Secrecy Analysis of RIS-Aided mmWave Systems over Independent Fluctuating Two-Ray Fading Channels

Phuc V. Trinh and Shinya Sugiura*
Institute of Industrial Science, The University of Tokyo, Tokyo 153-8505, Japan
Email: {trinh, sugiura}@iis.u-tokyo.ac.jp

***Abstract*—In this paper, we examine a millimeter-wave (mmWave) wiretap scenario where a multiple-antenna base station (Alice) communicates with a legitimate user (Bob) via a reconfigurable intelligent surface, while multiple colluding eavesdroppers (Eves) attempt to passively intercept the communications using the maximal-ratio combining scheme. We develop a framework for achieving the maximum effective secrecy throughput (EST) that meets both reliability and secrecy constraints. Firstly, we derive a generalized and tractable form of the independent fluctuating two-ray (IFTR) distribution for accurately modeling mmWave fading channels. Secondly, we propose a novel approximation method to statistically characterize the end-to-end channels, considering the phase-shift estimation errors at both Bob and the colluding Eves over the IFTR channels. Finally, we derive a new closed-form EST metric and its asymptotic expression.**

I. Introduction

Millimeter-wave (mmWave) frequencies offer significantly more bandwidth than traditional microwave frequencies. However, their high directivity and significant attenuation require precise beamforming. Recently, reconfigurable intelligent surfaces (RISs) have been proposed to overcome blockages caused by obstacles like buildings and trees. Furthermore, physical-layer security (PLS) emerges as a key defense mechanism, offering *information-theoretic security*. Early seminal studies introduced the wiretap scenario, where an eavesdropper (Eve) attempts to intercept the communications between a transmitter (Alice) and a receiver (Bob) [1]. Achieving information-theoretic security requires the eavesdropping channel capacity ($C_{\rm E}$) to be smaller than the legitimate channel capacity ($C_{\rm B}$), resulting in a secrecy capacity ($C_{\rm s}$) equal to the difference between $C_{\rm B}$ and $C_{\rm E}$. The *reliability constraint* is met if the codeword rate $R_{\rm c}$ does not exceed $C_{\rm B}$, while the *secrecy constraint* requires the redundancy rate $R_{\rm r}=R_{\rm c}-R_{\rm s}$ to be higher than $C_{\rm E}$, with the target secrecy rate $R_{\rm s}$.

Alice can satisfy the reliability constraint if the legitimate channel's instantaneous channel state information (CSI) is known. However, the secrecy constraint may not be guaranteed due to a lack of Eve's instantaneous CSI in passive eavesdropping scenarios. Therefore, it is more practical to assume that Alice has knowledge of the average CSI of the eavesdropping channel [2]. Recently, the effective secrecy throughput (EST) has been introduced, which captures both the reliability and secrecy constraints of wiretap channels [3], [4]. The EST determines *the average rate of confidential information transmitted from Alice to Bob without being eavesdropped on*. Furthermore, the EST can be maximized by adaptively adjusting $R_{\rm c}$ and $R_{\rm s}$ according to $C_{\rm B}$ [3] (i.e., adaptive-rate scheme), considering the maximum secrecy outage due to the eavesdropping channel denoted as $P_{\rm out}^{\rm Eve}$ [4]. The EST of the adaptive-rate scheme has not been studied in the context of RIS-aided mmWave PLS.

Given the high complexity of the RIS-induced multiplicative fading channels, only a few studies have investigated the information-theoretic PLS of RIS-aided mmWave systems over Rician channels [5], [6]. Generally, mmWave links are often described using the Rician fading model, incorporating a dominant line-of-sight (LoS) component along with scattered ones. However, in 2017, the fluctuating two-ray (FTR) fading model, which considers two fluctuating LoS components alongside a diffuse component, proved to offer a better fit compared to the Rician model [7]. In 2023, a more generalized independent FTR (IFTR) model was introduced, where the two LoS components fluctuate independently and experience differing fading severity [8].

In this paper, we investigate the information-theoretic EST of an RIS-aided mmWave system that satisfies both reliability and secrecy constraints using the adaptive-rate scheme. Furthermore, we consider the phase estimation errors at both Bob and multiple colluding Eves. We newly derive a generalized closed-form expression for the IFTR distribution, a state-of-the-art fading model that accurately captures the statistical characteristics of mmWave channels. We optimize the RIS reflection phase shifts with the maximum ratio transmission (MRT) beamforming at Alice, and derive new approximate closed-form expressions for the received SNR distributions at both Bob and multiple colluding Eves using a maximal-ratio combining (MRC) scheme. We formulate

Preprint for publication in *IEEE Asia-Pacific Conference on Communications*, 2024, DOI: 10.1109/APCC62576.2024.10768064.

the maximum EST of RIS-aided mmWave systems for a given target secrecy rate $R_{\rm s}$ in the adaptive-rate scheme. Exact closed-form expressions for $P_{\rm out}^{\rm Eve}$ and EST along with its asymptotic expression are derived.

II. System and Channel Models

A. System Model

In our wiretap scenario, a BS (Alice) sends confidential messages over mmWave channels to a user (Bob) via an RIS, while E colluding Eves try to intercept. Alice is equipped with M antennas, and both Bob and the e-th Eve ($e = 1, \cdots, E$) have a single antenna. The direct link between Alice and Bob is obstructed and communication link is realized through the RIS. The RIS consists of L passive reflecting elements arranged in a uniform array, configurable via an RIS microcontroller connected to Alice. Considering a passive eavesdropping scenario, Alice knows only the average CSI regarding Eve while possessing the instantaneous CSI for Bob [2].

