hybrid beamforming and reflecting phase shifts will be analyzed in the following sections, and secure transmission strategies to protect BS-IRS link and IRS-user link will be respectively designed.

III. BS-IRS Link Eavesdropping With Single Eavesdropper

When the eavesdropper Eve approaches the BS, the BS-IRS link eavesdropping occurs. In this way, Eve can both intercept and block confidential signals emitted from the BS. To degrade the information leakage at Eve, the zero-forcing (ZF) principle is used to null out the confidential signals leaked in the eavesdropper channel, i.e., $\bar{\mathbf{g}}_{BE}^H \mathbf{F}_{RF}\mathbf{f}_{BB} = 0$. With the residual information leakage caused by imperfect ECSI, the worst-case secrecy rate maximization problem of the hybrid beamformer at the BS and reflecting phase shifts at multiple IRSs can be expressed as

$$\begin{aligned} (\text{P1}): \max_{\mathbf{F}_{RF},\mathbf{f}_{BB},\mathbf{\Theta}_k} & \frac{1 + \frac{1}{\sigma_D^2} \left|\sum_{k=1}^{K} \mathbf{h}_{D,k}^H \mathbf{\Theta}_k \mathbf{H}_{BI,k}^H \mathbf{F}_{RF}\mathbf{f}_{BB}\right|^2}{1 + \frac{1}{\sigma_E^2} \left(|\bar{\mathbf{g}}_{BE}^H \mathbf{F}_{RF}\mathbf{f}_{BB}| + \epsilon\|\mathbf{F}_{RF}\mathbf{f}_{BB}\|\right)^2} \\ \text{s.t.} & \begin{cases} \bar{\mathbf{g}}_{BE}^H \mathbf{F}_{RF}\mathbf{f}_{BB} = 0, \\ \|\mathbf{F}_{RF}\mathbf{f}_{BB}\|^2 \le P_s, \\ |[\mathbf{\Theta}_k]_{i,i}|^2 = |e^{j\theta_{k,i}}| = 1, \theta_{k,i} \in [0, 2\pi), \forall k, i. \end{cases} \end{aligned} \tag{19}$$

From (19) we can clearly see that the hybrid beamformer $(\mathbf{F}_{RF}, \mathbf{f}_{BB})$ and the reflecting matrix $\mathbf{\Theta}_k$ are coupled with each other, and the unit modulus constraints of the elements in $\mathbf{\Theta}_k$ are non-convex. Thus, it is difficult to solve P1 directly.

In particular, since Eve intercepts the transmit beam of the BS instead of the reflecting beams of IRSs, the reflecting matrix $\mathbf{\Theta}_k$ design is only associated with the received information rate at Bob, i.e, the numerator of the objective function. To solve the formulated non-convex problem, we hence propose to design the reflecting beamforming and hybrid beamforming alternatively. Specifically, we first derive the function expression of reflecting phase shifts with respect to the hybrid beamformer based on the numerator, i.e., $\mathbf{\Theta}_k(\mathbf{F}_{RF}, \mathbf{f}_{BB})$. By substituting the derived $\mathbf{\Theta}_k(\mathbf{F}_{RF}, \mathbf{f}_{BB})$ into the original problem, we then transform problem P1 into another optimization problem of the hybrid beamformer and solve it according to the ZF beamforming principle.

[6] For IRS-user link eavesdropping, Eve has no links between BS and $k \neq m$ IRS, thus no signal is received from them.

[7] For any vectors $\mathbf{a} \in \mathbb{C}^{N\times 1}$, $\mathbf{b} \in \mathbb{C}^{N\times 1}$, and $\mathbf{x} \in \mathbb{C}^{N\times 1}$, $|\mathbf{a}^H\mathbf{x} + \mathbf{b}^H\mathbf{x}| \le |\mathbf{a}^H\mathbf{x}| + |\mathbf{b}^H\mathbf{x}| \le |\mathbf{a}^H\mathbf{x}| + \|\mathbf{b}^H\| \cdot \|\mathbf{x}\|$.

A. Reflecting Matrix Design

To simplify the expression of the objective function in problem P1, here we define $\boldsymbol{\phi} = [\hat{\boldsymbol{\theta}}_1^T, \hat{\boldsymbol{\theta}}_2^T, \ldots, \hat{\boldsymbol{\theta}}_K^T]^T$. Then the optimization problem with respect to reflecting phase shifts at all IRSs can be formulated as

$$(\text{P1.1}): \max_{\hat{\boldsymbol{\theta}}_k, k \in \mathcal{K}} |\boldsymbol{\phi}^T \text{diag}\{\mathbf{h}_D^*\} \mathbf{H}_{BI}^H \mathbf{F}_{RF} \mathbf{f}_{BB}|^2$$

$$\text{s.t.} \begin{cases} \boldsymbol{\phi} = \left[\hat{\boldsymbol{\theta}}_1^T, \hat{\boldsymbol{\theta}}_2^T, \ldots, \hat{\boldsymbol{\theta}}_K^T\right]^T, \\ |[\hat{\boldsymbol{\theta}}_k]_i|^2 = |e^{j\theta_{k,i}}| = 1, \theta_{k,i} \in [0, 2\pi), \forall i. \end{cases} \tag{20}$$

where $\mathbf{h}_D = [\mathbf{h}_{D,1}^T, \mathbf{h}_{D,2}^T, \ldots, \mathbf{h}_{D,K}^T]^T \in \mathbb{C}^{NK \times 1}$ accommodates all channels from K IRs to Bob, and $\mathbf{H}_{BI} = [\mathbf{H}_{BI,1}, \mathbf{H}_{BI,2}, \ldots, \mathbf{H}_{BI,K}] \in \mathbb{C}^{M \times NK}$ denotes the equivalent channel from the BS to all IRSs.

Applying Cauchy-Schwarz inequality to the objective function in the above problem P1.1, we can clarify that

$$|\boldsymbol{\phi}^T \text{diag}\{\mathbf{h}_D^*\} \mathbf{H}_{BI}^H \mathbf{F}_{RF} \mathbf{f}_{BB}|^2 \overset{(a)}{\leq} \|\boldsymbol{\phi}^T\|^2 \cdot \|\text{diag}\{\mathbf{h}_D^*\} \mathbf{H}_{BI}^H \mathbf{F}_{RF} \mathbf{f}_{BB}\|^2. \tag{21}$$

The equality of (a) can be established only if $\angle(\boldsymbol{\phi}^*) = \angle(\text{diag}\{\mathbf{h}_D^H\} \mathbf{H}_{BI}^H \mathbf{F}_{RF} \mathbf{f}_{BB})$.

Thus, the optimal reflecting phase that maximizes the secrecy rate performance can be calculated in a closed-form as

$$\angle(\hat{\boldsymbol{\theta}}_k^{opt}) = -\angle\left(\text{diag}\{\mathbf{h}_D^H\} \mathbf{H}_{BI}^H \mathbf{F}_{RF} \mathbf{f}_{BB}\right), \forall k. \tag{22}$$

B. Hybrid Beamforming Design

With the obtained reflecting phase shifts $\boldsymbol{\Theta}_k(\mathbf{F}_{RF}, \mathbf{f}_{BB})$, the original problem P1 can be expressed as

$$(\text{P1.2}): \max_{\mathbf{F}_{RF}, \mathbf{f}_{BB}} \frac{1 + \mathbf{f}_{BB}^H \mathbf{F}_{RF}^H \mathbf{R}_{BD} \mathbf{F}_{RF} \mathbf{f}_{BB}}{1 + \frac{\epsilon^2}{\sigma_E^2} \mathbf{f}_{BB}^H \mathbf{F}_{RF}^H \mathbf{F}_{RF} \mathbf{f}_{BB}}$$

$$\text{s.t.} \begin{cases} \bar{\mathbf{g}}_{BE}^H \mathbf{F}_{RF} \mathbf{f}_{BB} = 0, \\ \|\mathbf{F}_{RF} \mathbf{f}_{BB}\|^2 \leq P_s. \end{cases} \tag{23}$$

where $\mathbf{R}_{BD} = \frac{N}{\sigma_D^2} \mathbf{H}_{BI} \text{diag}\{\mathbf{h}_D\} \text{diag}\{\mathbf{h}_D^*\} \mathbf{H}_{BI}^H$.

Note that as the analog beamformer $\mathbf{F}_{RF}$ and digital beamformer $\mathbf{f}_{BB}$ are always coupled with each other, here we temporarily couple them as a single vector variable $\mathbf{w} = \mathbf{F}_{RF} \mathbf{f}_{BB}$ to make the formulated problem easier to solve.

With the ZF beamforming protocol and the generalized eigenvector decomposition, the optimal hybrid beamforming can be derived according to the following proposition.

Proposition 1: The closed-form solution of $\mathbf{w}$ of problem P1.2 can be derived as

$$\mathbf{w}^{opt} = \sqrt{\frac{P_s}{\mathbf{q}_1^H \mathbf{B}_1^H \mathbf{B}_1 \mathbf{q}_1}} \mathbf{B}_1 \mathbf{q}_1, \tag{24}$$

where $\mathbf{B}_1$ is defined as the null space of the eavesdropper channel $\bar{\mathbf{g}}_{BE}^H$, and $\mathbf{q}_1$ denotes the unit-norm eigenvector of the matrix $[\frac{1}{P_s} \mathbf{B}_1^H \mathbf{B}_1 + \frac{\epsilon^2}{\sigma_E^2} \mathbf{B}_1^H \mathbf{B}_1]^{-1} [\frac{1}{P_s} \mathbf{B}_1^H \mathbf{B}_1 + \mathbf{B}_1^H \mathbf{R}_{BD} \mathbf{B}_1]$ corresponding to its maximum eigenvalue.

