Physical Layer Security of Large Reflecting Surface Aided Communications with Phase Errors

José David Vega Sánchez, Pablo Ramírez-Espinosa and F. Javier López-Martínez

***Abstract*—The physical layer security (PLS) performance of a wireless communication link through a large reflecting surface (LRS) with phase errors is analyzed. Leveraging recent results that express the LRS-based composite channel as an equivalent scalar fading channel, we show that the eavesdropper's link is Rayleigh distributed and independent of the legitimate link. The different scaling laws of the legitimate and eavesdroppers signal-to-noise ratios with the number of reflecting elements, and the reasonably good performance even in the case of coarse phase quantization, show the great potential of LRS-aided communications to enhance PLS in practical wireless set-ups.**

***Index Terms*—Fading channels, large reflecting surfaces, phase errors, physical layer security, wireless communications.**

I. Introduction

Recently, large reflecting surfaces (LRSs) have been proposed as a new paradigm to noticeably improve the performance of emerging networks in terms of system performance and energy-efficiency. An LRS consists of a large number of low-cost passive reflecting units, where each element can adaptively adjust the amplitude reflection and/or the phase shift of the incident signals [1]. These smart passive devices can be integrated into the infrastructure of future wireless networks to control the radio propagation environment. In practice, effects associated to the imperfect phase-shift capabilities need to be considered for a proper system design [2–5].

On the other hand, physical layer security (PLS) has drawn full attention for ensuring secure wireless communications in a low complexity manner. Specifically, PLS intelligently exploits the inherent randomness of the wireless medium to protect the information in the physical layer [6]. From an information-theoretic perspective, LRS is a new approach to improve the PLS performance by reconfiguring the wireless environment for the benefit of the legitimate user. In this sense, several researchers have addressed their efforts to investigate PLS on LRS-aided wireless communications systems [7–10]. Because of the rather complex nature of the LRS composite fading model, the analytical characterization of PLS performance metrics is utterly unfeasible and most works often resort to optimization techniques to maximize the secrecy rates.

In this paper, we investigate the performance of an LRS-aided communication system with imperfect phase compensation in terms of its PLS performance. Because of the intricate characterization of PLS in the context of LRS, we leverage the recent formulation of the LRS composite fading channel as an equivalent scalar channel [11] to gain an understanding of the potential of LRS-based communications for PLS. The key contributions of this paper are: first, we prove that despite the equivalent channels at both receivers share a number of components, they are statistically independent under some mild conditions. We also show that the distribution of the eavesdropper's equivalent scalar fading channel is Rayleigh distributed and its average signal-to-noise ratio (SNR) scales with n, while the average SNR at the legitimate receiver scales with n^2. Finally, we exemplify the limitations of the equivalent scalar channel approximations for asymptotic high-SNR analyses, which should be interpreted with caution for outage-based performance metrics. *Notations:* Throughout this letter, $f_Z(\cdot)$ and $F_Z(\cdot)$ denote the PDF and the CDF of a random variable (RV) Z, respectively. $\mathrm{W} \sim \mathcal{U}[-\pi, \pi)$ means that the RV W is uniformly distributed on $[-\pi, \pi)$. $\mathbb{E}\{\}$ is the expectation operator.

II. System Model

We consider an LRS-assisted wireless communication set-up consisting of one source node Alice (A), one legitimate node Bob (B), one eavesdropper Eve (E), and an LRS, which assists the communication between the legitimate nodes. In the system, the direct link is neglected[1], and all terminals are assumed to be equipped with a single antenna, while the LRS has n low-cost passive reflecting elements $R_1 \dots R_n$. We denote as $H_{i,1}$ the fading channel coefficient between the source A and the reflecting element R_i, whereas $H_{i,\mathrm{b}}$ and $H_{i,\mathrm{e}}$ are the fading channel coefficients between R_i and the legitimate receiver B and the eavesdropper E, respectively. Without loss of generality, we consider normalized fading coefficients with unitary power, and the corresponding average magnitudes are given $\forall i = 1 \dots n$ by $a_1 = \mathbb{E}\{|H_{i,1}|\}$, $a_{2,\mathrm{b}} = \mathbb{E}\{|H_{i,\mathrm{b}}|\}$ and $a_{2,\mathrm{e}} = \mathbb{E}\{|H_{i,\mathrm{e}}|\}$. We note that $\{a_1, a_{2,\mathrm{b}}, a_{2,\mathrm{e}}\} \leq 1$ in all instances, where the equality only holds in the limit of a deterministic fading channel, i.e., in the absence of fading. For the sake of compactness, $a_{\mathrm{b}} = \sqrt{a_1 a_{2,\mathrm{b}}}$ is defined. The received signal at B can be expressed as

$$Y_{\mathrm{b}} = \sqrt{P_T L_{\mathrm{b}}} \sum_{i=1}^{n} H_{i,1} e^{j\phi_i} H_{i,\mathrm{b}} X + W_b, \tag{1}$$

[1]This assumption is related to one of the key use cases of LRS, which is overcoming non-LOS scenarios [12].