The signals transmitted from Alice, reflected by the RIS, and received by Bob and the e-th Eve can be expressed, respectively, as $y_{\rm B} = \mathbf{g}_{\rm B}^{\rm H}\mathbf{\Phi}\mathbf{H}\mathbf{f}s + n_{\rm B}$, $y_{{\rm E}_e} = \mathbf{g}_{{\rm E}_e}^{\rm H}\mathbf{\Phi}\mathbf{H}\mathbf{f}s + n_{{\rm E}_e}$, where $\mathbf{f}$ is the normalized beamforming vector, s is the transmit symbol satisfying $\mathbb{E}[|s|^2] = 1$ with $\mathbb{E}[\cdot]$ the statistical expectation, while $n_{\rm B} \sim \mathcal{CN}\left(0, \sigma_{\rm B}^2\right)$ and $n_{{\rm E}_e} \sim \mathcal{CN}\left(0, \sigma_{{\rm E}_e}^2\right)$ are respectively the complex zero-mean additive white Gaussian noise (AWGN) at Bob and the e-th Eve with variances $\sigma_{\rm B}^2$ and $\sigma_{{\rm E}_e}^2$. Additionally, $\mathbf{H} \in \mathbb{C}^{L\times M}$ denotes the channel matrix between Alice and the RIS, where $\mathbf{H} = \left(\mathbf{h}\mathbf{a}_L\left(\theta_{\rm RIS}^{\rm AoA,a}, \theta_{\rm RIS}^{\rm AoA,e}\right)\right)\mathbf{a}_M^H\left(\theta_{\rm BS}^{\rm AoD,a}, \theta_{\rm BS}^{\rm AoD,e}\right)$, with $\mathbf{h} \in \mathbb{C}^{L\times 1}$ the Alice-RIS complex channel coefficient vector, $\mathbf{a}_L\left(\theta_{\rm RIS}^{\rm AoA,a}, \theta_{\rm RIS}^{\rm AoA,e}\right)$ and $\mathbf{a}_M\left(\theta_{\rm BS}^{\rm AoD,a}, \theta_{\rm BS}^{\rm AoD,e}\right)$ the array response vectors containing the azimuth (elevation) angle of arrival (AoA) $\theta_{\rm RIS}^{\rm AoA,a}$ ($\theta_{\rm RIS}^{\rm AoA,e}$) at the RIS and angle of departure (AoD) at the BS $\theta_{\rm BS}^{\rm AoD,a}$ ($\theta_{\rm BS}^{\rm AoD,e}$), respectively. $\mathbf{g}_{\rm B} \in \mathbb{C}^{1\times L}$ and $\mathbf{g}_{{\rm E}_e} \in \mathbb{C}^{1\times L}$ represent the RIS-Bob and RIS-e-th Eve channel vectors, respectively expressed as $\mathbf{g}_{\rm B} = \mathbf{g}_{\rm b}\mathbf{a}_L\left(\theta_{\rm RIS}^{\rm AoD,a}, \theta_{\rm RIS}^{\rm AoD,e}\right)$ and $\mathbf{g}_{{\rm E}_e} = \mathbf{g}_e\mathbf{a}_L\left(\theta_{\rm RIS}^{\rm AoD,a}, \theta_{\rm RIS}^{\rm AoD,e}\right)$, where $\mathbf{g}_{\rm b}$ and $\mathbf{g}_e$ are the complex channel coefficient vectors, $\mathbf{a}_L\left(\theta_{\rm RIS}^{\rm AoD,a}, \theta_{\rm RIS}^{\rm AoD,e}\right)$ denotes the array response vector with the azimuth (elevation) AoD $\theta_{\rm RIS}^{\rm AoD,a}$ ($\theta_{\rm RIS}^{\rm AoD,e}$) at the RIS. Given a uniform square planar array implemented at both Alice and the RIS, the array response vector can be generally expressed as [6], [9]

$$\mathbf{a}_U\left(\theta_P^{A,{\rm a}}, \theta_P^{A,{\rm e}}\right) = \Big[1, \cdots, e^{i2\pi\frac{d}{\lambda}\left(x\sin\left(\theta_P^{A,{\rm a}}\right)\sin\left(\theta_P^{A,{\rm e}}\right) + y\cos\left(\theta_P^{A,{\rm e}}\right)\right)}, \cdots, e^{i2\pi\frac{d}{\lambda}\left(\left(\sqrt{U}-1\right)\sin\left(\theta_P^{A,{\rm a}}\right)\sin\left(\theta_P^{A,{\rm e}}\right) + \left(\sqrt{U}-1\right)\cos\left(\theta_P^{A,{\rm e}}\right)\right)}\Big]^T, \quad (1)$$

where i denotes the imaginary unit, d and λ respectively indicate the element spacing and signal wavelength, $0 \le x, y < \sqrt{U}$ are the element indices in the plane, $U \in \{L, M\}$ denotes the number of elements in the array response vector, $A \in \{\text{AoA}, \text{AoD}\}$ and $P \in \{\text{BS}, \text{RIS}\}$. The phase shifts of all RIS elements are controlled via the diagonal matrix $\mathbf{\Phi} = \text{diag}(\boldsymbol{\rho})$. The amplitude responses are given by $\boldsymbol{\rho} = \left[e^{i\phi_1}, \cdots, e^{i\phi_L}\right]$. Here, $\phi_l \in [-\pi, \pi)$, $(l = 1, \cdots, L)$, is the controlled phase shift of the l-th RIS element.

Theorem 1. *By employing MRT beamforming at Alice and considering phase estimation errors at Bob, the instantaneous received SNR at Bob is given by* $\gamma_B = \bar{\gamma}_B M\left|\sum_{l=1}^{L}|h_l|\,|g_{B,l}|e^{i\tilde{\theta}_{B,l}}\right|^2$, *where* $\bar{\gamma}_B = \frac{E_s}{\sigma_B^2}$ *with* E_s *the average transmitted energy per symbol,* $|h_l|$ *and* $|g_{B,l}|$ *respectively the amplitudes of Alice-RIS and RIS-Bob channels for the* l*-th RIS element, and* $\tilde{\theta}_{B,l}$ *the phase estimation errors at Bob.*

Proof. See Appendix A. □

Lemma 1. *Taking into account the residual phase errors from phase trackers like phase-locked loops (PLL), the phase estimation errors* $\tilde{\theta}_{B,l}$ *at Bob can be modeled by a zero-mean von Mises distribution, expressed as* $f_{\tilde{\theta}_{B,l}}\left(\tilde{\theta}_{B,l}\right) = \frac{e^{\kappa_{PE}\cos\left(\tilde{\theta}_{B,l}\right)}}{2\pi I_0(\kappa_{PE})}$, $\tilde{\theta}_{B,l} \in [-\pi, \pi)$, *where* $I_0(\cdot)$ *denotes the modified Bessel function of the first kind of order zero, and* κ_{PE} *indicates the loop SNR, which is the amount of SNR within the bandwidth of the PLL.*

Proof. It follows from the results of [10], [11]. □

Theorem 2. *Considering phase estimation errors at the* e*-th Eve, the instantaneous received SNR is given as* $\gamma_{E_e} = \bar{\gamma}_{E_e} M\left|\sum_{l=1}^{L}|h_l|\,|g_{E_e,l}|\,e^{i\tilde{\theta}_{E,l}}\right|^2$, *where* $\bar{\gamma}_{E_e} = \frac{E_s}{\sigma_{E_e}^2}$, $|g_{E_e,l}|$ *is the amplitude of the RIS-*e*-th Eve channel for the* l*-th RIS element, and* $\tilde{\theta}_{E,l}$ *denotes the phase estimation errors at the* e*-th Eve.*

Proof. See Appendix B. □

Lemma 2. *Since the MRT beamforming is applied at Alice to maximize the received SNR at Bob, Eve completely lacks knowledge about the channel phases, and thus Eve's phase estimation errors* $\tilde{\theta}_{E,l}$ *are uniformly distributed on* $[-\pi, \pi)$. *As a result,* γ_{E_e} *in Theorem 2 can be rewritten as* $\gamma_{E_e} = \bar{\gamma}_{E_e} ML^2|k_{E_e}|^2$, *where* $|k_{E_e}|^2$ *is exponentially distributed with the probability density function (PDF) expressed as* $f_{|k_{E_e}|^2}\left(|k_{E_e}|^2\right) = \frac{L}{2}e^{-\left(\frac{L}{2}\right)|k_{E_e}|^2}$.