Proof: Please see Appendix A. □

Algorithm 1: Alternative Algorithm for WCSR Maximization.

```
Initialize channel condition $\mathbf{h}_{D,k}$, $\mathbf{H}_{BI,k}$, $\bar{\mathbf{g}}_{BE}$ and $\epsilon$.
Calculate analog beamforming $\mathbf{F}_{RF}^{opt}$ based on equation (25).
With the obtained $\mathbf{F}_{RF}^{opt}$, calculate the digital beamforming vector $\mathbf{f}_{BB}^{opt}$ using (26).
With the obtained hybrid beamformers $\mathbf{F}_{BF}^{opt}$ and $\mathbf{f}_{BB}^{opt}$, derive the optimal solution of reflecting phase shifts $\hat{\boldsymbol{\theta}}_k^{opt}, \forall k$.
return $(\mathbf{F}_{BF}^{opt}, \mathbf{f}_{BB}^{opt}, \hat{\boldsymbol{\theta}}_k^{opt})$.
```

As the analog beamforming is implemented by THz phase shifts, while the digital beamforming has full control over both the amplitude and the phase of the signal [40]. Considering the power constraint at the BS, we thus define the analog beamformer for each antenna subarray as $\mathbf{f}_{RF,n} = \frac{1}{\sqrt{M/N_{RF}}}[e^{j\varphi_1}, \ldots, e^{j\varphi_{\frac{M}{N_{RF}}}}], \forall n$, where $\varphi_i \in [0, 2\pi), \forall i$ denotes the angle of each phase shift. Then we propose to decouple $\mathbf{f}_{RF,n}$ from the solution $\mathbf{w}^{opt}$ as

$$\mathbf{f}_{RF,n}^{opt} = \frac{1}{\sqrt{M/N_{RF}}} e^{j\angle(\mathbf{G}_n \mathbf{w})}, \forall n, \tag{25}$$

where $\mathbf{G}_n = [\mathbf{0}_{(n-1)\frac{M}{N_RF}}, \mathbf{I}_{\frac{M}{N_RF}}, \mathbf{0}_{(N_{RF}-n)\frac{M}{N_RF}}]$.

With the obtained solution of analog beamformer $\mathbf{F}_{RF}^{opt} = \text{diag}\{\mathbf{f}_{RF,1}^{opt}, \ldots, \mathbf{f}_{RF,N_{RF}}^{opt}\}$, the closed-form digital beamformer can be derived as

$$\mathbf{f}_{BB}^{opt} = \sqrt{\frac{P_s}{\mathbf{q}^H \mathbf{B}^H \mathbf{B} \mathbf{q}}} \mathbf{B} \mathbf{q}, \tag{26}$$

in which given the null space of $\bar{\mathbf{g}}_{BE}^H \mathbf{F}_{RF}$, i.e., the matrix $\mathbf{B}$, the vector $\mathbf{q}$ represents the unit-norm eigenvector of the matrix $[\frac{1}{P_s} \mathbf{B}^H \mathbf{B} + \frac{\epsilon^2}{\sigma_E^2} \mathbf{B}^H \mathbf{F}_{RF}^H \mathbf{I}_{N_{RF}} \mathbf{F}_{RF} \mathbf{B}]^{-1} [\frac{1}{P_s} \mathbf{B}^H \mathbf{B} + \mathbf{B}^H \mathbf{F}_{RF}^H \mathbf{R}_{BD} \mathbf{F}_{RF} \mathbf{B}]$ corresponding to the maximum eigenvalue.

With the obtained solution of hybrid analog and digital beamforming, the reflecting phase shifts in (22) can be updated. Consequently, the whole secure transmission strategy for BS-IRS link eavesdropping attacks can be summarized as Algorithm 1.

IV. IRS-User Link-Eavesdropping With Single Eavesdropper

For the IRS-user link eavesdropping attack, the information leakage occurs among the communication between the m-th IRS and Bob, and Eve can block partial information transmission among this link.

$$R_s^{wc} = \frac{1 + \frac{1}{\sigma_D^2} \left|\sum_{k=1}^K \mathbf{h}_{D,k}^H \boldsymbol{\Theta}_k \mathbf{H}_{BI,k}^H \mathbf{F}_{RF} \mathbf{f}_{BB}\right|^2}{1 + \frac{1}{\sigma_E^2} \left(|\bar{\mathbf{g}}_{IE}^H \boldsymbol{\Theta}_m \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB}| + \epsilon \|\boldsymbol{\Theta}_m \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB}\|\right)^2} \tag{27}$$

In comparison with BS-IRS link-eavesdropping, the IRS-user link-eavesdropping leads to the worst-case secrecy rate maximization problem more intractable. Specifically, the worst-case secrecy rate in (27) is a fractional function for both hybrid beamforming and reflecting phase shifts, which allows $\mathbf{F}_{RF}\mathbf{f}_{BB}$ design and $\mathbf{\Theta}_k, k \in \mathcal{K}$ design to be coupled with each other. Moreover, the unit modulus constraints of reflecting phase shifts and imperfect ECSI lead to ZF principle difficult to implement at the IRS. The reason is that if ZF principle is used for the IRS-Eve link, each element of $\bar{\mathbf{g}}_{IE,m}^H\mathbf{\Theta}_m$ is required to be zero. That is the product of each element of eavesdropper channel $\bar{\mathbf{g}}_{IE,m}$ and each $e^{j\theta_{m,i}}$ is equal to zero, which is infeasible.[8]

Here instead of maximizing the secrecy rate directly, we aim to maximize it with a given information leakage threshold γ_0, and formulate the optimization problem as equation (28). In the formulated problem, it is obvious that its objective function is still not jointly concave with respect to hybrid beamforming and reflecting beamforming. Additionally, with a given information leakage at Eve, the lower bound of R_s^{wc} in (27) can be obtained as $R_s^{wc} \geq (1 + \frac{1}{\sigma_D^2}|\sum_{k=1}^{K} \mathbf{h}_{D,k}^H\mathbf{\Theta}_k\mathbf{H}_{BI,k}^H\mathbf{F}_{RF}\mathbf{f}_{BB}|^2)/(1+\gamma_0)$, which is concave with respect to $\mathbf{F}_{RF}\mathbf{f}_{BB}$ and $\mathbf{\Theta}_k$.

Hence, instead of (28) shown at the bottom of this page, we propose to jointly design hybrid beamforming and reflecting beamforming with the lower bound of R_s^{wc}, i.e.,

$$\text{(P2)}: \max_{\mathbf{F}_{RF},\mathbf{f}_{BB},\mathbf{\Theta}_k} \frac{1}{\sigma_D^2}\left|\sum_{k=1}^{K}\mathbf{h}_{D,k}^H\mathbf{\Theta}_k\mathbf{H}_{BI,k}^H\mathbf{F}_{RF}\mathbf{f}_{BB}\right|^2$$

$$\text{s.t.} \begin{cases} \gamma_{ewc}(\mathbf{F}_{RF},\mathbf{f}_{BB},\hat{\boldsymbol{\theta}}_m) \leq \gamma_0, \\ \|\mathbf{F}_{RF}\mathbf{f}_{BB}\|^2 \leq P_s, \\ |[\mathbf{\Theta}_k]_{i,i}|^2 = |e^{j\theta_{k,i}}| = 1, \theta_{k,i} \in [0, 2\pi), \forall k, i. \end{cases} \tag{29}$$

In the above problem, the information leakage constraint is

$$\left(|\bar{\mathbf{g}}_{IE}^H\mathbf{\Theta}_m\mathbf{H}_{BI,m}^H\mathbf{F}_{RF}\mathbf{f}_{BB}| + \epsilon\|\mathbf{\Theta}_m\mathbf{H}_{BI,m}^H\mathbf{F}_{RF}\mathbf{f}_{BB}\|\right)^2 \leq \gamma_0 \cdot \sigma_E^2.$$

It can be proved that the above problem P2 remains non-convex due to the unit modulus constraint and coupled variables. As an alternative, an iterative algorithm is hence proposed in this section, in which the hybrid beamforming and reflecting phase shifts can be iteratively designed by converting the original problem into two subproblems.

A. Hybrid Beamforming Design

When the eavesdropper intercepts the m-th IRS-user link, its eavesdropping performance mainly relies on the reflecting beam, rather than the transmit beam from the BS. Therefore, the hybrid beamforming is first designed. In particular, since the analog beamforming is implemented by THz phase shifts, we can also define $\mathbf{f}_{RF,n}$ as the same expression in Section III, i.e., $\mathbf{f}_{RF,n}^{(i)} = \frac{1}{\sqrt{M/N_{RF}}}e^{j\varphi_i}, \forall n, i$. Then we have $\mathbf{F}_{RF}^H\mathbf{F}_{RF} = \mathbf{I}_{N_{RF}}$, and the power constraint at the BS can be reduced to $\|\mathbf{F}_{RF}\mathbf{f}_{BB}\|^2 = \|\mathbf{f}_{BB}\|^2 \leq P_s$. Then the subproblem with respect to $(\mathbf{F}_{RF}, \mathbf{f}_{BB})$ can be written as

$$\text{(P2.1)}: \max_{\mathbf{F}_{RF},\mathbf{f}_{BB}} |\mathbf{h}_D^H\text{diag}\{\boldsymbol{\phi}\}\mathbf{H}_{BI}^H\mathbf{F}_{RF}\mathbf{f}_{BB}|^2$$

$$\text{s.t.} \begin{cases} \gamma_{ewc}(\mathbf{F}_{RF},\mathbf{f}_{BB},\hat{\boldsymbol{\theta}}_m) \leq \gamma_0, \\ \|\mathbf{f}_{BB}\|^2 \leq P_s, \\ |\mathbf{f}_{RF,n}^{(i)}| = 1/\sqrt{M/N_{RF}}, \forall n, i. \end{cases} \tag{30}$$

It is obvious that the formulated hybrid beamforming problem is non-convex due to the coupled analog and digital beamformer, and the constant modulus constraint for each entry of $\mathbf{F}_{RF}$. To tackle the above non-convex problem, the suboptimal two-stage-based hybrid beamforming strategy [40], [41] is proposed by decoupling the above problem into an analog beamforming problem and a digital beamforming problem. In the first stage, the RF analog beamforming design aims to maximize the achievable array gain offered by a large number of antennas at the BS. In the second stage, the digital beamforming is then designed to maximize the information rate at Bob with a given information leakage at Eve.