Manuscript received July 24, 2020; revised XXX. The review of this paper was coordinated by Dr. Cunhua Pan. The work of J. D. Vega Sánchez was funded by the Escuela Politécnica Nacional, for the development of the project PIGR-19-06 and through a teaching assistant fellowship for doctoral studies. The work of F.J. Lopez-Martinez was funded by the Spanish Government and the European Fund for Regional Development FEDER (project TEC2017-87913-R) and by Junta de Andalucia (project P18-RT-3175, TETRA5G).

J. D. Vega Sánchez is with Departamento de Electrónica, Telecomunicaciones y Redes de Información, Escuela Politécnica Nacional (EPN), Quito, 170525, Ecuador. (e-mail: jose.vega01@epn.edu.ec).

P. Ramírez-Espinosa is with the Connectivity Section, Department of Electronic Systems, Aalborg University, Aalborg Øst 9220, Denmark (e-mail: pres@es.aau.dk).

F. J. Lopez-Martinez is with Departamento de Ingenieria de Comunicaciones, Universidad de Malaga - Campus de Excelencia Internacional Andalucia Tech., Malaga 29071, Spain (e-mail: fjlopezm@ic.uma.es).

where X is the transmitted symbol, P_T indicates the transmit power at A, L_b encompasses the path losses for the A-R and R-B links, the antenna gains and reflection losses, and W_b is the additive white Gaussian noise (AWGN) term with N_0 power. Now, the LRS designs the phase shifts for each element ϕ_i so that all phase contributions due to $\angle H_{i,1}$ and $\angle H_{i,\mathrm{b}}$ are compensated[2] However, the imperfect phase estimation and the limited quantization of phase states at the LRS causes that a residual random phase error Θ_i still persists [11], i.e., $\phi_i = -\angle H_{i,1} - \angle H_{i,\mathrm{b}} + \Theta_i$. The equivalent complex channel observed by the legitimate receiver can hence be expressed as

$$H_\mathrm{b} = \frac{1}{n}\sum_{i=1}^{n} |H_{i,1}\|H_{i,\mathrm{b}}|\, e^{j\Theta_i}, \tag{2}$$

and (1) is reformulated as:

$$Y_\mathrm{b} = n\sqrt{P_T L_\mathrm{b}} H_b X + W_b \tag{3}$$

Now, the received signal at E can be expressed as

$$Y_\mathrm{e} = \sqrt{P_T L_\mathrm{e}} \sum_{i=1}^{n} H_{i,1} e^{j\phi_i} H_{i,\mathrm{e}} X + W_e, \tag{4}$$

where the L_e and W_e are defined in a similar way as L_b and W_b. Because the phase shifts ϕ_i are designed to compensate for the effect of the fading channel coefficients of the legitimate link, the residual phase errors Ψ_i affecting the eavesdropper link will be much larger than the legitimate counterpart and, whenever $\angle H_{i,\mathrm{e}} \sim \mathcal{U}[-\pi, \pi)$, then $\Psi_i \sim \mathcal{U}[-\pi, \pi)$ [14] regardless of the phase distribution of $\angle H_{i,1}$. We can define the equivalent complex channel observed by E as

$$H_\mathrm{e} = \frac{1}{n}\sum_{i=1}^{n} |H_{i,1}\|H_{i,\mathrm{e}}|\, e^{j\Psi_i}, \tag{5}$$

that yields

$$Y_\mathrm{e} = n\sqrt{P_T L_\mathrm{e}} H_e X + W_e \tag{6}$$

With the previous definitions, the instantaneous SNR at the legitimate and eavesdropper's links are given by

$$\gamma_\mathrm{b} = n^2 \overline{\gamma}_{0,\mathrm{b}} |H_\mathrm{b}|^2, \tag{7}$$

$$\gamma_\mathrm{e} = n^2 \overline{\gamma}_{0,e} |H_\mathrm{e}|^2, \tag{8}$$

where we defined $\overline{\gamma}_{0,\mathrm{b}} = P_T L_\mathrm{b}/N_0$ and $\overline{\gamma}_{0,e} = P_T L_\mathrm{e}/N_0$ as the average SNRs at the legitimate and eavesdropper's sides in the case of a single reflector LRS (i.e., $n = 1$).

We aim to determine the system performance in terms of its achievable secrecy rate C_S defined as [15]

$$C_\mathrm{S} = \max\left\{C_\mathrm{b} - C_\mathrm{e}, 0\right\}, \tag{9}$$

where $C_\mathrm{b} = \log_2(1+\gamma_\mathrm{b})$ and $C_\mathrm{e} = \log_2(1+\gamma_\mathrm{e})$ are the capacities of the main and eavesdropper channels, respectively. We first consider a passive eavesdropper for which Alice does not have channel state information (CSI) knowledge. Under this premise, Alice can only transmit at a constant secrecy rate R_S and security will be compromised whenever R_S exceeds C_S. The secrecy outage probability (SOP) is formulated as the probability that the instantaneous C_S falls below such rate R_S, i.e., $\mathrm{P} = \Pr\left\{C_\mathrm{S} < R_\mathrm{S}\right\} = \int_0^\infty F_{\gamma_\mathrm{b}}\left(\tau\gamma_\mathrm{e} + \tau - 1\right) f_{\gamma_\mathrm{e}}(\gamma_\mathrm{e}) d\gamma_\mathrm{e}$, where $\tau \triangleq 2^{R_\mathrm{S}}$. We also study the active eavesdropping case, in which the CSI of both the main and the eavesdropper channels is available at Alice. Therefore, Alice can use such information to adapt her rate. In this setup, the average secrecy rate (ASR) $\mathcal{R}_\mathrm{S} = \mathbb{E}\{C_\mathrm{S}\}$ is the usual metric to evaluate the secrecy performance. To derive the ASR's analytical expressions in this letter, we have used the formulations proposed in [16, Proposition 3].