Proof. Following [10, Corollary 2], the phase estimation errors $\tilde{\theta}_{{\rm E},l}$ are uniformly distributed in $[-\pi, \pi)$, thus the equivalent channel of the e-th eavesdropping link $|k_{{\rm E}_e}| \overset{\triangle}{=} \left|\frac{1}{L}\sum_{l=1}^{L}|h_l||g_{{\rm E}_e,l}|e^{i\tilde{\theta}_{{\rm E},l}}\right|$ closely resembles Rayleigh fading with zero-mean and variance $\mathbb{E}[|k_{{\rm E}_e}|^2] = 1/L$. Hence, $\gamma_{{\rm E}_e}$ in Theorem 2 is exponentially distributed by following [5]. This is equivalent to $\gamma_{{\rm E}_e} = \bar{\gamma}_{{\rm E}_e} ML^2|k_{{\rm E}_e}|^2$, with the PDF of $|k_{{\rm E}_e}|^2$ expressed as in Lemma 2. This completes the proof. □

Lemma 3. *Considering the MRC colluding scheme and assuming that eavesdropping links are independent and identically distributed (i.i.d.) with* $\bar{\gamma}_{E_1}=\cdots=\bar{\gamma}_{E_E}=\bar{\gamma}_{E_s}$*, the instantaneous SNR at the super Eve is given as* $\gamma_{E_{MRC}} = \bar{\gamma}_{E_s} ML^2 k_{E_{MRC}}$*, where* $k_{E_{MRC}} = \sum_{e=1}^{E} |k_{E_e}|^2$*. The cumulative distribution function (CDF) of* $k_{E_{MRC}}$ *is expressed as* $F_{k_{E_{MRC}}}(k_{E_{MRC}})=\frac{\gamma\left(\alpha_E,\beta_E k_{E_{MRC}}\right)}{\Gamma(\alpha_E)}$*, where* $\alpha_E=E$*,* $\beta_E = L/2$*, and* $\gamma(\cdot,\cdot)$ *is the lower incomplete Gamma function [12, (8.350.1)].*

Proof. In the MRC scheme, the super Eve combines the instantaneous SNR of all channels, representing the most powerful eavesdropping scenario. Assuming all channels are i.i.d., one should find the distribution of $k_{\mathrm{E_{MRC}}} = \sum_{e=1}^{E} |k_{\mathrm{E}_e}|^2$. From Lemma 2, $|k_{\mathrm{E}_e}|^2$ is exponentially distributed with the rate parameter of $L/2$. Hence, the sum of E i.i.d. exponential RVs follows a Gamma distribution with the shape parameter $\alpha_{\mathrm{E}} = E$ and the inverse scale parameter $\beta_{\mathrm{E}} = L/2$. This completes the proof. □

Remark 1. *From Lemma 3, it is deduced that* $\mathbb{E}[\gamma_{E_{MRC}}]=\bar{\gamma}_{E_s} 2MLE$ *due to* $\mathbb{E}[k_{E_{MRC}}]=\alpha_E/\beta_E=2E/L$*, indicating that* $\mathbb{E}[\gamma_{E_{MRC}}]$ *scales linearly with L, E, and M.*

B. Proposed IFTR Channel Model

In Theorem 1, $|h_l|$ and $|g_{\mathrm{B},l}|$ are assumed to follow the state-of-the-art IFTR fading model. The IFTR model has been proposed recently in [8], and a more tractable representation has been formulated in [13]. The complex baseband voltage of the mmWave channel can be expressed as [8]

$$V = \sqrt{\zeta_1} V_1 e^{i\psi_1} + \sqrt{\zeta_2} V_2 e^{i\psi_2} + X + iY, \qquad (2)$$

where V_1 and V_2 are the average amplitudes of the first and second specular, i.e., LoS, components, while ψ_1 and ψ_2 correspondingly represent the independent and uniformly distributed random phases of the two fluctuating specular waves. The term $X+iY$ in (2) denotes the diffuse component with $X, Y \sim \mathcal{CN}\left(0,\sigma^2\right)$. Moreover, ζ_1 and ζ_2 are the unit-mean Gamma distributed RV with the PDF given by $f_{\zeta_\iota}(\upsilon) = \frac{m_\iota^{m_\iota} \upsilon^{m_\iota-1}}{\Gamma(m_\iota)} e^{-m_\iota \upsilon}$, $\iota=1,2$, where $\Gamma(\cdot)$ denotes the Gamma function [12, (9.310.1)]. Subsequently, m_1 and m_2 are the fading severity parameters of the specular components. Considering that ζ_1 and ζ_2 are independent with different fluctuations, we define the physically-motivated parameters K and Δ as $K = \frac{V_1^2+V_2^2}{2\sigma^2}$, $\Delta = \frac{2V_1V_2}{V_1^2+V_2^2}$, where K denotes the power ratio of the specular to the diffuse components and $\Delta \in [0,1]$ provides a measure of the similarity of the specular components. Additionally, ancillary parameters K_1 and K_2 defining the power ratios of each specular component to the diffuse one are respectively given by [13] $K_1 \triangleq \frac{V_1^2}{2\sigma^2} = \frac{K\left(1+\sqrt{1-\Delta^2}\right)}{2}$, $K_2 \triangleq \frac{V_2^2}{2\sigma^2} = \frac{K\left(1-\sqrt{1-\Delta^2}\right)}{2}$. When $\Delta = 0$ and $K = 0$, IFTR models reduce to the Rayleigh distribution. We define the average power envelope of the IFTR random variable (RV) as $\mathbb{E}[|V|^2] \triangleq \nu = V_1^2+V_2^2+2\sigma^2 = 2\sigma^2(1+K)$, and the total power of scattered waves as $2\sigma^2 = \nu/(1+K)$.

Theorem 3. *Let* $Z \sim \mathcal{IFTR}\left(m_1, m_2, K_1, K_2, \Delta, \sigma\right)$ *be the squared IFTR RV. The PDF of* Z *is given by*

$$f_Z\left(Z\right) = \sum_{j=0}^{\infty} \Lambda_j f_G\left(Z; j+1, 2\sigma^2\right), \qquad (3)$$

where $f_G\left(Z;j+1,2\sigma^2\right) \triangleq \frac{Z^j e^{-\frac{Z}{2\sigma^2}}}{\Gamma(j+1)(2\sigma^2)^{j+1}}$*. Also, we have, and* Λ_j *is given as in (4), where* m_1*,* m_2 *can take arbitrary real values,* $(x)_n = \Gamma(x+n)/\Gamma(x)$ *is the Pochhammer symbol,* $(\cdot)!$ *is the factorial, and* ${}_2F_1(\cdot)$ *is the Gauss hypergeometric function [12, (9.14.2)].*

Proof. We derive (3) by following [14]. Notably, another closed-form expression of (4) was derived in [13, (11)] in terms of the regularized Gauss hypergeometric function. However, this function is indeterminate when its third parameter is a non-positive integer. With the help of [12, (9.101.1)] and following [14], we arrive at (4), which is valid for both positive and non-positive integer values of the third parameter in the Gauss hypergeometric function. This completes the proof. □

Lemma 4. *Let* $X \triangleq \prod_{\ell=1}^{N} \sqrt{Z_\ell}$ *with the* ς*-th moment of* X *given by* $\mathbb{E}[X^\varsigma] = \mu_X(\varsigma) = \prod_{\ell=1}^{N} \sum_{j_\ell=0}^{\infty} \Lambda_{j_\ell} \left(2\sigma_\ell^2\right)^{\frac{\varsigma}{2}} \frac{\Gamma\left(1+j_\ell+\frac{\varsigma}{2}\right)}{\Gamma(j_\ell+1)}$.