1) Analog Beamforming Design: In order to decouple the analog and digital beamformers, an upper bound of array gain between the BS and the destination is first derived. For the partially-connected hybrid beamforming architecture, the upper bound of array gain can be obtained using Cauchi-Schwarz inequality, i.e.,

$$\begin{aligned} |\tilde{\mathbf{h}}^H\mathbf{F}_{RF}\mathbf{f}_{BB}|^2 &\overset{(a)}{\leq} \|\tilde{\mathbf{h}}^H\mathbf{F}_{RF}\|^2 \cdot \|\mathbf{f}_{BB}\|^2 \\ &= \|\mathbf{f}_{BB}\|^2 \cdot \sum_{n=1}^{N_{RF}} |\tilde{\mathbf{h}}_n^H\mathbf{f}_{RF,n}|^2, \end{aligned} \tag{31}$$

where $\tilde{\mathbf{h}}^H = \mathbf{h}_D^H\text{diag}\{\boldsymbol{\phi}\}\mathbf{H}_{BI}^H$ denotes the equivalent channel from BS to Bob, and $\tilde{\mathbf{h}}_n = [\tilde{\mathbf{h}}^{((n-1)\frac{M}{N_{RF}}+1)}, \ldots, \tilde{\mathbf{h}}^{(n\frac{M}{N_{RF}})}], \forall n$.

Then the optimization problem with respect to analog beamforming to maximize the upper bound of array gain can be

$$\max_{\mathbf{F}_{RF},\mathbf{f}_{BB},\mathbf{\Theta}_k} \frac{1 + \frac{1}{\sigma_D^2}\left|\sum_{k=1}^{K}\mathbf{h}_{D,k}^H\mathbf{\Theta}_k\mathbf{H}_{BI,k}^H\mathbf{F}_{RF}\mathbf{f}_{BB}\right|^2}{1 + \frac{1}{\sigma_E^2}\left(|\bar{\mathbf{g}}_{IE}^H\mathbf{\Theta}_m\mathbf{H}_{BI,m}^H\mathbf{F}_{RF}\mathbf{f}_{BB}| + \epsilon\|\mathbf{\Theta}_m\mathbf{H}_{BI,m}^H\mathbf{F}_{RF}\mathbf{f}_{BB}\|\right)^2}$$

$$\text{s.t.} \begin{cases} \gamma_{ewc}(\mathbf{F}_{RF},\mathbf{f}_{BB},\hat{\boldsymbol{\theta}}_m) \leq \gamma_0, \\ \|\mathbf{F}_{RF}\mathbf{f}_{BB}\|^2 \leq P_s, \\ |[\mathbf{\Theta}_k]_{i,i}|^2 = |e^{j\theta_{k,i}}| = 1, \theta_{k,i} \in [0, 2\pi), \forall k, i. \end{cases} \tag{28}$$

[8] Note that if the product of two complex numbers x and y is equal to zero, then at least one of them is zero, which is contrary to the system assumption.

written as

$$\max_{\mathbf{f}_{RF,n}} \|\tilde{\mathbf{h}}_n^H \mathbf{f}_{RF,n}\|^2, \ \text{s.t.} \ |\mathbf{f}_{RF,n}^{(i)}| = \frac{1}{\sqrt{M/N_{RF}}}, \forall n, i. \tag{32}$$

It is obvious that the above problem is equivalent to the equality gain transmission problem [42], which has the analytical solution as

$$\mathbf{f}_{RF,n}^{(i)} = \frac{1}{\sqrt{M/N_{RF}}} e^{j(\zeta + \angle \tilde{\mathbf{h}}_n^{(i)})} \tag{33}$$

where $\zeta \in (0, 2\pi]$ is an arbitrary phase, and $\angle \tilde{\mathbf{h}}_n^{(i)}$ is the phase angle of the i-th element of $\tilde{\mathbf{h}}_n$.

2) Digital Beamforming Design: With the obtained analog beamformer, the subproblem of digital beamforming design can be written as

$$\begin{aligned} &(\text{P2.2}): \max_{\mathbf{f}_{BB}} |\mathbf{h}_D^H \text{diag}\{\boldsymbol{\phi}\} \mathbf{H}_{BI}^H \mathbf{F}_{RF} \mathbf{f}_{BB}|^2 \\ &\text{s.t.} \begin{cases} \gamma_{ewc}(\mathbf{F}_{RF}, \mathbf{f}_{BB}, \hat{\boldsymbol{\theta}}_m) \leq \gamma_0, \\ \|\mathbf{f}_{BB}\|^2 \leq P_s. \end{cases} \end{aligned} \tag{34}$$

Then the solution can be derived based on the following Proposition 2.

Proposition 2: With the limited information leakage at Eve, the closed-form solution of digital beamformer, which maximizes the information rate received at the legal user, can be obtained as

$$\mathbf{f}_{BB}^{opt} = \mu \mathbf{q}, \tag{35}$$

where μ is the power constraint factor and is described as

$$\mu = \min \left\{ \sqrt{P_s}, \frac{\sqrt{\gamma_0}\sigma_E}{|\bar{\mathbf{g}}_{IE}^H \boldsymbol{\Theta}_m \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{q}| + \epsilon \|\mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{q}\|} \right\},$$

and the vector $\mathbf{q}$ is

$$\mathbf{q} = \frac{\mathbf{F}_{RF}^H \mathbf{H}_{BI} \text{diag}\{\boldsymbol{\phi}^*\} \mathbf{h}_D}{\|\mathbf{F}_{RF}^H \mathbf{H}_{BI} \text{diag}\{\boldsymbol{\phi}^*\} \mathbf{h}_D\|}.$$

Proof: Please see Appendix B. □

B. Reflecting Beamforming Design

Before solving the solution of reflecting beamforming, here we first rewrite the objective function of problem P2, and utilizing the triangle inequality we can obtain that

$$\begin{aligned} &|\mathbf{h}_D^H \text{diag}\{\boldsymbol{\phi}\} \mathbf{H}_{BI}^H \mathbf{F}_{RF} \mathbf{f}_{BB}|^2 \overset{(a)}{\leq} \\ &\qquad g(\tilde{\boldsymbol{\phi}}) + \left| \hat{\boldsymbol{\theta}}_m^T \text{diag}\{\mathbf{h}_{D,m}^*\} \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB} \right|^2 \end{aligned} \tag{36}$$

in which the function $g(\tilde{\boldsymbol{\phi}}) = |\tilde{\boldsymbol{\phi}}^T \text{diag}\{\tilde{\mathbf{h}}_D^*\} \tilde{\mathbf{H}}_{BI}^H \mathbf{F}_{RF} \mathbf{f}_{BB}|^2$, and the vector $\tilde{\boldsymbol{\phi}} = [\hat{\boldsymbol{\theta}}_1^T, \ldots, \hat{\boldsymbol{\theta}}_{m-1}^T, \hat{\boldsymbol{\theta}}_{m+1}^T, \ldots, \hat{\boldsymbol{\theta}}_K^T]^T$, $\tilde{\mathbf{h}}_D = [\mathbf{h}_{D,1}^T, \ldots, \mathbf{h}_{D,m-1}^T, \mathbf{h}_{D,m+1}^T, \ldots \mathbf{h}_{D,K}^T]^T$, and the matrix $\tilde{\mathbf{H}}_{BI} = [\mathbf{H}_{BI,1}, \ldots, \mathbf{H}_{BI,m-1}, \mathbf{H}_{BI,m+1}, \ldots, \mathbf{H}_{BI,K}]$. The equality in (a) holds if and only if

$$\begin{aligned} &\angle(\hat{\boldsymbol{\theta}}_m^T \text{diag}\{\mathbf{h}_{D,m}^*\} \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB}) \\ &\qquad = \angle(\tilde{\boldsymbol{\phi}}^T \text{diag}\{\tilde{\mathbf{h}}_D^*\} \tilde{\mathbf{H}}_{BI}^H \mathbf{F}_{RF} \mathbf{f}_{BB}) \\ &\qquad \triangleq \varphi_0. \end{aligned} \tag{37}$$

Thereby, with the designed hybrid beamforming at the BS, the subproblem of reflecting phase shifts under a given information leakage constraint can be written as

$$\begin{aligned} &(\text{P2.3}): \max_{\hat{\boldsymbol{\theta}}_k, k \in \mathcal{K}} g(\tilde{\boldsymbol{\phi}}) + |\hat{\boldsymbol{\theta}}_m^T \text{diag}\{\mathbf{h}_{D,m}^*\} \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB}|^2 \\ &\text{s.t.} \begin{cases} |\hat{\boldsymbol{\theta}}_m^T \text{diag}\{\mathbf{g}_{IE}^*\} \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB}|^2 \leq Q(\gamma_0), \\ |[\hat{\boldsymbol{\theta}}_k]_i|^2 = |e^{j\theta_{k,i}}| = 1, \theta_{k,i} \in [0, 2\pi), \forall k, i. \\ Eq.(37) \end{cases} \end{aligned} \tag{38}$$

where $Q(\gamma_0) = (\sigma_E \sqrt{\gamma_0} - \epsilon \|\mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB}\|)^2$.

It can be intuitively seen that $g(\tilde{\boldsymbol{\phi}})$ is independent with reflecting beamforming $\hat{\boldsymbol{\theta}}_m$ at the m-th IRS, and the optimal $\tilde{\boldsymbol{\phi}}$ for $(k \neq m)$th IRS is only determined by $g(\tilde{\boldsymbol{\phi}})$ and the constraint in equation (37). In other words, for any given $\hat{\boldsymbol{\theta}}_m$, the optimal $\tilde{\boldsymbol{\phi}}$ which maximizing the secrecy rate performance can be derived from the equivalent problem $\max g(\tilde{\boldsymbol{\phi}}), s.t.(37)$.