[2]Neglecting the eavesdropper's phase information for the phase-shift design maximizes the SNR at the legitimate receiver, although it is suboptimal for PLS performance [13]. However, this choice avoids the inherent optimization problem related to phase-shift design while achieving nearly as good performance when the eavesdropper's channel becomes more degraded than the legitimate one.

III. SNR DISTRIBUTIONS

A. Distribution of γ_b

For sufficiently large n, [11] proved that the distribution of H_b is that of a non-circularly symmetric complex Gaussian random variable (RV) with $U_\mathrm{b} = \Re(H_\mathrm{b})$ and $V_\mathrm{b} = \Im(H_\mathrm{b})$, so that $U_\mathrm{b} \sim \mathcal{N}\left(\mu, \sigma^2_{U_\mathrm{b}}\right)$ and $V_\mathrm{b} \sim \mathcal{N}\left(0, \sigma^2_{V_\mathrm{b}}\right)$, where the parameters of $\mu = \varphi_1 a_\mathrm{b}^2$, $\sigma^2_{U_\mathrm{b}} = \frac{1}{2n}\left(1 + \varphi_2 - 2\varphi_1^2 a_\mathrm{b}^4\right)$ and $\sigma^2_{V_\mathrm{b}} = \frac{1}{2n}\left(1 - \varphi_2\right)$, and φ_j are the j^{th} circular moments of Θ_i. This implies that $R_\mathrm{b} = |H_\mathrm{b}|$ follows the Beckmann distribution [17] and hence, the average SNR at the legitimate receiver γ_b follows a (squared) Beckmann distribution which is fully characterized by the following set of parameters $K = \mu^2/(\sigma^2_{U_\mathrm{b}} + \sigma^2_{V_\mathrm{b}})$, $q = \sigma_{U_\mathrm{b}}/\sigma_{V_\mathrm{b}}$ and $\overline{\gamma}_\mathrm{b} = \mathbb{E}\{\gamma_\mathrm{b}\}$. We note that the parameters K and q have a similar definition as those of the Rician and Hoyt [18] distributions, respectively. In the scenario under consideration, we have that

$$K = n\frac{\varphi_1^2 a_\mathrm{b}^4}{1-\varphi_1^2 a_\mathrm{b}^4}, \tag{10}$$

$$q = \sqrt{\frac{1+\varphi_2-2\varphi_1^2 a_\mathrm{b}^4}{1-\varphi_2}}, \tag{11}$$

$$\overline{\gamma}_\mathrm{b} = n^2 \overline{\gamma}_{0,\mathrm{b}}\left[\varphi_1^2 a_\mathrm{b}^4 + \tfrac{1}{n}\left(1 - \varphi_1^2 a_\mathrm{b}^4\right)\right]. \tag{12}$$

As stated in [11], the average SNR scales with n^2. We also observe that the line-of-sight (LOS) condition of the equivalent scalar channel, captured by K, grows with n. Notably, the non-circular symmetry caused by the phase errors captured by $q \in [1, \infty)$ is independent of the number of elements of the LRS. We note that in the absence of phase errors, then H_b becomes a real Gaussian RV and hence $|H_\mathrm{b}|$ follows a folded normal (FN) distribution [19] with parameter K given by (10) with $\varphi_1 = 1$, and for which the PDF and CDF have a simple closed-form expression. The distribution of R_b is well approximated by a Nakagami-m distribution in [11], and hence γ_b can be approximated by a gamma distribution with shape parameter $m = \frac{n}{2}\frac{\varphi_1^2 a_\mathrm{b}^4}{1+\varphi_2-2\varphi_1^2 a_\mathrm{b}^4}$ and scale parameter $\overline{\gamma}_\mathrm{b} = n^2 \overline{\gamma}_{0,\mathrm{b}} \varphi_1^2 a_\mathrm{b}^4$. This can be seen as a generalization of the well-known approximation of the Rician distribution by a Nakagami-m distribution [20]. We see that similarly to K, m also scales with n. Because of the dissimilar behavior of the FN, the Beckmann and the Nakagami-m distributions in terms of diversity order [21], we will consider all such distributions in the derivation of the PLS performance metrics, in order to obtain insights on when these distributions are useful to approximate the true distribution of γ_b.

B. Distribution of $\gamma_{\rm e}$

When the LRS designs its phase shifts according to the legitimate link, the resulting phase distributions for each of the eavesdropper's R-E links Ψ_i are uniformly distributed by virtue of [14]. This implies that the distribution of $R_{\rm e} = |H_{\rm e}|$ is Rayleigh distributed according to [11, Corol. 2] with variance $\mathbb{E}\{R_{\rm e}^2\} = 1/n$. Hence, $\gamma_{\rm e}$ is exponentially distributed with $\overline{\gamma}_{\rm e} = n\overline{\gamma}_{0,{\rm e}}$.