Proof. The ς-th statistical moment of X can be calculated as $\mathbb{E}[X^\varsigma] = \prod_{\ell=1}^{N} \mathbb{E}\left[\left(Z_\ell\right)^{\frac{\varsigma}{2}}\right] = \prod_{\ell=1}^{N} \int_0^\infty Z_\ell^{\frac{\varsigma}{2}} f_{Z_\ell}(Z_\ell) \mathrm{d}Z_\ell$. With the help of (3), [12, (3.381.9)] and [12, (8.356.3)], we finally arrive at the result in Lemma 4. This completes the proof. □

III. Proposed Statistical Approximation

Theorem 4. *Let* $Y_{B,l} \triangleq |h_l|\,|g_{B,l}| e^{i\bar{\theta}_{B,l}}$ *and* $Z_B \triangleq \left|\sum_{l=1}^{L} Y_{B,l}\right|^2$*, with* $l = 1, \cdots, L$*. For all values of* l*,* h_l *and* $g_{B,l}$ *are i.i.d. RVs. Meanwhile, for each* l*-th RIS element,* h_l *and* $g_{B,l}$ *are i.n.i.d. RVs . Thus,* $Y_{B,l}$ *are i.i.d RVs for all values of* l*. The true PDF of* Z_B *can be approximated by that of a generalized Gamma distribution, i.e.,* $Z_B \sim \mathcal{G}(\alpha_{Z_B}, \beta_{Z_B})$*, given by*

$$f_{Z_B}(z;\alpha_{Z_B},\beta_{Z_B}) = \frac{1}{2\sqrt{z}} \frac{\beta_{Z_B}^{\alpha_{Z_B}}}{\Gamma\left(\alpha_{Z_B}\right)} \left(\sqrt{z}\right)^{\alpha_{Z_B}-1} e^{-\beta_{Z_B}\sqrt{z}}, \qquad (5)$$

where $\alpha_{Z_B} = L\alpha_{Y_{B,l}}$ *and* $\beta_{Z_B} = \beta_{Y_{B,l}}$*, with* $\alpha_{Y_{B,l}}$ *and* $\beta_{Y_{B,l}}$ *expressed as* $\alpha_{Y_{B,l}} = \frac{(\mathbb{E}[Y_{B,l}])^2}{\mathbb{V}[Y_{B,l}]} = \frac{\left(\mu_{Y_{B,l}}(1)\right)^2}{\mu_{Y_{B,l}}(2) - \left(\mu_{Y_{B,l}}(1)\right)^2}$*,* $\beta_{Y_{B,l}} = \frac{\mathbb{E}[Y_{B,l}]}{\mathbb{V}[Y_{B,l}]} = \frac{\mu_{Y_{B,l}}(1)}{\mu_{Y_{B,l}}(2) - \left(\mu_{Y_{B,l}}(1)\right)^2}$*, with* $\mathbb{V}[\cdot]$ *the statistical variance. In addition,* $\mu_{Y_{B,l}}(1)$ *and* $\mu_{Y_{B,l}}(2)$ *are respectively the first and second moments of* $Y_{B,l}$*.*

$$\Lambda_j=\frac{m_1^{m_1}m_2^{m_2}}{\Gamma(m_1)\Gamma(m_2)}\sum_{k=0}^{j}\binom{j}{k}\sum_{q=0}^{j-k}\binom{j-k}{q}\frac{K_1^q K_2^{j-k-q}}{j!}\sum_{\imath=0}^{k}\binom{k}{\imath}\frac{\Gamma\left(m_1+q+\imath\right)}{\left(K_1+m_1\right)^{m_1+q+\imath}}\frac{\Gamma\left(m_2+j-k-q+\imath\right)}{\left(K_2+m_2\right)^{m_2+j-k-q+\imath}}$$
$$\times\left(\frac{K\Delta}{2}\right)^{2\imath}(-1)^k\begin{cases}\dfrac{(m_1+q+\imath)_{k-2\imath}(m_2+j-k-q+\imath)_{k-2\imath}\left(\frac{K^2\Delta^2}{4(K_1+m_1)(K_2+m_2)}\right)^{k-2\imath}}{\frac{{}_2F_1\left(m_1+q-\imath+k,m_2+j-q-\imath;1+k-2\imath;\frac{K^2\Delta^2}{4(K_1+m_1)(K_2+m_2)}\right)}{(k-2\imath)!}}, & k>2\imath,\\ \dfrac{{}_2F_1\left(m_1+q+\imath,m_2+j-k-q+\imath;1-k+2\imath;\frac{K^2\Delta^2}{4(K_1+m_1)(K_2+m_2)}\right)}{\Gamma(1-k+2\imath)}, & k\le 2\imath.\end{cases} \tag{4}$$

Proof. See Appendix C. □

Corollary 1. *For a large L, the average received SNR at Bob can be written as $\mathbb{E}[\gamma_{\mathrm{B}}]=\bar{\gamma}_B ML^2\alpha^2_{Y_{B,l}}\beta^{-2}_{Y_{B,l}}$.*

Proof. From Theorem 4, it is deduced that $\mathbb{E}[Z_{\mathrm{B}}]=L\alpha_{Y_{\mathrm{B},l}}\left(L\alpha_{Y_{\mathrm{B},l}}+1\right)\beta^{-2}_{Y_{\mathrm{B},l}}$. For a large L, $L\alpha_{Y_{\mathrm{B},l}}\gg 1$, hence $\mathbb{E}[Z_{\mathrm{B}}]=L^2\alpha^2_{Y_{\mathrm{B},l}}\beta^{-2}_{Y_{\mathrm{B},l}}$. With the help of Theorem 1, the final expression of $\mathbb{E}[\gamma_{\mathrm{B}}]$ can be given as in Corollary 1. This completes the proof. □