On the basis of Cauchy-Schwarz inequality, the solution of $\tilde{\boldsymbol{\phi}}$ can be obtained as

$$\begin{aligned} \tilde{\boldsymbol{\phi}}^{opt} &= [(\hat{\boldsymbol{\theta}}_1^{opt})^T, \ldots, (\hat{\boldsymbol{\theta}}_{m-1}^{opt})^T, (\hat{\boldsymbol{\theta}}_{m+1}^{opt})^T, \ldots, (\hat{\boldsymbol{\theta}}_K^{opt})^T]^T \\ &= e^{j\left(\varphi_0 - \angle\left(\text{diag}\{\tilde{\mathbf{h}}_D^H\} \tilde{\mathbf{H}}_{BI}^H \mathbf{F}_{RF} \mathbf{f}_{BB}\right)\right)} \end{aligned} \tag{39}$$

With the solution $\tilde{\boldsymbol{\phi}}^{opt}$, the problem P2.3 is reduced as an optimization problem of the reflecting beamformer at the m-th IRS, i.e.,

$$\begin{aligned} &(\text{P2.3}') \max_{\hat{\boldsymbol{\theta}}_m} |\hat{\boldsymbol{\theta}}_m^T \text{diag}\{\mathbf{h}_{D,m}^*\} \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB}|^2 \\ &\text{s.t.} \begin{cases} |\hat{\boldsymbol{\theta}}_m^T \text{diag}\{\mathbf{g}_{IE}^*\} \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB}|^2 \leq Q(\gamma_0), \\ |[\hat{\boldsymbol{\theta}}_m]_i|^2 = |e^{j\theta_{m,i}}| = 1, \theta_{m,i} \in [0, 2\pi), \forall i, \\ \tilde{\boldsymbol{\phi}} = \tilde{\boldsymbol{\phi}}^{opt} \end{cases} \end{aligned} \tag{40}$$

To cope with the non-convexity caused by the unit modulus constraints of $\hat{\boldsymbol{\theta}}_m$, we propose to reformulate the above problem as an SDP one. Given the definition of $\boldsymbol{\Phi} \triangleq \hat{\boldsymbol{\theta}}_m^* (\hat{\boldsymbol{\theta}}_m^*)^H$ and moving the rank-one constraint $\text{rank}(\boldsymbol{\Phi}) = 1$, the problem P2.3′ can be reformulated as its relaxed form, i.e,

$$\begin{aligned} &\max_{\boldsymbol{\Phi} \succeq 0} \ \text{tr}(\mathbf{H}_D \boldsymbol{\Phi}) \\ &\text{s.t.} \begin{cases} \text{tr}(\mathbf{G}_E \boldsymbol{\Phi}) \leq Q(\gamma_0), \\ \text{tr}(\mathbf{E}_n \boldsymbol{\Phi}) = 1, \forall n, \end{cases} \end{aligned} \tag{41}$$

where $\mathbf{G}_E = \text{diag}\{\mathbf{g}_{IE}^*\} \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB} \mathbf{f}_{BB}^H \mathbf{F}_{RF}^H \mathbf{H}_{BI,m} \text{diag}\{\mathbf{g}_{IE}\}$, $\mathbf{H}_D = \text{diag}\{\mathbf{h}_{D,m}^*\} \mathbf{H}_{BI,m}^H \mathbf{F}_{RF} \mathbf{f}_{BB} \mathbf{f}_{BB}^H \mathbf{F}_{RF}^H \mathbf{H}_{BI,m} \text{diag}\{\mathbf{h}_{D,m}\}$. The matrix $\mathbf{E}_n \in \mathbb{C}^{N \times N}$ is defined as $\mathbf{E}_n(i, j) = 1$ for $i = j = n$, otherwise $\mathbf{E}_n(i, j) = 0$.

Algorithm 2: Iterative Algorithm.

```
Initialize $\hat{\boldsymbol{\theta}}_k^0 = [e^{j\theta_{k,1}^0}, e^{j\theta_{k,2}^0}, \ldots, e^{j\theta_{k,N}^0}]^T, k \in \mathcal{K}$,
    $\boldsymbol{\Theta}_k^0 = \mathrm{diag}\{\hat{\boldsymbol{\theta}}_k^0\}$, $\mathbf{F}_{BF}^0$, $\mathbf{f}_{BB}^0$, $\varepsilon$, and set $n = 0$.
Calculate $R_s^{wc}(\mathbf{F}_{RF}^0, \mathbf{f}_{BB}^0, \hat{\boldsymbol{\theta}}_k^0)$.
repeat
    $n = n + 1$
    With the fixed $\hat{\boldsymbol{\theta}}_k^{n-1}$, calculate $\mathbf{F}_{BF}^n$ and $\mathbf{f}_{BB}^n$ by using Proposition 2.
    For $k = m$, calculate the SDR solution $\boldsymbol{\Phi}^{opt}$, derive its eigen-decomposition, then obtain the rank-one solution $\boldsymbol{\Phi}^{opt} = \hat{\boldsymbol{\theta}}_m^n (\hat{\boldsymbol{\theta}}_m^n)^H$.
    For $k \neq m$, calculate $\hat{\boldsymbol{\theta}}_k^n$ by substituting $\hat{\boldsymbol{\theta}}_m^n$ into equation (39).
    The solution of all reflecting beamformers is $\boldsymbol{\phi}^n = [(\hat{\boldsymbol{\theta}}_1^n)^T, \ldots, (\hat{\boldsymbol{\theta}}_{m-1}^n)^T, (\hat{\boldsymbol{\theta}}_m^n)^T, (\hat{\boldsymbol{\theta}}_{m+1}^n)^T, \ldots, (\hat{\boldsymbol{\theta}}_K^n)^T]^T$
    Calculate $(R_s^{wc})^n = R_s^{wc}(\mathbf{F}_{RF}^n, \mathbf{f}_{BB}^n, \boldsymbol{\phi}^n)$.
until $|(R_s^{wc})^n - (R_s^{wc})^{n-1}| \leq \varepsilon$.
return $\mathbf{F}_{BF}^{opt}\mathbf{f}_{BB}^{opt} = \mathbf{F}_{BF}^n\mathbf{f}_{BB}^n$ and $\hat{\boldsymbol{\theta}}_k^{opt} = \hat{\boldsymbol{\theta}}_k^n, k \in \mathcal{K}$.
```

The relaxed problem in (41) is a standard SDP problem, and it can be solved via CVX tools with interior-point algorithms. Then the rank-one solution $\hat{\boldsymbol{\theta}}_m^{opt}$ can be derived by the Gaussian randomization method [13].

C. Iterative Algorithm Description

By iteratively updating the hybrid beamforming and reflecting phase shifts based on the above two subsections, the optimization problem P2 can be solved.

The main steps in our proposed iterative algorithm are summarized as Algorithm 2. The algorithm guarantees that the objective function in P2 is non-decreasing after each iteration. With the limited transmit power at the BS, the achievable secrecy rate is upper bounded by a finite value. Consequently, the convergence of Algorithm 2 is guaranteed. If we assume the iteration number is N_{iter}, the complexity of our proposed iterative algorithm can be calculated relying on the hybrid beamforming and reflecting beamforming design and N_{iter}. For the hybrid beamforming design, the complexity of obtaining analog beamformer about $\mathcal{O}(N^2 + NM)$, and the complexity of deriving digital beamformer is about $\mathcal{O}(MNN_{RF})$. For the reflecting beamforming design, the complexity of obtaining $\boldsymbol{\Theta}_k, k \neq m$ is $\mathcal{O}((N-1)N^2M)$, while the complexity using SDP method to derive $\boldsymbol{\Theta}_m$ is about $\mathcal{O}(N^{3.5})$ [43]. Thus the complexity of the iterative algorithm is about $\mathcal{O}(N^3(M + \sqrt{N})N_{iter})$.

V. Secrecy Performance for Multi-Eavesdropper System

In this section, we will study the secrecy performance in the case of multiple eavesdroppers, and provide a hybrid beamforming and reflecting beamforming scheme to maximize the worst-case secrecy rate with imperfect ECSI. In the multi-eavesdropper system, K_E non-colluding eavesdroppers are assumed to be randomly located in the communication area. Thus both BS-IRS links and IRS-user links may be intercepted and blocked by eavesdroppers, i.e., two types of eavesdropping attacks can co-occur. When Eve approaches the BS, it intercepts and can block some BS-IRS links. Otherwise, when Eve is located between IRS and Bob, the IRS-user link eavesdropping will occur.

Without loss generality, we assume that the number of BS-IRS link-based eavesdropping is K_B and the number of IRS-user link-based eavesdropping is K_I, and $K_B + K_I = K_E$. Thus the worst-case secrecy rate for multi-eavesdropper system can be written as

$$\begin{aligned} R_s^{wc} &= [\log_2(1 + \gamma_D) - \log_2(1 + \max_{n \in \mathcal{K}_E} \max_{\|\Delta \mathbf{g}_E\| \leq \epsilon} \gamma_{E,n})]^+ \\ &= [\log_2(1 + \gamma_D) - \log_2(1 + \gamma_{ewc}^{\max})]^+, \end{aligned} \tag{42}$$

where $\gamma_{ewc}^{\max}$ denotes the maximum SNR received at all non-colluding eavesdroppers, and it can be written as

$$\begin{aligned} \gamma_{ewc}^{\max} &= \max_{n \in \mathcal{K}_E} \max_{\|\Delta \mathbf{g}_E\| \leq \epsilon} \gamma_{E,n} \\ &= \max \left(\max_{i \in \mathcal{K}_B} \max_{\|\Delta \mathbf{g}_E\| \leq \epsilon} \gamma_{E,i}^B, \max_{j \in \mathcal{K}_I} \max_{\|\Delta \mathbf{g}_E\| \leq \epsilon} \gamma_{E,j}^I \right) \end{aligned} \tag{43}$$

in which $\mathcal{K}_E = \mathcal{K}_B \cup \mathcal{K}_I$, and $\mathcal{K}_B = \{1, 2, \ldots, K_B\}$, $\mathcal{K}_I = \{1, 2, \ldots, K_I\}$. $\max_{\|\Delta \mathbf{g}_E\| \leq \epsilon} \gamma_{E,i}^B$ and $\max_{\|\Delta \mathbf{g}_E\| \leq \epsilon} \gamma_{E,j}^I$ respectively represent the received SNR for BS-IRS link-based eavesdropping and IRS-user link-based eavesdropping, and their definitions can be found in equations (17) and (18).

To maximize the worst-case secrecy rate performance, a joint optimization problem with respect to hybrid beamforming and reflecting phase shifts are formulated as

$$\begin{aligned} (\mathrm{P3}):\ &\max_{\mathbf{F}_{RF}, \mathbf{f}_{BB}, \boldsymbol{\Theta}_k} R_s^{wc}(\mathbf{F}_{RF}, \mathbf{f}_{BB}, \boldsymbol{\Theta}_k) \\ &\text{s.t.} \begin{cases} \|\mathbf{F}_{RF}\mathbf{f}_{BB}\|^2 \leq P_s, \\ \theta_{k,i} \in [0, 2\pi), \forall i, k. \end{cases} \end{aligned} \tag{44}$$

It is intuitive that the objective function in the above problem has two different expressions based on two types of eavesdropping attacks. Specifically, if $\max_{i \in \mathcal{K}_B} \max_{\|\Delta \mathbf{g}_E\| \leq \epsilon} \gamma_{E,i}^B > \max_{j \in \mathcal{K}_I} \max_{\|\Delta \mathbf{g}_E\| \leq \epsilon} \gamma_{E,j}^I$, the maximum SNR $\gamma_{ewc}^{\max}$ is intercepted from BS-IRS links, and the objective function in P3 has a similar expression to problem P1. Then the optimal solution of hybrid beamforming and reflecting beamforming can be obtained via Algorithm 1. Otherwise, $\gamma_{ewc}^{\max}$ is obtained from IRS-user links, and the problem in (44) can be regarded as a similar problem to P2. Then the solution can be derived via Algorithm 2.