Remark 1 (Scaling law for $\overline{\gamma}_{\rm e}$)**.** *Notably, the average SNR at the eavesdropper scales with n, whereas the average SNR at the legitimate receiver scales with n^2. Hence, the scaling law for the ratio of legitimate and wiretap SNRs is*

$$\left.\frac{\overline{\gamma}_{\rm b}}{\overline{\gamma}_{\rm e}}\right|_{n\uparrow} = n\frac{\overline{\gamma}_{0,{\rm b}}}{\overline{\gamma}_{0,{\rm e}}}\left[\varphi_1^2 a_{\rm b}^4 + \frac{1}{n}\left(1-\varphi_1^2 a_{\rm b}^4\right)\right] \tag{13}$$

This implies that, as long as the operational assumptions for the LRS hold, the use of a larger LRS can provide an SNR boost to the legitimate link compared to the eavesdropper's counterpart.

Inspection of (2) and (5) reveals that the legitimate and eavesdropper's links share a common part through $H_{i,1}$. However, we will now prove that both equivalent channels are statistically independent. This will allow to reformulate the PLS problem as a simpler one based on scalar channel representations, with evident analytical benefits as stated in the next Section.

Theorem 1 (Independence of legitimate and wiretap links)**.** *Let us consider the equivalent legitimate and wiretap channels in* (2) *and* (5)*. Then, H_b and H_e are independent if $\angle H_{i,{\rm e}} \sim \mathcal{U}[-\pi,\pi)$. This is the case, e.g., of considering Rayleigh fading for the LRS to eavesdropper's links.*

Proof. See Appendix A. □

IV. PLS Performance

We now derive analytical expressions for the chief PLS performance metrics defined previously. We consider three different scenarios for our analysis, which imply different approximations for the legitimate/wiretap links, respectively: (*a*) no phase errors – FN/Rayleigh case; (*b*) phase errors – Beckmann/Rayleigh case; (*c*) phase errors – Nakagami/Rayleigh case. We will refer to these scenarios with the subindices FR, BR and NR, respectively.

A. SOP Analysis

Lemma 1 (SOP in FNR scenario)**.** *The SOP and the asymptotic SOP expressions ($\overline{\gamma}_{\rm b} \to \infty$) in the absence of phase errors for LRS-aided communications are given by*

$$\mathrm{P}_{\rm FR} = 1 - Q_{0.5}\left(a_0, b_0\right) + e^{\frac{\tau-1}{\tau\overline{\gamma}_{\rm e}}+c_s}\frac{a_s}{\sqrt{K}}Q_{0.5}\left(a_s, b_s\right), \tag{14}$$

$$\mathrm{P}_{\rm FR}^{\infty} \simeq e^{-K/2+\frac{\tau-1}{\tau\overline{\gamma}_{\rm e}}}\sqrt{\frac{\tau\overline{\gamma}_{\rm e}(1+K)}{2\overline{\gamma}_{\rm b}}}\tilde{\Gamma}\left(1.5, \frac{\tau-1}{\tau\overline{\gamma}_{\rm e}}\right), \tag{15}$$

with $\tau = 2^{R_{\rm S}}$, $\tilde{\Gamma}(\cdot,\cdot)$ is the regularized upper incomplete Gamma function, $a_s = \sqrt{\frac{K(K+1)}{K+1-2\overline{\gamma}_{\rm b}s}}$, $b_s = \sqrt{2\left(\frac{K+1}{2\overline{\gamma}_{\rm b}} - s\right)z}$, $s = -\frac{1}{\tau\overline{\gamma}_{\rm e}}$, $z = \tau - 1$ and $c_s = \frac{K\overline{\gamma}_{\rm b}s}{K+1-2\overline{\gamma}_{\rm b}s}$. The Marcum Q-function of order 0.5 can be easily computed with the help of the Gaussian Q function as $Q_{0.5}(a,b) = Q(b-a)+Q(b+a)$.

Proof. First, (14) is obtained from [22] by specializing the parameter of the κ-μ distribution to $\mu_{\kappa\text{-}\mu} = 0.5$ and some manipulations. Then, (15) is obtained by using the approach in [23] with $\mu_{\kappa\text{-}\mu} = 0.5$, and then substituting in the definition of SOP followed by some manipulations. □

Lemma 2 (SOP in BR scenario)**.** *The SOP and the asymptotic SOP expressions ($\overline{\gamma}_{\rm b} \to \infty$) considering phase errors in the LRS-aided communications are given by*

$$\mathrm{P}_{\rm BR} = F_{\gamma_{\rm b}}(\tau-1) + \exp\left(\tfrac{\tau-1}{\tau\overline{\gamma}_{\rm e}}\right)\mathcal{M}_{\gamma_{\rm b}}^{u}\left(-\tfrac{1}{\tau\overline{\gamma}_{\rm e}}, \tau-1\right). \tag{16}$$

$$\mathrm{P}_{\rm BR}^{\infty} \simeq \exp\left(-\frac{K\left(1+q^2\right)}{2q^2}\right)\frac{(1+K)\left(1+q^2\right)(\overline{\gamma}_{\rm e}\tau+\tau-1)}{2q\overline{\gamma}_{\rm b}} \tag{17}$$

where $F_{\gamma_{\rm b}}(\cdot)$ [22, Eq. (7)] is the CDF of a squared Beckmann distribution, and $\mathcal{M}_{\gamma_{\rm b}}^{u}(\cdot,\cdot)$ [22, Eq. (3)] is the upper-incomplete moment generating function (MGF) of the RV $\gamma_{\rm b}$, which follows a squared Beckmann distribution.