Remark 2. *Corollary 1 shows that $\mathbb{E}[\gamma_B]$ is directly proportional to M and L^2, indicating that increasing both the number of antennas M at Alice and the number of RIS elements L could enhance the average received SNR at Bob. However, the impact of L is more pronounced, as the optimal beamforming design in Theorem 1 results in a performance gain of ML in the Alice-RIS links and an additional gain of L in the RIS-Bob links. Furthermore, using Remark 1, the ratio $\frac{\mathbb{E}[\gamma_B]}{\mathbb{E}[\gamma_{E_{MRC}}]}$ scales with L, suggesting that increasing L yields a larger performance gain than increasing M.*

IV. Effective Secrecy Throughput Analyses

We assume that Alice knows Bob's instantaneous CSI [2], ensuring that the reliability constraint $R_{\mathrm{c}}\le C_{\mathrm{B}}$ is always met by adaptively setting the codeword rate to the instantaneous channel capacity, i.e., $R_{\mathrm{c}}=C_{\mathrm{B}}$. The violation of the secrecy constraint is then defined as the probability that R_{r} is less than C_{E}. According to [4, (3)], the EST of the adaptive-rate scheme under the MRC colluding attack is given by

$$\Psi=R_{\mathrm{s}}\left(1-P_{\mathrm{out}}^{\mathrm{Eve}}\right)=R_{\mathrm{s}}(1-\Pr(R_{\mathrm{r}}\le\log_2(1+\gamma_{\mathrm{E_{MRC}}}))), \tag{6}$$

where $P_{\mathrm{out}}^{\mathrm{Eve}}=\Pr(R_{\mathrm{r}}\le C_{\mathrm{E}})$ is the secrecy outage due to the eavesdropping channel, and $\gamma_{\mathrm{E_{MRC}}}$ is the instantaneous SNR at the super Eve, defined in Lemma 3. With the help of Lemma 3, a closed-form expression of (6) is derived as $\Psi=\frac{R_{\mathrm{s}}}{\Gamma(E)}\gamma\left(E,\frac{\left(2^{C_{\mathrm{B}}-R_{\mathrm{s}}}-1\right)}{2ML\bar{\gamma}_{\mathrm{E_s}}}\right)$. In the adaptive-rate scheme, R_{s} is adaptively adjusted within $0<R_{\mathrm{s}}<C_{\mathrm{B}}$. As a result, $C_{\mathrm{B}}=\log_2(1+\bar{\gamma}_{\mathrm{B}}MZ_{\mathrm{B}})>R_{\mathrm{s}}$, i.e., $Z_{\mathrm{B}}>\left(2^{R_{\mathrm{s}}}-1\right)/\left(\bar{\gamma}_{\mathrm{B}}M\right)$, has to be satisfied, which is achievable owing to the availability of the instantaneous CSI Z_{B}. Thus, C_{B}, averaging over all acceptable realizations of Z_{B}, is calculated as $C_{\mathrm{B}}=\int_{(2^{R_{\mathrm{s}}}-1)/(\bar{\gamma}_{\mathrm{B}}M)}^{\infty}\log_2(1+\bar{\gamma}_{\mathrm{B}}MZ_{\mathrm{B}})f_{Z_{\mathrm{B}}}(Z_{\mathrm{B}})\,\mathrm{d}Z_{\mathrm{B}}$, where $f_{Z_{\mathrm{B}}}(\cdot)$ is given in (5). To ensure that Eve does not operate at a very low outage probability to compromise secrecy, the EST is imposed by a $P_{\mathrm{out}}^{\mathrm{Eve}}$-constraint expressed as $\Psi=\begin{cases}\Psi, & \text{if } P_{\mathrm{out}}^{\mathrm{Eve}}\le P_{\mathrm{out}}^{\mathrm{Eve,th}},\\ 0, & \text{if } P_{\mathrm{out}}^{\mathrm{Eve}}>P_{\mathrm{out}}^{\mathrm{Eve,th}},\end{cases}$ where $P_{\mathrm{out}}^{\mathrm{Eve,th}}$ is the maximum allowed value of $P_{\mathrm{out}}^{\mathrm{Eve}}$ [4]. Note that $P_{\mathrm{out}}^{\mathrm{Eve,th}}=1$ corresponds to Ψ with no constraints.

Lemma 5. *The optimal value R_s^* that maximizes Ψ, denoted as Ψ_{max}, with eavesdropper outage constraints for the RIS-aided mmWave system is given by $R_s^*=\min\left(R_{s,1}^*,R_{s,2}^*\right)$, where $R_{s,1}^*$ is the unconstrained optimal value of R_s given by the solution of the following fixed-point equation $R_{s,1}^*=\frac{\gamma\left(E,\frac{\left(2^{C_B-R_{s,l-1}^*}\right)}{2ML\bar{\gamma}_{E_s}}\right)(2ML\bar{\gamma}_{E_s})^E e^{\frac{2^{C_B-R_{s,l-1}^*}}{2ML\bar{\gamma}_{E_s}}}}{2^{C_B-R_{s,l}^*}\left(2^{C_B-R_{s,l}^*}-1\right)^{E-1}\log(2)}$, and $R_{s,2}^*$ is the constrained optimal value of R_s, given by $R_{s,2}^*=\log_2\left(\frac{2^{C_B}}{1+\left[2ML\bar{\gamma}_{E_s}\Gamma^{-1}\left(E,P_{out}^{Eve,th}\Gamma(E)\right)\right]^2}\right)$, where $\Gamma^{-1}(\cdot,\cdot)$ denotes the inverse of the upper incomplete Gamma function $\Gamma(\cdot,\cdot)$ defined in [12, (8.350.2)].*

Proof. See Appendix D. □

Corollary 2. *When $\bar{\gamma}_{E_s}\to 0$ and $\bar{\gamma}_{E_s}\to\infty$, we have the asymptotic results $\Psi\to R_s$ and $\Psi\to 0$, respectively.*

Proof. With the help of [12, (8.352.6)] and setting $E=1$, we can write $\Psi=R_{\mathrm{s}}\left(1-e^{-\left(\frac{2^{C_{\mathrm{B}}-R_{\mathrm{s}}}-1}{2ML\bar{\gamma}_{\mathrm{E_s}}}\right)}\right)$. Then, it is deduced that Ψ converges to R_{s} when $\bar{\gamma}_{\mathrm{E_s}}\to 0$. This completes the proof. □

V. Numerical Results and Discussions

In this section, we present the EST results for the adaptive-rate scheme in bit per channel use (bpcu). The truncation value for the infinite summation in (3) is set at 40, validated by Monte-Carlo simulations. System and channel parameters are listed in the caption of Fig. 1.