Before summarizing the secure transmission strategy for multi-eavesdropper systems, the following Proposition 3 is first proposed to determine the analytical expression of $\gamma_{ewc}^{\max}$.

Proposition 3: If matrix $\mathbf{A} = (\mathbf{H}_{BI,q}\boldsymbol{\Theta}_q^H \bar{\mathbf{g}}_{IE,q}\bar{\mathbf{g}}_{IE,q}^H \boldsymbol{\Theta}_q \mathbf{H}_{BI,q}^H - \bar{\mathbf{g}}_{BE,p}\bar{\mathbf{g}}_{BE,p}^H)$ is positive semidefinite, we can express the maximum SNR received by all eavesdroppers as $\gamma_{ewc}^{\max} = \gamma_{ewc,q}^I$, otherwise $\gamma_{ewc}^{\max} = \gamma_{ewc,p}^B$, in which $p = \arg\max_{i \in \mathcal{K}_B} \max_{\|\Delta \mathbf{g}_E\| \leq \epsilon} \gamma_{E,i}^B$ and $q = \arg\max_{j \in \mathcal{K}_I} \max_{\|\Delta \mathbf{g}_E\| \leq \epsilon} \gamma_{E,j}^I$.

Algorithm 3: Secure Transmission with Multi-Eavesdroppers.

```
Initialize $\mathbf{F}_{BF}^0, \mathbf{f}_{BB}^0$,
    $\hat{\boldsymbol{\theta}}_k^0 = [e^{j\theta_{k,1}^0}, e^{j\theta_{k,2}^0}, \ldots, e^{j\theta_{k,N}^0}]^T, k \in \mathcal{K}$,
    $\boldsymbol{\Theta}_k^0 = \mathrm{diag}\{\hat{\boldsymbol{\theta}}_k^0\}$.
Calculate $m = \arg\max_{k \in \mathcal{K}} \gamma_{ewc,k}$ and
    $R_s^{wc}(\mathbf{F}_{RF}^0, \mathbf{f}_{BB}^0, \hat{\boldsymbol{\theta}}_k^0)$.
if A $\preceq$ 0 then
    Find the optimal hybrid beamforming $\mathbf{F}_{BF}^{opt}, \mathbf{f}_{BB}^{opt}$ and
    reflecting phase shifts $\hat{\boldsymbol{\theta}}_k^{opt}$ by using Algorithm 1.
else
    Adopt the iterative algorithm in Algorithm 2 to
    calculate $\mathbf{F}_{BF}^{opt}, \mathbf{f}_{BB}^{opt}$ and $\hat{\boldsymbol{\theta}}_k^{opt}$ iteratively, and return
    the solution when the algorithm converges.
end if
return $(\mathbf{F}_{BF}^{opt}, \mathbf{f}_{BB}^{opt}, \hat{\boldsymbol{\theta}}_k^{opt})$.
```

Proof: Please see Appendix C. □

On the basis of the above proposition, the secure transmission scheme for multiple eavesdroppers can be summarized as Algorithm 3, which can both resist BS-IRS link-eavesdropping and IRS-user link-eavesdropping attacks.

VI. Simulation Results and Analysis

This section will validate the accuracy and effectiveness of our proposed theoretical results and present the worst-case secrecy rate performance for the IRS-assisted THz system with blocking eavesdroppers. In the following, all simulation results are obtained by averaging over 10^3 independent trials. To evaluate blocking effects of eavesdroppers on confidential information transmission, all users are assumed to be located in a three-dimensional space. In particular, BS and Bob are located at (0,0,2.5) and (50,0,1.4) in meter (m), respectively. Meanwhile, the eavesdropper and multiple IRSs are randomly distributed in the communication area. We assume that IRSs are installed at a height of 2 m, and the height of eavesdroppers is 1.8 m for IRS-user link eavesdropping activity or 2.3 m for BS-IRS link eavesdropping activity.[9] Unless otherwise specified, the transmit frequency and transmit power at the BS with $M = 5^2$ antennas are set to $f = 0.3$ THz and $P_s = 20$ dBm, respectively. In our considered system, there are $K = 3$ IRSs in total and each of them is equipped with $N = 6^2$ reflecting elements. Besides, the antenna gain is set to 14 dBi, the number of paths is $L = 3$ and the absorption coefficient of the medium can be obtained with the help of HITRAN database [35].

A. BS-IRS Link Eavesdropping With Single Eve

As THz waves are vulnerable to blockage events, secure communication in such high-frequency bands may suffer both malicious eavesdropping attacks and additional blockages by eavesdroppers within THz beams. Therefore, the power loss caused by eavesdropper blocking is one of the crucial factors influencing the secure transmission design in THz bands. Fig. 5 gives the worst-case secrecy rate performance of IRS-assisted THz systems with BS-IRS link eavesdropping attacks, wherein two benchmark scenarios are included and the blocking-based power loss varies from -20 dB to 0 dB. "Block-Free" denotes the scenario where the eavesdropper intercepts signals without blocking. "Block-Unaware" is the scenario with blocking eavesdropper, but legal users are not aware the blocking effects on secure transmission.

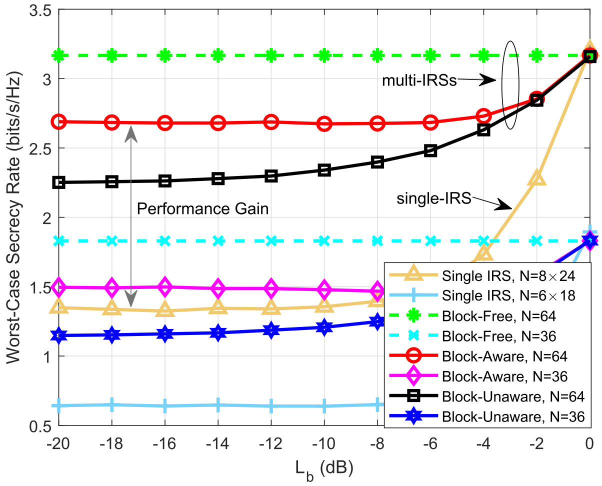


Fig. 5. WCSR performance versus the blockage-based power loss L_b, in which the BS-IRS link is intercepted by Eve.

It can be seen from Fig. 5 that with the increase of L_b, the secrecy rate increases consistently and is upper-bounded by that of the blockage-free system. The reason for this phenomenon is that the increased L_b means the less confidential information transmission between BS-IRS links blocked by eavesdroppers, which consequently leads to less secrecy performance loss. Specifically, when $N = 64$ reflecting elements are provided by each IRS, 14.8% of secrecy performance gain of the blockage-aware scheme is lost from $L_b = 0$ dB to $L_b = -20$ dB. In comparison, the secrecy performance loss is more than 28.7% for blockage-unaware scheme. This demonstrates that the successful awareness of blocking eavesdroppers is a crucial issue in protecting secure THz communications. It also shows that our proposed scheme has superb performance in reducing the loss of secrecy rate. Besides, since the large-scale reflecting elements equipped at each IRS can enable sharper reflecting beams, more signal power can be steered to the desired user Bob. Thereby, compared with $N = 36$, the secrecy performance for $N = 64$ is enhanced. Moreover, it also can be seen that compared with the scenario centralizing all NK elements in one large IRS ("Single IRS"), when $L_b = -16$ dB and $N = 64$ our proposed multi-IRS scenario can bring more than twice the secrecy performance gain.

In the IRS-assisted secure THz communications, increasing transmit power at the BS can not only enhance the received confidential signal power at the desired user, but also increase

[9] In this case, an eavesdropper can be an unmanned aerial vehicle or other human-controlled wireless receive points.

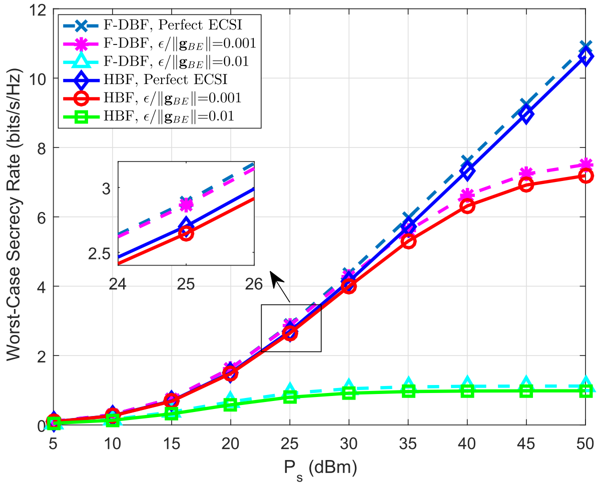


Fig. 6. WCSR versus the transmit power P_s at the BS, in which the BS-IRS link is intercepted by Eve.

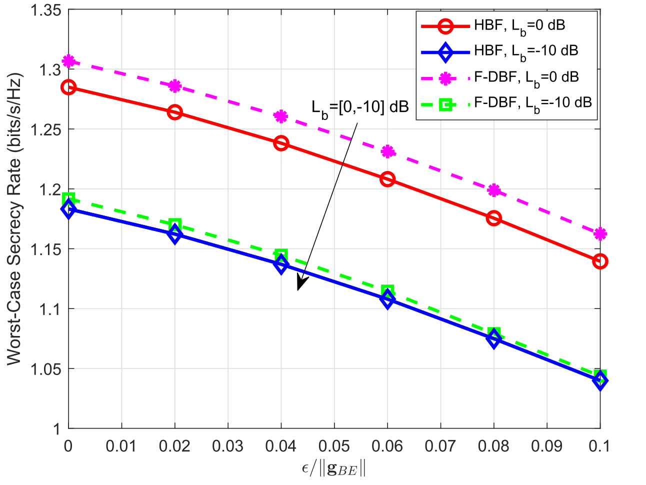


Fig. 7. WCSR versus the level of bounded uncertainty region of ECSI, in which the IRS-user link is intercepted, and $L_b = [-10, 0]$ dB and $N = 6^2$.

the information leakage at eavesdroppers. Fig. 6 illustrates the worst-case secrecy rate performance with different transmit power P_s in the presence of BS-IRS link eavesdropping attacks. We can observe that with the imperfect ECSI, the secrecy rate increases with P_s in the lower power regime, while for the high power regime, the secrecy rate increase slowly. It is because of the close distance between Eve and BS and THz beam misalignment caused by imperfect ECSI, excessive power at the BS leads to more information leakage, rather than information rate enhancement at desired users. In comparison, since the accurate ECSI can be used to design optimal beamforming and reflecting phase shifts, the information leakage in perfect ECSI transmission can be suppressed using the ZF beamforming scheme. Thus the WCSR can monotonically increase with the transmit power P_s. Besides, compared with the conventional fully-digital beamforming scheme ('F-DBF'), our proposed hybrid beamforming scheme ('HBF') achieves satisfactory secrecy performance with a smaller number of RF chains and lower complexity.