Proof. $\mathrm{P}_{\rm BR}$ can be obtained directly from [22, Eq. (21)] with the respective substitutions. On the other hand, the $\mathrm{P}_{\rm BR}^{\infty}$ is derived by using [21, Proposition 3], in which $d = 1$, using the MGF of γ_b. □

Lemma 3 (SOP in NR scenario)**.** *The SOP and the asymptotic SOP expressions ($\overline{\gamma}_{\rm b} \to \infty$) considering phase errors in the LRS-aided communications can be approximated as*

$$\mathrm{P}_{\rm NR} = \tilde{\gamma}\left(m, \tfrac{(\tau-1)m}{\overline{\gamma}_{\rm b}}\right) + e^{\frac{\tau-1}{\tau\overline{\gamma}_{\rm e}}}\frac{\tilde{\Gamma}\left(m, (\tau-1)\left(\frac{m}{\overline{\gamma}_{\rm b}}+\frac{1}{\tau\overline{\gamma}_{\rm e}}\right)\right)}{\left(1+\frac{\overline{\gamma}_{\rm b}}{m\tau\overline{\gamma}_{\rm e}}\right)^{m}}, \tag{18}$$

$$\mathrm{P}_{\rm NR}^{\infty} \simeq e^{\frac{\tau-1}{\tau\overline{\gamma}_{\rm e}}}\left(\tfrac{\tau m\overline{\gamma}_{\rm e}}{\overline{\gamma}_{\rm b}}\right)^{m}\tilde{\Gamma}\left(m+1, \tfrac{\tau-1}{\tau\overline{\gamma}_{\rm e}}\right). \tag{19}$$

where $\tilde{\gamma}(\cdot,\cdot)$ is the regularized lower incomplete Gamma functions [24, Eq. (8.350.1)].

Proof. As in the proof of Lemma 2, (18) is obtained from [22] by setting the parameters of the κ-μ distribution $\kappa = 0$ and $\mu = m$. Then, (19) is obtained as a particular case of [16, Eq. (21)] with the respective substitutions. □

All performance metrics in Lemmas 1-3 are given in closed-form except for (16), for which the evaluation of $\mathcal{M}_{\gamma_{\rm b}}^{u}(\cdot,\cdot)$ is carried out numerically through an inverse Laplace transformation [25] over a shifted and scaled version of the (conventional) MGF of $\gamma_{\rm b}$, as in [22, Eq. 4], which is obtained from [20, Eq. (2.41)] with $r \to \infty$. Inspection of (15), (17) and (19) reveals a different secrecy diversity order for each of the approximations, i.e., $1/2$, 1 and m for the FR, BR and NR cases, respectively. The implications arising from this observation will be discussed in the Numerical Results section.

B. ASR Analysis

For compactness, we use a common formulation for the ASR metrics in the FR, NR and BR scenarios.

Lemma 4. *The ASR and the asymptotic ASR ($\overline{\gamma}_{\rm b} \to \infty$) formulations over Z/Rayleigh fading channels for LRS-aided communications can be obtained as*

$$\mathcal{R}_{\rm S} = \overline{C}_{\rm B} - \overline{C}_{\rm E} + \mathcal{G}_{\rm Z}\left(\overline{\gamma}_{\rm b}, \overline{\gamma}_{\rm e}\right) \tag{20}$$

$$\mathcal{R}_{\rm S}^{\infty} \approx \overline{C}_{\rm B} - \overline{C}_{\rm E}, \tag{21}$$

$$\approx \log_2\left(\overline{\gamma}_{\rm b}\right) - t_{\rm Z} - \overline{C}_{\rm E}, \tag{22}$$

where Z=$\{$*Folded Normal*, *Beckmann*, *Nakagami*$\}$ *indicates the distribution of the legitimate link, and* $t_{\rm Z}$ *is a constant value that captures the fading severity loss of the legitimate link [16]. We note that* $\overline{C}_{\rm E} = \frac{e^{1/\overline{\gamma}_{\rm e}}}{\ln 2} E_1\left(\frac{1}{\overline{\gamma}_{\rm e}}\right)$ *denotes the average capacity of the wiretap link under the Rayleigh approximation, with* $E_1(\cdot)$ *being the Exponential integral function, and the term* $\mathcal{G}_{\rm Z}(\overline{\gamma}_{\rm b}, \overline{\gamma}_{\rm e}) = \frac{e^{1/\overline{\gamma}_{\rm e}}}{\ln 2} \int_0^1 \frac{1}{u} e^{-1/(u\overline{\gamma}_{\rm e})} M_{\gamma_{\rm b}}\left(\frac{-1}{u\overline{\gamma}_{\rm e}}\right) du \geq 0$*, where* $\mathcal{M}_{\gamma_{\rm b}}(\cdot)$ *is the (conventional) MGF of* $\gamma_{\rm b}$.