In Fig. 1a, we demonstrate the effectiveness of various RIS sizes in enhancing the secrecy throughput. Increasing the RIS size by raising L significantly improves $\Psi_{\max}$, as Bob's SNR gain is L times greater than Eve's, as noted in Remark 2. Assuming the largest RIS size with

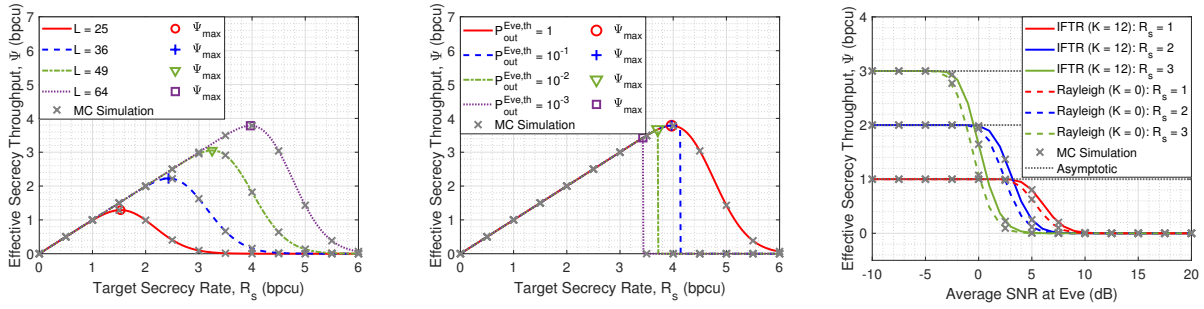

Fig. 1. (a) varying L, $P_{\text{out}}^{\text{Eve,th}} = 1$; (b) varying $P_{\text{out}}^{\text{Eve,th}}$, $L = 64$. Common parameters in (a) and (b): $\bar{\gamma}_B = 10$ dB, $\bar{\gamma}_{E_s} = -5$ dB, $M = 36$, $E = 9$; (c) Exact and asymptotic Ψ with varying R_s over IFTR and Rayleigh channels, $L = 64$, $M = 36$, $E = 9$, $P_{\text{out}}^{\text{Eve,th}} = 1$, $\bar{\gamma}_B = 10$ dB. IFTR fading parameters: $h_l \sim \mathcal{IFTR}\left(m_{1,h}, m_{2,h}, K_{1,h}, K_{2,h}, \Delta_h, \sigma_h\right)$ with $m_{1,h} = 2$, $m_{2,h} = 7.5$, $K_{1,h} = 5$, $K_{2,h} = 7$. $g_{\text{B},l} \sim \mathcal{IFTR}\left(m_{1,g}, m_{2,g}, K_{1,g}, K_{2,g}, \Delta_g, \sigma_g\right)$ with $m_{1,g} = 7.5$, $m_{2,g} = 2$, $K_{1,g} = 5$, $K_{2,g} = 7$. Phase estimation-error: $\kappa_{\text{PE}} = 45$ dB.

$L = 64$ and $E = 9$ eavesdroppers, we further examine the EST performance under eavesdropper outage constraints defined in Lemma 5, across different $P_{\text{out}}^{\text{Eve,th}}$ levels, as shown in Fig. 1b. It is observed that Alice can maintain $\Psi_{\max} \approx 3.78$ bpcu corresponding to $R_{\text{s},1}^*$ at $P_{\text{out}}^{\text{Eve,th}} = 1$ and $R_{\text{s},2}^*$ at $P_{\text{out}}^{\text{Eve,th}} = 10^{-1}$. However, to meet the secrecy constraint with $P_{\text{out}}^{\text{Eve}} < 10^{-1}$, Alice must reduce R_{s}^* to a lower rate, resulting in the decreased achievable $\Psi_{\max}$. For instance, the $\Psi_{\max}$ is reduced to 3.67 bpcu and 3.43 bpcu when $P_{\text{out}}^{\text{Eve,th}} = 10^{-2}$ and 10^{-3}, respectively. In practice, Alice can pre-define the $P_{\text{out}}^{\text{Eve,th}}$ constraint based on the average CSI estimated for Eve and the desired achievable $\Psi_{\max}$.

In Fig. 1c, the analytical results of Ψ are plotted against $\bar{\gamma}_{\text{E}_\text{s}}$ for different values of R_{s} over IFTR (i.e., mmWave) and Rayleigh (i.e., microwave) channels. The asymptotic results confirm that $\Psi \to R_{\text{s}}$ and $\Psi \to 0$ when $\bar{\gamma}_{\text{E}_\text{s}} \to 0$ and $\bar{\gamma}_{\text{E}_\text{s}} \to \infty$, respectively, as stated in Corollary 2. Additionally, the EST performance is identical over both mmWave and Rayleigh channels when $\bar{\gamma}_{\text{E}_\text{s}} \to 0$ and $\bar{\gamma}_{\text{E}_\text{s}} \to \infty$. Within a practical range of $\bar{\gamma}_{\text{E}_\text{s}}$ (e.g., $-5 \sim 10$ dB), mmWave channels achieve a higher EST performance than Rayleigh channels for the same $\bar{\gamma}_{\text{E}_\text{s}}$. This performance gain increases with higher values of R_{s}. The maximum performance gain in mmWave channels is about 0.57 bpcu at $\bar{\gamma}_{\text{E}_\text{s}} = 0$ dB with $R_{\text{s}} = 3$ bpcu, and about 0.19 bpcu at $\bar{\gamma}_{\text{E}_\text{s}} = 6$ dB with $R_{\text{s}} = 1$ bpcu. This security gain is due to the strong LoS components in mmWave links, represented by the physical parameter $K = 12$ dB in the IFTR model, compared to $K = 0$ dB in the Rayleigh model.

VI. Conclusions

In this paper, we presented the first investigation of information-theoretic PLS performance in terms of the EST for RIS-aided mmWave systems using the IFTR fading model and considering multiple colluding Eves under the MRC scheme. We provided a tractable expression of the IFTR model and approximated the true statistical PDF of the end-to-end SNR at Bob by a generalized Gamma distribution. For the end-to-end SNR at the super Eve under the MRC scheme, we employed a Gamma distribution. Using these approximations, we determined the maximum EST satisfying both reliability and secrecy constraints in the adaptive-rate scheme.

Appendix A
Proof of Theorem 1

Following the framework in [6] and applying the MRT beamformer $\mathbf{f} = \left(\mathbf{g}_{\text{B}}^{\text{H}}\mathbf{\Phi}\mathbf{H}\right)^{H} / \left\|\mathbf{g}_{\text{B}}^{\text{H}}\mathbf{\Phi}\mathbf{H}\right\|$, the optimal RIS phase shifts can be calculated by maximizing the received SNR at Bob as $\mathbf{\Phi}^{\text{opt}} = \underset{\Phi}{\text{argmax}} \left|\mathbf{g}_{\text{B}}^{\text{H}}\mathbf{\Phi}\mathbf{H}\mathbf{f}\right|^2 = \underset{\Phi}{\text{argmax}} \left\|\mathbf{g}_{\text{B}}^{\text{H}}\mathbf{\Phi}\mathbf{H}\right\|^2 = \underset{\Phi}{\text{argmax}} \left|\mathbf{g}_{\text{B}}^{\text{H}}\mathbf{\Phi}\mathbf{h}\mathbf{a}_L\left(\theta_{\text{RIS}}^{\text{AoA,a}}, \theta_{\text{RIS}}^{\text{AoA,e}}\right)\right|^2 \left\|\mathbf{a}_M^{\text{H}}\left(\theta_{\text{BS}}^{\text{AoD,a}}, \theta_{\text{BS}}^{\text{AoD,e}}\right)\right\|^2$.