B. IRS-User Link Eavesdropping With Single Eve

It is generally known that the randomness of wireless channels is used to design secure transmission schemes in the physical layer, and the availability of ECSI determines the achievable secrecy performance. Fig. 7 shows the impact of ECSI uncertainty on the secrecy performance of the IRS-user link eavesdropping attack. Results reveal that the increased level of ECSI uncertainty leads to a degraded secrecy rate performance. The reason is that the imperfect ECSI makes the inefficiency of transmit beamforming and reflecting beamforming design, which in turn yields a serious information leakage at eavesdroppers, finally resulting in secrecy performance loss. Besides, results also show that the WCSR performance of our proposed hybrid beamforming scheme approaches that of the fully-digital beamforming scheme. The secrecy performance loss of hybrid beamforming is because of the limited number of RF chains and the modulus constraint. Nevertheless, the comparable secrecy performance demonstrates the effectiveness of our proposed hybrid beamforming scheme. In addition, as analyzed in Fig. 5, the blockage of eavesdroppers also performs destructive effects on secure transmission in IRS-assisted THz systems.

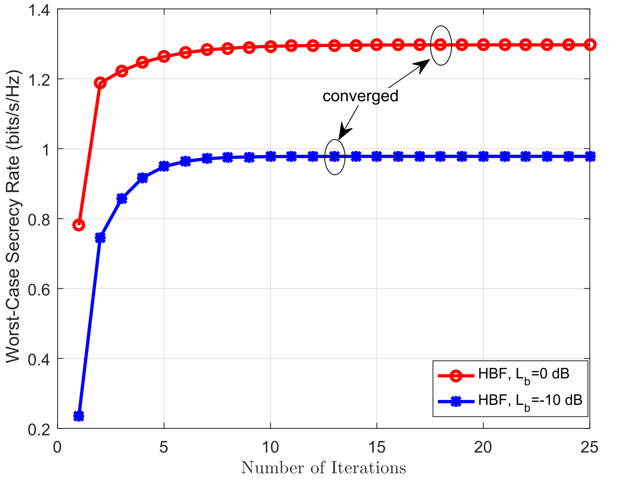


Fig. 8. Convergence performance of Algorithm 2 (i.e., iterative algorithm), wherein $N = 6^2$ and $\epsilon/\|\mathbf{g}_E\| = 0.02$, $\mathbf{g}_E$ denoting $\mathbf{g}_{BE}$ and $\mathbf{g}_{IE}$.

As described in Section IV, all results in Fig. 7 are obtained via our proposed iterative algorithm. Intuitively, the effectiveness and performance of an iterative algorithm depend on its convergence. Taking one transmission block as an example, we study the convergence property of our proposed algorithm when $\epsilon/\|\mathbf{g}_E\| = 0.02$. As shown in Fig. 8, the proposed algorithm monotonically converges under different blocking conditions and it has a fast convergence speed. In particular, the worst-case secrecy rate value reaches a plateau after 13 iterations on average for the scenario of $L_b = -10$ dB. For the blockage-free condition, i.e., $L_b = 0$ dB, the worst-case secrecy rate value can also reach its plateau after 18 iterations on average. The results

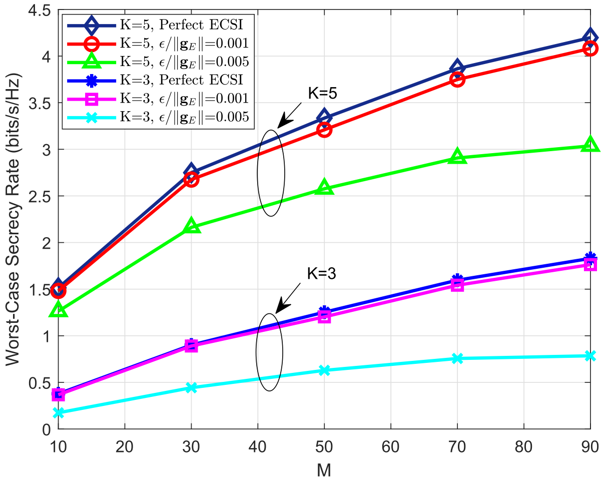


Fig. 9. WCSR versus the number of antennas at the BS, wherein $K_E = 3$ eavesdroppers intercept $K = [3, 5]$ IRS-assist information transmission.

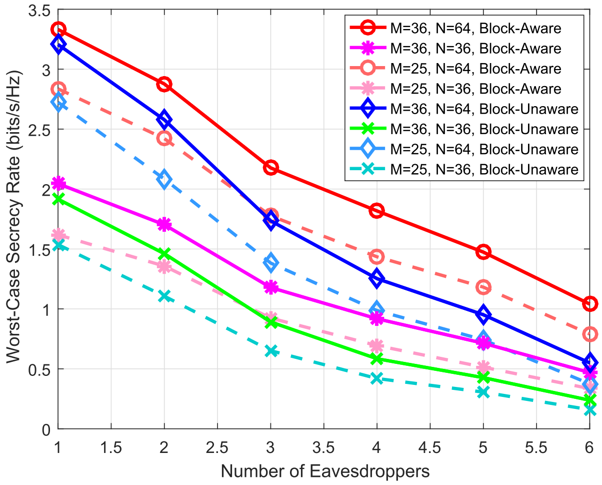


Fig. 10. WCSR versus the number of multiple eavesdroppers, in which the number of IRSs is set to $K = 3$.

of Fig. 8 indicates that the theoretical analysis in Section IV is valid from the simulation perspective.

C. Secure Communications With Multiple Eavesdroppers

We study the secrecy performance of the multi-IRS-assisted THz system in the presence of multiple eavesdroppers. Since multiple eavesdroppers can intercept different links between legal users (BS and Bob) and multiple IRSs, the worst-case secrecy rate versus the number of IRSs and eavesdroppers are respectively investigated. As shown in Fig. 9, it is evident that as the number of IRSs K increases from 3 to 5, the secrecy rate increases monotonously. The reason is that compared with $K = 3$, $K = 5$ IRSs can provide more paths and spatial degrees of freedom for confidential information transmission, a large amount of confidential signal power is steered to the desired destination, and the information leakage at eavesdroppers is suppressed. Thereby the secrecy rate is enhanced via multiple IRSs. Besides, due to the sharper transmit beams offered by multiple antennas, increasing the number of transmit antennas M at the BS is beneficial for secrecy performance improvement.

Fig. 10 illustrates the secrecy rate performance with different numbers of eavesdroppers. Results reveal that multiple eavesdroppers can intuitively intercept more confidential signals than the single-eavesdropper systems, leading to profound secrecy rate loss. Moreover, in terms of the blockage-prone nature of THz waves, eavesdroppers can also severely degrade the received signal strength at Bob and the system secrecy rate gain because of their blockage effects. In particular, when $M = 36$ transmit antennas and $N = 64$ reflecting elements are equipped, $K_E = 6$ eavesdroppers in a blockage-aware THz system lead to about 2.2 bits/s/Hz secrecy rate loss than the case of $K_E = 1$ eavesdropper. In comparison, 14.2% of secrecy rate gain of blockage-unaware systems will be additionally degraded. Such severe performance loss demonstrates that eavesdroppers' blockage is as essential as their interception behaviors for THz systems, and the awareness of blocking is one of the key aspects to determine the security of THz communications.

VII. Conclusion

This paper investigated the hybrid beamforming and reflecting beamforming design for securing IRS-assisted THz systems. In terms of the blockage-prone nature in the THz band, the blocking-based path loss is investigated and two types of blocking eavesdropping attacks were introduced, i.e., BS-IRS link eavesdropping and IRS-user link eavesdropping. To maximize secrecy rate performance, the joint optimization problem of hybrid beamforming at the BS and reflecting phase shifts at multiple IRSs was formulated. For the BS-IRS link eavesdropping attack, an alternative method was proposed to design ZF-principle-based hybrid beamformer and reflecting beamformer. For IRS-user link-based eavesdropping, an SDP method-enabled iterative algorithm was proposed to derive solutions of beamformers. Finally, the robust secure transmission scheme was proposed to against multiple blocking eavesdroppers in IRS-assisted THz systems. Simulation results have revealed that because of the captured blockage-prone nature of THz waves, our proposed secure transmission scheme can significantly boost secrecy rate performance and resist both BS-IRS link-eavesdropping and IRS-user link-eavesdropping attacks. The blocking eavesdropping attack is under our current study, and the secure THz communication design subjected to unpredictable blockage will be considered in our future work.

Appendix A
Proof of Proposition 1

Before solving the optimization problem, the constraints will be first analyzed. On the one hand, a power control factor $0 \leq \delta \leq 1$ is defined, then the power constraint in problem P1.2$'$ is rewritten as $\|\mathbf{w}\|^2 = \|\mathbf{F}_{RF}\mathbf{f}_{BB}\|^2 = \delta P_s$. Under the positive secrecy rate constraint $\gamma_D > \max_k \gamma_{ewc,k}$, we can formulate the system WCSR as a function of δ, i.e., $R_s^{wc}(\delta) = \frac{1+a_1\delta}{1+a_2\delta}$, where parameters can be obtained on the basis of equation (42). By determining the sign of derivative of $R_s^{wc}(\delta)$, it is proved that the WCSR is an increasing function of δ, i.e., the optimal $\delta^{opt} = 1$.