Proof. See Appendix B. □

The previous Lemma allows us to evaluate the ASR in the investigated scenario in a compact form. Analytical expressions for $\overline{C}_{\rm B}$ can be derived in all instances using a similar approach as in [26, 27], although they are not explicitly reproduced due to space limitation. We note that as pointed out in [16], the term $\mathcal{G}_{\rm Z}(\overline{\gamma}_{\rm b}, \overline{\gamma}_{\rm e})$ vanishes as $\overline{\gamma}_{\rm b}$ grows, which in our case happens as n is increased.

V. Numerical evaluation

We now evaluate the effect of phase errors on the secrecy performance metrics in the investigated scenario, as well as the goodness of the scalar approximations for the equivalent composite channel in LRS-assisted communications. For the links between A and the LRS, and between the LRS and B, we consider Rician fading with parameter $K = 1$. The links between the LRS and E are assumed to be Rayleigh distributed, so that $a_1 = a_{2,\rm b} = \sqrt{\pi/(4(K+1))}\,{}_1F_1(-1/2, 1, -K)$, where ${}_1F_1(\cdot)$ is Kummer hypergeometric's function, and $a_{2,\rm e} = \sqrt{\pi}/2$. For compactness, we consider phase errors due to the finite number of phase shifts available at the LRS; similar conclusions can be extracted by using the phase error model [11], based on the Von Mises distribution. Hence, the phase errors are uniformly distributed in the interval $[-u_{n_b}, u_{n_b}]$ with $u_{n_{\rm b}} = -2^{-n_b}\pi$, where $n_{\rm b}$ is the number of quantization bits used to encode the phase shifts. Thus, from [11] we have $\varphi_i = \frac{\sin(u_{n_{\rm b}+1-i})}{u_{n_{\rm b}+1-i}}$ for $i = \{1, 2\}$.

In the next figures, we set $\overline{\gamma}_{0,\rm e} = 10$ dB, a fixed transmit power P_T, and study the effect of increasing $n_{\rm b}$; the ideal case of no phase errors is included as a reference in all instances. The exact values for the secrecy metrics are obtained through Monte Carlo (MC) simulations. The analytical secrecy performance metrics in the FR, NR, and BR cases are included using the results in Section IV. These have also been double-checked offline with additional MC simulations, which are not included in the figures for the sake of readability.

Fig. 1 shows the ASR as a function of $\overline{\gamma}_{0,\rm b}$, for different values of $n_{\rm b}$ and number of elements at the LRS through n. Theoretical values have been evaluated with the analytical expressions for (20) and are represented using solid lines. Asymptotic values are computed with (21) for the BR case, and as (22) for the FR and NR cases with $t_{\rm FR}$ and $t_{\rm NR}$ in [27, Table II]. We extract important insights from the observation of Fig. 1: (*i*) increasing n allows for improving the ASR for a fixed $\overline{\gamma}_{0,\rm b}$, thanks to the different scaling laws of the legitimate and wiretap average SNRs; (*ii*) FR (no phase errors) and BR (phase errors) equivalent scalar approximations work pretty well regardless of n, while the NR one underestimates the true

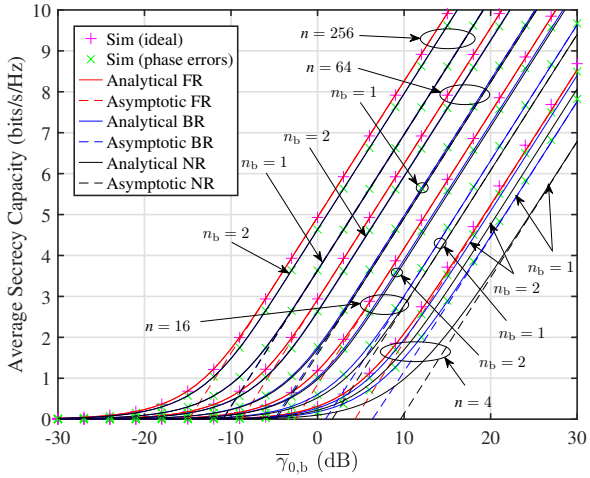

Fig. 1. ASR as a function of $\overline{\gamma}_{0,\rm b}$ for different values of $n_{\rm b}$ and n. Markers correspond to the legitimate and eavesdropper channels in (2) and (5).