Using the identity $\left\|\mathbf{a}_M^{\text{H}}\left(\theta_{\text{BS}}^{\text{AoD,a}}, \theta_{\text{BS}}^{\text{AoD,e}}\right)\right\|^2 = M$ directly deduced from (1), after some mathematical manipulations, we have $\mathbf{\Phi}^{\text{opt}} = \underset{\Phi}{\text{argmax}} \left|\sum_l^L h_l^* g_{\text{B},l}^* a_l\left(\theta_{\text{RIS}}^{\text{AoA,a}}, \theta_{\text{RIS}}^{\text{AoA,e}}\right) e^{i\phi_l}\right|^2$, where $a_l\left(\theta_{\text{RIS}}^{\text{AoA,a}}, \theta_{\text{RIS}}^{\text{AoA,e}}\right)$ denotes the l-th element in the array response vector $\mathbf{a}_L\left(\theta_{\text{RIS}}^{\text{AoA,a}}, \theta_{\text{RIS}}^{\text{AoA,e}}\right)$. Thus, the optimal RIS phase shifts are derived as $\phi_l^{\text{opt}} = -\angle\left(h_l^* g_{\text{B},l}^* a_l\left(\theta_{\text{RIS}}^{\text{AoA,a}}, \theta_{\text{RIS}}^{\text{AoA,e}}\right)\right)$, where $\angle$ gives the phase of the complex value. The corresponding optimal reflection matrix can be obtained as $\mathbf{\Phi}^{\text{opt}} = \text{diag}\left(e^{-i\angle\left(\text{diag}\left(\mathbf{g}_{\text{B}}^{\text{H}}\right)\mathbf{h}\mathbf{a}_L\left(\theta_{\text{RIS}}^{\text{AoA,a}}, \theta_{\text{RIS}}^{\text{AoA,e}}\right)\right)}\right)$. Using the optimal reflection matrix, the ideal received instantaneous SNR at Bob is given as $\gamma_{\text{B}} = \bar{\gamma}_{\text{B}} M \left|\sum_{l=1}^L |h_l| |g_{\text{B},l}|\right|^2$. However, considering that the phase shifts induced by the channels are not perfectly estimated by Bob, we model the deviation from the ideal setting by the phase estimation error $\tilde{\theta}_{\text{B},l}$ [10]. This completes the proof.

Appendix B
Proof of Theorem 2

The received instantaneous SNR at the e-th Eve can be expressed as $\gamma_{\text{E}_e} = \bar{\gamma}_{\text{E}_e} \left|\mathbf{g}_{\text{E}_e}^{\text{H}}\mathbf{\Phi}\mathbf{H}\mathbf{f}\right|^2 =$

$\bar{\gamma}_{\mathrm{E}_e}\left|\mathbf{g}_{\mathrm{E}_e}^{\mathrm{H}}\mathbf{\Phi}\mathbf{H}\frac{\mathbf{g}_{\mathrm{B}}\mathbf{\Phi}^H\mathbf{H}^H}{\left\|\mathbf{g}_{\mathrm{B}}^{\mathrm{H}}\mathbf{\Phi}\mathbf{H}\right\|}\right|^2$. Using the identity $\left\|\mathbf{a}_M^{\mathrm{H}}(\theta_{\mathrm{BS}}^{\mathrm{AoD,a}},\theta_{\mathrm{BS}}^{\mathrm{AoD,e}})\right\|^2 = M$ deduced from (1), we then have $\gamma_{\mathrm{E}_e} = \bar{\gamma}_{\mathrm{E}_e}M\left|\mathbf{g}_{\mathrm{E}_e}^{\mathrm{H}}\mathbf{\Phi}\mathbf{h}\mathbf{a}_L(\theta_{\mathrm{RIS}}^{\mathrm{AoA,a}},\theta_{\mathrm{RIS}}^{\mathrm{AoA,e}})\right|^2 = \bar{\gamma}_{\mathrm{E}_e}M\left|\sum_{l=1}^{L} g_{\mathrm{E}_e,l}^* h_l^* a_l(\theta_{\mathrm{RIS}}^{\mathrm{AoA,a}},\theta_{\mathrm{RIS}}^{\mathrm{AoA,e}})e^{i\phi_l}\right|^2$. Using the identity $\left|a_l(\theta_{\mathrm{RIS}}^{\mathrm{AoA,a}},\theta_{\mathrm{RIS}}^{\mathrm{AoA,e}})\right| = 1$ deduced from (1), and the optimal RIS phase shifts $\phi_l^{\mathrm{opt}} = -\angle\left(h_l^* g_{\mathrm{B},l}^* a_l(\theta_{\mathrm{RIS}}^{\mathrm{AoA,a}},\theta_{\mathrm{RIS}}^{\mathrm{AoA,e}})\right)$, we arrive at $\gamma_{\mathrm{E}_e} = \bar{\gamma}_{\mathrm{E}_e}M\left|\sum_{l=1}^{L} g_{\mathrm{E}_e,l}^* h_l^* e^{-i\angle(h_l^* g_{\mathrm{B},l}^*)}\right|^2$. Since $\mathbf{\Phi}$ is optimized by maximizing the received SNR at Bob, it is impossible for Eve to perfectly estimate the phase shifts and compensate for the channel phases. As a result, we consider that Eve suffers from severe phase estimation errors, denoted as $\tilde{\theta}_{\mathrm{E},l}$. This completes the proof.