That is, the WCSR $R_s^{wc}(\mathbf{w})$ can be maximized only when the power constraint of hybrid beamformer satisfies $\|\mathbf{w}\|^2 = P_s$.

On the other hand, to implement ZF beamforming, we first define matrix $\mathbf{B}$ as the null space of $\bar{\mathbf{g}}_{BE}^H$. Then, the hybrid beamformer can be written as a linear combination of the basis of the null space of $\bar{\mathbf{g}}_{BE}^H$. Define $\mathbf{v}$ as a column vector, then we have $\mathbf{w} = \mathbf{B}\mathbf{v}$. Thus, the optimization problem of digital beamformer $\mathbf{w}$ can be rewritten as

$$\max_{\mathbf{v}} \frac{\mathbf{v}^H\mathbf{B}^H\left[\frac{1}{P_s}\mathbf{I}_N + \mathbf{R}_{BD}\right]\mathbf{B}\mathbf{v}}{\mathbf{v}^H\mathbf{B}^H\left[\frac{1}{P_s}\mathbf{I}_N + \epsilon^2\mathbf{R}_{BE}\right]\mathbf{B}\mathbf{v}}, \text{ s.t. } \|\mathbf{B}\mathbf{v}\|^2 = P_s.$$

Since the matrices $\frac{1}{P_s}\mathbf{B}^H\mathbf{B} + \mathbf{B}^H\mathbf{R}_{BD}\mathbf{B}$ and $\frac{1}{P_s}\mathbf{B}^H\mathbf{B} + \epsilon^2\mathbf{B}^H\mathbf{R}_{BE}\mathbf{B}$ are diagonal, the above problem is a generalized eigenvector problem, thereby the solution can be obtained as $\mathbf{v}^{opt} = \mu\mathbf{q}^{unit}$. The scalar μ is determined by the power constraint, hence $\mu = \sqrt{P_s/(\mathbf{q}^{unit})^H\mathbf{B}^H\mathbf{B}\mathbf{q}^{unit}}$. $\mathbf{q}^{unit}$ is the unit-norm eigenvector of matrix $[\frac{1}{P_s}\mathbf{B}^H\mathbf{B} + \epsilon^2\mathbf{B}^H\mathbf{R}_{BE}\mathbf{B}]^{-1}[\frac{1}{P_s}\mathbf{B}^H\mathbf{B} + \mathbf{B}^H\mathbf{R}_{BD}\mathbf{B}]$ corresponding to the maximum eigenvalue. Therefore, optimal $\mathbf{w}$ can be obtained as

$$\mathbf{w}^{opt} = \sqrt{\frac{P_s}{(\mathbf{q}^{unit})^H\mathbf{B}^H\mathbf{B}\mathbf{q}^{unit}}}\mathbf{B}\mathbf{q}^{unit}.$$

Appendix B
Proof of Proposition 2

Here, to facilitate hybrid beamforming design, the analog and digital precoders are temporarily coupled together. In detail, for the objective function in problem P2.1, it can be proved that the IRS-assisted confidential communication between BS and Bob is equivalent to a MISO system. Thus, the hybrid beamformer should be directed in the same direction as the MRT (Maximum Ratio Transmission) beamforming, i.e.,

$$\mathbf{f}_{BB}^{opt} = \mu\mathbf{q} = \frac{\mathbf{F}_{RF}^H\mathbf{H}_{BI}\text{diag}\{\boldsymbol{\phi}^*\}\mathbf{h}_D}{\|\mathbf{F}_{RF}^H\mathbf{H}_{BI}\text{diag}\{\boldsymbol{\phi}^*\}\mathbf{h}_D\|},$$

where $\|\mathbf{q}\|^2 = 1$, and μ is a scalar, which can be determined based on the power constraint and a given information leakage threshold.

Substituting $\mathbf{f}_{BB}^{opt}$ into the first given information leakage threshold constraint in P2.1, then we have

$$\mu \leq \frac{\sqrt{\gamma_0}\sigma_E}{|\bar{\mathbf{g}}_{IE}^H\boldsymbol{\Theta}_m\mathbf{H}_{BI,m}^H\mathbf{F}_{RF}\mathbf{q}| + \epsilon\|\mathbf{H}_{BI,m}^H\mathbf{F}_{RF}\mathbf{q}\|}.$$

While according to the transmit power constraint in the original problem, μ also satisfies $\mu \leq \sqrt{P_s}$.

Appendix C
Proof of Proposition 3

With partial eavesdropper CSI, we define the gap between the maximum SNR received from BS-IRS links and the maximum SNR received by IRS-user links as

$$\gamma_h = \sqrt{\max_{i\in\mathcal{K}_B}\max_{\|\Delta\mathbf{g}_E\|\leq\epsilon}\gamma_{E,i}^B} - \sqrt{\max_{j\in\mathcal{K}_I}\max_{\|\Delta\mathbf{g}_E\|\leq\epsilon}\gamma_{E,j}^I} = a - b.$$

Here we assume that $p = \arg\max_{i\in\mathcal{K}_B}\max_{\|\Delta\mathbf{g}_E\|\leq\epsilon}\gamma_{E,i}^B$ and $q = \arg\max_{j\in\mathcal{K}_I}\max_{\|\Delta\mathbf{g}_E\|\leq\epsilon}\gamma_{E,j}^I$, then we have the parameters $a = |\bar{\mathbf{g}}_{BE,p}^H\mathbf{F}_{RF}\mathbf{f}_{BB}| - |\bar{\mathbf{g}}_{IE,q}^H\boldsymbol{\Theta}_q\mathbf{H}_{BI,q}^H\mathbf{F}_{RF}\mathbf{f}_{BB}| = a_1 - a_2$,$b = \epsilon(\|\boldsymbol{\Theta}_q\mathbf{H}_{BI,q}^H\mathbf{F}_{RF}\mathbf{f}_{BB}\| - \|\mathbf{F}_{RF}\mathbf{f}_{BB}\|) = b_1 - b_2$. Compared with the estimated channel $\bar{\mathbf{g}}_{BE,p}$ and $\bar{\mathbf{g}}_{IE,q}$, the error bound ϵ is very small, thus we have $|a| > |b|$. In the following, to determine the analytical expression of $\gamma_{ewc}^{\max}$ in (43), the sign of γ_h is analyzed.

- For $a > 0$ and $b > 0$, we have positive-definite matrix $\bar{\mathbf{g}}_{BE,p}\bar{\mathbf{g}}_{BE,p}^H - \mathbf{H}_{BI,q}\boldsymbol{\Theta}_q^H\bar{\mathbf{g}}_{IE,q}\bar{\mathbf{g}}_{IE,q}^H\boldsymbol{\Theta}_q\mathbf{H}_{BI,q}^H \succ 0$ and $\mathbf{H}_{BI,q}\mathbf{H}_{BI,q}^H - \mathbf{I}_M \succ 0$. On the basis of $|a| > |b|$, it can be obtained that $\gamma_h = a - b > 0$.
- For $a > 0$ and $b \leq 0$, we have positive definite matrix $\bar{\mathbf{g}}_{BE,p}\bar{\mathbf{g}}_{BE,p}^H - \mathbf{H}_{BI,q}\boldsymbol{\Theta}_k^H\bar{\mathbf{g}}_{IE,q}\bar{\mathbf{g}}_{IE,q}^H\boldsymbol{\Theta}_q\mathbf{H}_{BI,q}^H \succ 0$ and $\mathbf{I}_M - \mathbf{H}_{BI,q}\mathbf{H}_{BI,q}^H \succeq 0$. It is obvious that in this case $\gamma_h > 0$ holds.
- For $a \leq 0$ and $b > 0$, we have non-positive definite matrix $\bar{\mathbf{g}}_{BE,p}\bar{\mathbf{g}}_{BE,p}^H - \mathbf{H}_{BI,q}\boldsymbol{\Theta}_q^H\bar{\mathbf{g}}_{IE,q}\bar{\mathbf{g}}_{IE,q}^H\boldsymbol{\Theta}_q\mathbf{H}_{BI,q}^H \preceq 0$, and $\mathbf{I}_M - \mathbf{H}_{BI,q}\mathbf{H}_{BI,q}^H \prec 0$. Obviously, γ_h is less than 0.
- For $a \leq 0$ and $b \leq 0$, we have non-positive definite matrix $\bar{\mathbf{g}}_{BE,p}\bar{\mathbf{g}}_{BE,p}^H - \mathbf{H}_{BI,q}\boldsymbol{\Theta}_q^H\bar{\mathbf{g}}_{IE,q}\bar{\mathbf{g}}_{IE,q}^H\boldsymbol{\Theta}_q\mathbf{H}_{BI,q}^H \preceq 0$ and $\mathbf{H}_{BI,q}\mathbf{H}_{BI,q}^H - \mathbf{I}_M \preceq 0$. On the basis of $|a| > |b|$, it can be proved that $\gamma_h < 0$.

In summary, if we have $\mathbf{H}_{BI,q}\boldsymbol{\Theta}_q^H\bar{\mathbf{g}}_{IE,q}\bar{\mathbf{g}}_{IE,q}^H\boldsymbol{\Theta}_q\mathbf{H}_{BI,q}^H - \bar{\mathbf{g}}_{BE,q}\bar{\mathbf{g}}_{BE,p}^H \succ 0$, the maximum SNR received among all eavesdroppers is $\gamma_{ewc}^{\max} = \gamma_{ewc,q}^I$, otherwise $\gamma_{ewc}^{\max} = \gamma_{ewc,p}^B$.

References

[1] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?," *Nature Electron.*, vol. 3, pp. 20–29, Jan. 2020.

[2] H. Elayan, O. Amin, B. Shihada, R. M. Shubair, and M.-S. Alouini, "Terahertz band: The last piece of RF spectrum puzzle for communication systems," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1–32, Jan. 2020.

[3] M. H. Loukil, H. Sarieddeen, M.-S. Alouini, and T. Y. Al-Naffouri, "Terahertz-band MIMO systems: Adaptive transmission and blind parameter estimation," *IEEE Commun. Lett.*, vol. 25, no. 2, pp. 641–645, Feb. 2021.

[4] H. Sarieddeen, M.-S. Alouini, and T. Y. Al-Naffouri, "An overview of signal processing techniques for terahertz communications," *Proc. IEEE*, vol. 109, no. 10, pp. 1628–1665, Oct. 2021.