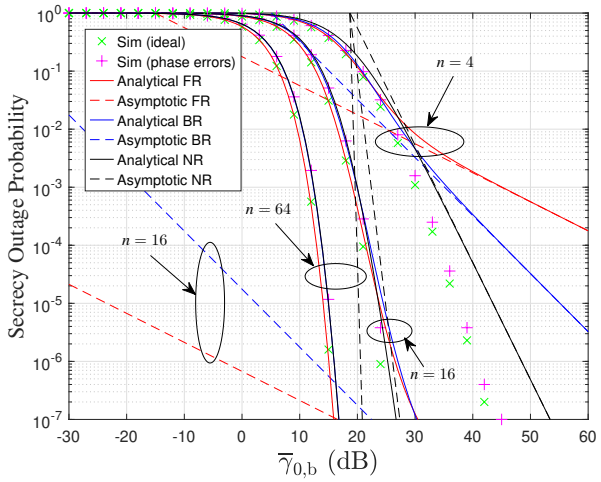

Fig. 2. SOP as a function of $\overline{\gamma}_{0,\rm b}$ for different values of n with $n_{\rm b} = 2$ and $n_{\rm b} \to \infty$. Markers correspond to the legitimate and eavesdropper channels in (2) and (5).

ASR for low n; (*iii*) asymptotic ASR expressions are tight for a wide range of SNR values; (*iv*) $\mathcal{R}_{\rm S}$ exhibits a linear behavior in log-scale for a wide range of SNRs, and such range of SNRs widens with n; and (*v*) the performance degradation with $n_{\rm b} = 2$ bits is small, which confirms that state-of-the-art solutions for LRS surfaces [28] may be enough to obtain a secrecy performance close to the case of no phase errors. Indeed, all previous remarks hold as long as the operating assumptions of the LRS in terms of size as n grows are valid.

Fig. 2 shows the SOP as a function of $\overline{\gamma}_{0,\rm b}$, for different values of n and $n_{\rm b} = \{2, \infty\}$. Theoretical values have been evaluated with the expressions included in Lemmas 1 to 3. Similar conclusions as in the ASR can be extracted, especially confirming that $n_{\rm b} = 2$ bits allow for a good performance compared to the ideal case. However, some relevant differences are observed: while the equivalent scalar approximations work well in all instances for large n, there are substantial differences between the exact simulated results and the FR, BR, and NR cases for lower n. More importantly, the asymptotic results for the SOP may induce to confusion if not interpreted

properly: while all asymptotic results are tight (i.e., they all coincide with the analytical SOP expressions for each case), the different secrecy diversity order inherent to each of the equivalent scalar approximations is translated into a different decay of the high-SNR slopes. Because of the high line-of-sight condition of the FR and BR scalar approximations, the asymptotes kick-in at very low SOP values; conversely, the NR asymptote seems to better capture the abrupt decay of the SOP for the operating range of probability values. In any case, asymptotic analyses for the SOP should be exercised with caution when using the equivalent scalar approximations, as they may not be representative of the actual behavior of the real LRS-assisted channel.

VI. Conclusions

The potential of LRS for PLS and the usefulness of equivalent scalar channel approximations for performance evaluation in such contexts have been exemplified, both theoretically and by simulation. Even when the LRS has a limited phase resolution of 2 bits, the different scaling laws for the desired and eavesdropper's SNRs allows for improving the PLS performance in LRS-assisted communications. Relevant aspects such as the consideration of multiantenna terminals and multiple agents, the optimal design of beamforming and phase-shifts, the effect of a direct link between the legitimate users, and the impact of spatial correlation and imperfect amplitude reflection in the LRS are key problems to be further investigated.

Appendix A
Proof of Theorem 1

Using the law of total expectation, and conditioning on the set $Z = \{H_{i,1}, H_{i,b}, \Theta_i\}$, we can write $\mathbb{E}\{H_\mathrm{b}H_\mathrm{e}\} = \mathbb{E}\{\mathbb{E}\{H_\mathrm{b}H_\mathrm{e}|Z\}\} = \mathbb{E}\{H_\mathrm{b}\mathbb{E}\{H_\mathrm{e}|Z\}\}$. Now, the inner expectation can be expanded as $\mathbb{E}\{H_\mathrm{e}|Z\} = \frac{1}{n}\sum_{i=1}^{n}|H_{i,1}|\mathbb{E}\left\{|H_{i,\mathrm{e}}|e^{j\Psi_i}\right\}$. Now, by virtue of [14] the distribution of Ψ_i is uniform in any interval of length 2π provided that $\angle H_{i,\mathrm{e}}$ is uniformly distributed in the same interval. Under the mild assumption that $|H_{i,\mathrm{e}}|$ and $e^{j\Psi_i}$ are independent, which is the case for instance of $|H_{i,\mathrm{e}}|$ being Rayleigh distributed, then it yields that $\mathbb{E}\{H_\mathrm{e}|Z\} = 0$. Hence, the independence between H_b and H_e is stated.

Appendix B
Proof of Lemma 4

From the definitions in [16, Eq. (29)] and [16, Eq. (30)], we use the expression of the CDF of the exponential distribution for the wiretap link. After integration by parts, two terms are identified; the first one corresponds to $\overline{C}_\mathrm{E}$ in (20), whereas the second one reduces to $\mathcal{G}_\mathrm{Z}(\overline{\gamma}_\mathrm{b}, \overline{\gamma}_\mathrm{e})$ after: (*i*) leveraging the integral definition of the Exponential integral function in [24] in (20), (*ii*) changing the order of integration, and (*iii*) using the definition of the MGF. As for the asymptotic ASR results, they hold by virtue of [16, eq. (43)].

References

[1] 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, 2020.