Appendix C
Proof of Theorem 4

Let us define $Y_{\mathrm{B},l}\triangleq|h_l|\,|g_{\mathrm{B},l}|e^{i\tilde{\theta}_{\mathrm{B},l}}$ and $X_{B,l}=|h_l|\,|g_{\mathrm{B},l}|$. Since $X_{B,l}$ and $e^{i\tilde{\theta}_{\mathrm{B},l}}$ are statistically independent, we infer that $\mathbb{E}[Y_{B,l}^{\varsigma}]=\mathbb{E}[X_{B,l}^{\varsigma}]\mathbb{E}\left[e^{i\varsigma\tilde{\theta}_{\mathrm{B},l}}\right]$, where $\mathbb{E}[X_{B,l}^{\varsigma}]$ can be directly derived from Lemma 4 as $\mathbb{E}\left[X_{B,l}^{\varsigma}\right] = \mu_{X_{B,l}}(\varsigma) = \sum_{j_1=0}^{\infty}\sum_{j_2=0}^{\infty}\Lambda_{l,j_1}\Lambda_{B,l,j_2}\left(2\sigma_1^2\right)^{\frac{\varsigma}{2}}\left(2\sigma_2^2\right)^{\frac{\varsigma}{2}}\frac{\Gamma\left(1+j_1+\frac{\varsigma}{2}\right)\Gamma\left(1+j_2+\frac{\varsigma}{2}\right)}{\Gamma(j_1+1)\Gamma(j_2+1)}$. On the other hand, the ς-th statistical moment of $e^{i\tilde{\theta}_{\mathrm{B},l}}$ can be deduced from the characteristic function of the von Mises distribution [10], written as $\mathbb{E}\left[e^{i\varsigma\tilde{\theta}_{\mathrm{B},l}}\right] = \frac{I_{\varsigma}(\kappa_{\mathrm{PE}})}{I_0(\kappa_{\mathrm{PE}})}$, where κ_{PE} is the loop SNR of the PLL defined in Lemma 2, $I_0(\cdot)$ and $I_{\varsigma}(\cdot)$ are the modified Bessel functions of the first kind with zero-order and ς-order, respectively. Then, the first and second moments of $Y_{B,l}$ can be derived by replacing $\varsigma=1,2$ in $\mathbb{E}\left[X_{B,l}^{\varsigma}\right]$, which are expressed as $\mu_{Y_{B,l}}(1)= 2\sigma_1\sigma_2\sum_{j_1=0}^{\infty}\sum_{j_2=0}^{\infty}\Lambda_{l,j_1}\Lambda_{B,l,j_2}\frac{I_1(\kappa_{\mathrm{PE}})\Gamma\left(j_1+\frac{3}{2}\right)\Gamma\left(j_2+\frac{3}{2}\right)}{I_0(\kappa_{\mathrm{PE}})\Gamma(j_1+1)\Gamma(j_2+1)}$, $\mu_{Y_{B,l}}(2) = 4\sigma_1^2\sigma_2^2\sum_{j_1=0}^{\infty}\sum_{j_2=0}^{\infty}\Lambda_{l,j_1}\Lambda_{B,l,j_2}\frac{I_2(\kappa_{\mathrm{PE}})\Gamma(j_1+2)\Gamma(j_2+2)}{I_0(\kappa_{\mathrm{PE}})\Gamma(j_1+1)\Gamma(j_2+1)}$, where Λ_{l,j_1} and Λ_{B,l,j_2} follow (4) in Theorem 3. Now, we propose to approximate $Y_{B,l}$ by a Gamma RV. Novel closed-form expressions for the approximated parameters $(\alpha_{Y_{B,l}},\beta_{Y_{B,l}})$ can be respectively derived by plugging $\mu_{Y_{B,l}}(1)$ and $\mu_{Y_{B,l}}(2)$ into $\alpha_{Y_{\mathrm{B},l}}$ and $\beta_{Y_{\mathrm{B},l}}$ in Theorem 4. Consequently, the true PDF of Z_B follows a generalized Gamma distribution, i.e., $Z_B \sim \mathcal{G}(\alpha_{Z_B},\beta_{Z_B})$. This completes the proof.

Appendix D
Proof of Lemma 5

The unconstrained optimal value $R_{\mathrm{s},1}^*$ in Lemma 5 can be obtained by applying the first-order derivative $\partial\Psi(R_{\mathrm{s}})/\partial R_{\mathrm{s}} = 0$, and solving to R_{s}. Similar to [3], [4], finding stationary points via the first-order derivative is untractable. Thus, we investigate through detailed simulations. Howver, one can derive the inverse function of $P_{\mathrm{out}}^{\mathrm{Eve}}$ inferred from the closed-form expression of Ψ for $P_{\mathrm{out}}^{\mathrm{Eve,th}}$ to find the constrained optimal value $R_{\mathrm{s},2}^*$. It is noted that Ψ increases for $R_{\mathrm{s}} < R_{\mathrm{s},1}^*$ and decreases for $R_{\mathrm{s}} > R_{\mathrm{s},1}^*$, thus the unconstrained $R_{\mathrm{s},1}^*$ represents the maximum target secrecy rate in the sense that any value other than the optimal value $R_{\mathrm{s}}^* = R_{\mathrm{s},1}^*$ will result in a lower value of Ψ. Nevertheless, with a pre-defined $P_{\mathrm{out}}^{\mathrm{Eve,th}}$ constraint for $P_{\mathrm{out}}^{\mathrm{Eve}}$, R_{s}^* cannot be larger than $R_{\mathrm{s},2}^*$. Therefore, R_{s}^* is the minimum value between $R_{\mathrm{s},1}^*$ and $R_{\mathrm{s},2}^*$. This completes the proof.

Acknowledgements

This work was supported in part by the Japan Society for Promotion of Science (JSPS) KAKENHI (Grants 23H00470, 24K17272, and 24K21615), and in part by the Japan Science and Technology Agency (JST) ASPIRE (Grant JPMJAP2345).

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, 2006, pp. 356–360.

[3] S. Yan *et al.*, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 11, pp. 6377–6388, 2015.

[4] M. E. P. Monteiro *et al.*, "Maximum secrecy throughput of transmit antenna selection with eavesdropper outage constraints," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 2069–2072, 2015.

[5] J. D. Vega Sánchez, P. Ramírez-Espinosa, and F. J. López-Martínez, "Physical layer security of large reflecting surface aided communications with phase errors," *IEEE Wirel. Commun. Lett.*, vol. 10, no. 2, pp. 325–329, 2021.

[6] W. Shi *et al.*, "On secrecy performance of RIS-assisted MISO systems over Rician channels with spatially random eavesdroppers," *IEEE Trans. Wirel. Commun., (Early access)*, pp. 1–15, 2024.

[7] J. M. Romero-Jerez *et al.*, "The fluctuating two-ray fading model: Statistical characterization and performance analysis," *IEEE Trans. Wirel. Commun.*, vol. 16, no. 7, pp. 4420–4432, 2017.

[8] M. Olyaee *et al.*, "The fluctuating two-ray fading model with independent specular components," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 5533–5545, 2023.

[9] S. Zhou *et al.*, "Spectral and energy efficiency of IRS-assisted MISO communication with hardware impairments," *IEEE Wirel. Commun. Lett.*, vol. 9, no. 9, pp. 1366–1369, 2020.

[10] M.-A. Badiu and J. P. Coon, "Communication through a large reflecting surface with phase errors," *IEEE Wirel. Commun. Lett.*, vol. 9, no. 2, pp. 184–188, 2020.

[11] M. Abdulaziz *et al.*, "A 10-mW mm-wave phase-locked loop with improved lock time in 28-nm FD-SOI CMOS," *IEEE Trans. Microw. Theory Tech.*, vol. 67, no. 4, pp. 1588–1600, 2019.

[12] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.

[13] M. Olyaee, H. Hashemi, and J. M. Romero-Jerez, "A tractable statistical representation of IFTR fading with applications," *IEEE Trans. Commun. (Early access)*, pp. 1–15, 2024.

[14] M. López-Benítez and J. Zhang, "Comments and corrections to "New results on the fluctuating two-ray model with arbitrary fading parameters and its applications"," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1938–1940, 2021.