[5] H. Sarieddeen, N. Saeed, T. Y. Al-Naffouri, and M.-S. Alouini, "Next generation terahertz communications: A rendezvous of sensing, imaging, and localization," *IEEE Commun. Mag.*, vol. 58, no. 5, pp. 69–75, May 2020.

[6] J. Ma *et al.*, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, pp. 89–93, Oct. 2018.

[7] Z. Wan, Z. Gao, F. Gao, M. D. Renzo, and M.-S. Alouini, "Terahertz massive MIMO with holographic reconfigurable intelligent surfaces," *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4732–4750, Jul. 2021.

[8] M. D. Renzo *et al.*, "Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come," *J. Wireless Commun. Netw.*, vol. 2019, pp. 1–20, May 2019.

[9] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

[10] S. Nie and I. F. Akyildiz, "Beamforming in intelligent environments based on ultra-massive MIMO platforms in millimeter wave and terahertz bands," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, 2020, pp. 8683–8687.

[11] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

[12] J. Ye, J. Qiao, A. Kammoun, and M.-S. Alouini, "Non-terrestrial communications assisted by reconfigurable intelligent surfaces," *Proc. IEEE*, 2022.

[13] Q. Wu and R. Zhang, "Beamforming optimization for wireless network aided by intelligent reflecting surface with discrete phase shifts," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1838–1851, Mar. 2020.

[14] Q. Nadeem, A. Kammoun, A. Chaaban, M. Debbah, and M.-S. Alouini, "Asymptotic max-min SINR analysis of reconfigurable intelligent surface assisted MISO systems," *IEEE Trans. Wireless Commun.*, vol. 19, no. 12, pp. 7748–7764, Dec. 2020.

[15] Q. Nadeem, H. Alwazani, A. Kammoun, A. Chaaban, M. Debbah, and M.-S. Alouini, "Intelligent reflecting surface assisted multi-user MISO communication: Channel estimation and beamforming design," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 661–680, Jun. 2020.

[16] B. Ning, Z. Chen, W. Chen, Y. Du, and J. Fang, "Terahertz multi-user massive MIMO with intelligent reflecting surface: Beam training and hybrid beamforming," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1376–1393, Feb. 2021.

[17] Z. Wan, Z. Gao, and M.-S. Alouini, "Broadband channel estimation for intelligent reflecting surface aided mmWave massive MIMO systems," in *Proc. IEEE Int. Conf. Commun.*, 2020, pp. 1–6.

[18] N. S. Perović, M. D. Renzo, and M. F. Flanagan, "Channel capacity optimization using reconfigurable intelligent surfaces in indoor mmWave environments," in *Proc. IEEE Int. Conf. Commun.*, 2020, pp. 1–7.

[19] M. T. Barros, R. Mullins, and S. Balasubramaniam, "Integrated terahertz communication with reflectors for 5G small-cell networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 5647–5657, Jul. 2017.

[20] P. Wang, J. Fang, X. Yuan, Z. Chen, and H. Li, "Intelligent reflecting surface-assisted millimeter wave communications: Joint active and passive precoding design," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 14960–14973, Dec. 2020.

[21] Y. Cao, T. Lv, and W. Ni, "Intelligent reflecting surface aided multi-user mmWave communications for coverage enhancement," in *Proc. IEEE Annu. Int. Symp. Pers., Indoor Mobile Radio Commun.*, 2020, pp. 1–6.

[22] X. Ma *et al.*, "Intelligent reflecting surface enhanced indoor terahertz communication systems," *Nano Commun. Netw.*, vol. 24, pp. 1–9, May 2020.

[23] Z. Chen, W. Chen, X. Ma, Z. Li, Y. Chi, and C. Han, "Taylor expansion aided gradient descent schemes for IRS-enabled terahertz MIMO systems," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops*, 2020, pp. 1–7.

[24] W. Chen, X. Ma, Z. Li, and N. Kuang, "Sum-rate maximization for intelligent reflecting surface based terahertz communication systems," in *Proc. IEEE/CIC Int. Conf. Commun. Workshops China*, 2019, pp. 153–157.

[25] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 2, pp. 1027–1053, Apr.–Jun. 2017.

[26] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[27] J. Qiao, H. Zhang, X. Zhou, and D. Yuan, "Joint beamforming and time switching design for secrecy rate maximization in wireless-powered FD relay systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 567–579, Jan. 2018.

[28] J. Qiao, H. Zhang, F. Zhao, and D. Yuan, "Secure transmission and self-energy recycling with partial eavesdropper CSI," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1531–1543, Jul. 2018.

[29] V. Petrov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Exploiting multipath terahertz communications for physical layer security in beyond 5G networks," in *Proc. IEEE Conf. Comput. Commun. Workshops*, 2019, pp. 865–872.

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

[31] B. Ning, Z. Chen, W. Chen, and L. Li, "Improving security of THz communication with intelligent reflecting surface," in *Proc. IEEE Globecom Workshops*, 2019, pp. 1–6.

[32] 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. 2068–2072, Dec. 2020.

[33] L. You *et al.*, "Network massive MIMO transmission over millimeter-wave and terahertz bands: Mobility enhancement and blockage mitigation," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 12, pp. 2946–2960, Dec. 2020.

[34] C. Han, J. M. Jornet, and I. F. Akyildiz, "Ultra-massive MIMO channel modeling for graphene-enabled terahertz-band communications," in *Proc. IEEE Veh. Technol. Conf.*, 2018, pp. 1–5.

[35] J. M. Jornet and I. F. Akyildiz, "Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3211–3221, Oct. 2011.

[36] V. Nurmoth *et al.*, "Deliverable D1.4 METIS channel models," in *Proc. Mobile Wireless Commun. Enablers Inf. Soc.*, 2015, pp. 35–51.

[37] C. Han, A. O. Bicen, and I. F. Akyildiz, "Multi-ray channel modeling and wideband characterization for wireless communications in the terahertz band," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2402–2412, May 2015.

[38] A. F. Molisch *et al.*, "Hybrid beamforming for massive MIMO: A survey," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 134–141, Sep. 2017.

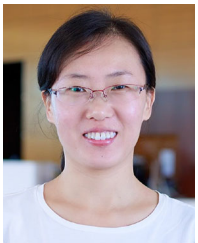
[39] Z. Zhang, Y. Cui, F. Yang, and L. Ding, "Analysis and optimization of outage probability in multi-intelligent reflecting surface-assisted systems," Sep. 2019. [Online]. Available: https://arxiv.org/abs/1909.02193

[40] H. Yuan, N. Yang, K. Yang, C. Han, and J. An, "Hybrid beamforming for terahertz multi-carrier systems over frequency selective fading," *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6186–6199, Oct. 2020.

[41] S. Wang, X. Xu, K. Huang, X. Ji, Y. Chen, and L. Jin, "Artificial noise aided hybrid analog-digital beamforming for secure transmission in MIMO millimeter wave relay systems," *IEEE Access*, vol. 7, pp. 28597–28606, 2019.

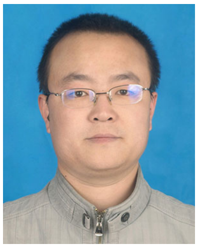
[42] C. Fang, B. Makki, J. Li, and T. Svensson, "Hybrid precoding in cooperative millimeter wave networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 5373–5388, Aug. 2021.

[43] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2009.



Jingping Qiao (Member, IEEE) received the B.E. degree from the School of Information Engineering, Inner Mongolia University of Science & Technology, Baotou, China, in 2012, and the Ph.D. degree from Shandong University, Jinan, China, in 2018. She is currently a Lecturer with the School of Information Science and Engineering, Shandong Normal University. From 2019 to 2021, she was a Visiting Scholar with the Computer, Electrical and Mathematical Science and Engineering Division, King Abdullah University of Science and Technology, Thuwal, Saudi Arabia. Her research interests include physical layer security, cooperative (relay) systems, terahertz communications, intelligent reflecting surface, and signal processing for wireless communications.

Chuanting Zhang (Member, IEEE) received the B.S. and M.S. degrees in computer science from the Inner Mongolia University of Science and Technology, Baotou, China, in 2011 and 2014, respectively, and the Ph.D. degree in communication and information systems from Shandong University, Jinan, China. He is currently a Senior Research Associate with the University of Bristol, Bristol, U.K. He was a Postdoctoral Fellow with the Computer, Electrical and Mathematical Science and Engineering Division, King Abdullah University of Science and Technology, Thuwal, Saudi Arabia. His research interests include spatial-temporal data analysis, federated learning, and graph mining.



Anming Dong (Member, IEEE) received the B.E. degree in electronic information science and technology from Liaocheng University, Liaocheng, China, in 2004, the M.E. degree in communications and information systems from Lanzhou University, Lanzhou, China, in 2007, and the Ph.D. degree in communications and information systems from Shandong University, Jinan, China, in 2016. From 2016 to 2021, he was with the School of Computer Science and Technology, Qilu University of Technology (Shandong Academy of Sciences), Jinan. He is currently an Associate Professor with the Big Data Institute & School of Mathematics and Statistics, Qilu University of Technology. His research interests include MIMO techniques, deep learning for wireless communications, and optimization techniques for signal processing and wireless communications. He was the recipient of the Excellent Doctoral Dissertation Awards of Shandong Province, in 2017.

Ji Bian (Member, IEEE) received the B.Sc. degree in electronic information science and technology from Shandong Normal University, Jinan, Chian, in 2010, the M.Sc. degree in signal and information processing from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2013, and the Ph.D. degree in information and communication engineering from Shandong University, in 2019. From 2017 to 2018, he was a Visiting Scholar with the School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, U.K. He is currently a Lecturer with the School of Information Science and Engineering, Shandong Normal University. His research interests include 6G channel modeling and wireless Big Data.

Mohamed-Slim Alouini (Fellow, IEEE) was born in Tunis, Tunisia. He received the Ph.D. degree in electrical engineering from the California Institute of Technology, Pasadena, CA, USA, in 1998. He was a Faculty Member with the University of Minnesota, Minneapolis, MN, USA, and then with Texas A&M University at Qatar, Education City, Doha, Qatar, before joining the King Abdullah University of Science and Technology, Thuwal, Saudi Arabia, as a Professor of electrical engineering, in 2009. His research interests include the modeling, design, and performance analysis of wireless communication systems.