[2] D. Li, "Ergodic Capacity of Intelligent Reflecting Surface-Assisted Communication Systems With Phase Errors," *IEEE Commun. Lett.*, vol. 24, no. 8, pp. 1646–1650, 2020.

[3] Y. Han, W. Tang, S. Jin, C. Wen, and X. Ma, "Large Intelligent Surface-Assisted Wireless Communication Exploiting Statistical CSI," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8238–8242, 2019.

[4] S. Hong, C. Pan, H. Ren, K. Wang, K.K. Chai, and A. Nallanathan, "Robust Transmission Design for Intelligent Reflecting Surface Aided Secure Communication Systems with Imperfect Cascaded CSI," *arXiv preprint arXiv:2004.11580*, 2020.

[5] K. Zhi, C. Pan, H. Ren, and K. Wang, "Uplink Achievable Rate of Intelligent Reflecting Surface-Aided Millimeter-Wave Communications with Low-Resolution ADC and Phase Noise," Aug 2020, arXiv:2008.00437.

[6] D. P. Osorio, J. D. Vega Sánchez, and H. Alves, *Physical-Layer Security for 5G and Beyond*, ch. 1, pp. 1–19. John Wiley & Sons, 2019.

[7] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, 2019.

[8] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2019.

[9] J. Chen, Y. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599–82612, 2019.

[10] G. Zhou, C. Pan, H. Ren, K. Wang, A. Nallanathan, and K.K. Wong, "User Cooperation for IRS-aided Secure SWIPT MIMO: Active Attacks and Passive Eavesdropping," *arXiv preprint arXiv:2006.05347*, 2020.

[11] M. Badiu and J. P. Coon, "Communication Through a Large Reflecting Surface With Phase Errors," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 184–188, 2020.

[12] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M. Alouini, R. Zhang, "Wireless Communications Through Reconfigurable Intelligent Surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

[13] B. Feng, Y. Wu, and M. Zheng, "Secure Transmission Strategy for Intelligent Reflecting Surface Enhanced Wireless System," in *11th Int. Conf. on Wireless Commun. and Signal Proc. (WCSP)*, pp. 1–6, 2019.

[14] F. J. Scire, "A probability density function theorem for the modulo y values of the sum of two statistically independent processes," *Proc. IEEE*, vol. 56, pp. 204–205, Feb 1968.

[15] A. D. Wyner, "The Wire-Tap Channel," *Bell Labs Tech. J.*, vol. 54, pp. 1355–1367, Apr. 1975.

[16] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. N. Nkouatchah, and U. S. Dias, "Transmit Antenna Selection in Secure MIMO Systems Over $\alpha-\mu$ Fading Channels," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6483–6498, 2019.

[17] P. Beckmann, "Statistical distribution of the amplitude and phase of a multiply scattered field," *J. Res. Natl. Bur. Stand. (U. S.)-D. Radio Propagation*, vol. 66D, no. 3, pp. 231–240, 1962.

[18] R. S. Hoyt, "Probability Functions for the Modulus and Angle of the Normal Complex Variate," *Bell Labs Tech. J.*, vol. 26, pp. 318–359, Apr. 1947.

[19] J. Reig, V. M. Rodrigo Peñarrocha, L. Rubio, M. T. Martínez-Inglés, and J. M. Molina-García-Pardo, "The Folded Normal Distribution: A New Model for the Small-Scale Fading in Line-of-Sight (LOS) Condition," *IEEE Access*, vol. 7, pp. 77328–77339, 2019.

[20] M. K. Simon and M.-S. Alouini, *Digital Communications over Fading Channels*. John Wiley & Sons, Inc., 2 ed., 2005.

[21] Z. Wang and G. B. Giannakis, "A simple and general parameterization quantifying performance in fading channels," *IEEE Trans. Commun.*, vol. 51, no. 8, pp. 1389–1398, 2003.

[22] F. J. Lopez-Martinez, J. M. Romero-Jerez, and J. F. Paris, "On the Calculation of the Incomplete MGF With Applications to Wireless Communications," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 458–469, 2017.

[23] V. Perim, J. D. V. Sánchez, and J. C. S. S. Filho, "Asymptotically exact approximations to generalized fading sum statistics," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 205–217, 2020.

[24] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*. San Diego, CA, USA: Academic Press, 7 ed., 2007.

[25] J. Abate and W. Whitt, "Numerical Inversion of Laplace Transforms of Probability Distributions," *ORSA J. Comput.*, vol. 7, no. 1, pp. 36–43, 1995.

[26] D. B. Da Costa and M. D. Yacoub, "Average channel capacity for generalized fading scenarios," *IEEE Commun. Lett.*, vol. 11, no. 12, pp. 949–951, 2007.

[27] L. Moreno-Pozas, F. J. Lopez-Martinez, J. F. Paris, and E. Martos-Naya, "The κ–μ Shadowed Fading Model: Unifying the κ–μ and η–μ Distributions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9630–9641, 2016.

[28] L. D. et al., "Reconfigurable Intelligent Surface-Based Wireless Communications: Antenna Design, Prototyping, and Experimental Results," *IEEE Access*, vol. 8, pp. 45913–45923, 2020.