



Secure Outage Analysis of RIS-Assisted Communications With Discrete Phase Control

Wei Shi, Jindan Xu, Wei Xu, Marco Di Renzo, Chunming Zhao

► To cite this version:

Wei Shi, Jindan Xu, Wei Xu, Marco Di Renzo, Chunming Zhao. Secure Outage Analysis of RIS-Assisted Communications With Discrete Phase Control. IEEE Transactions on Vehicular Technology, 2023, 72 (4), pp.5435-5440. 10.1109/TVT.2022.3224967 . hal-04261257

HAL Id: hal-04261257

<https://hal.science/hal-04261257>

Submitted on 26 Oct 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Secure Outage Analysis of RIS-Assisted Communications with Discrete Phase Control

Wei Shi, Jindan Xu, Wei Xu, *Senior Member, IEEE*, Marco Di Renzo, *Fellow, IEEE*, and Chunming Zhao

Abstract

This correspondence investigates a reconfigurable intelligent surface (RIS)-assisted wireless communication system with security threats. The RIS is deployed to enhance the secrecy outage probability (SOP) of the data sent to a legitimate user. By deriving the distributions of the received signal-to-noise-ratios (SNRs) at the legitimate user and the eavesdropper, we formulate, in a closed-form expression, a tight bound for the SOP under the constraint of discrete phase control at the RIS. The SOP is characterized as a function of the number of antenna elements, N , and the number of discrete phase choices, 2^b . It is revealed that the performance loss in terms of SOP due to the discrete phase control is ignorable for large N when $b \geq 3$. In addition, we explicitly quantify this SOP loss when binary phase shifts with $b = 1$ is utilized. It is identified that increasing the RIS antenna elements by 1.6 times can achieve the same SOP with binary phase shifts as that by the RIS with ideally continuous phase shifts. Numerical simulations are conducted to verify the accuracy of these theoretical observations.

Index Terms

Reconfigurable intelligent surface (RIS), physical layer security, secrecy outage probability, discrete phase shifts.

I. INTRODUCTION

Reconfigurable intelligent surface (RIS) is a metasurface that consists of a large number of passive reflecting elements with integrated low power electronics [1] [2]. A main feature of an RIS is that the amplitude and phase of each reflecting element can be independently controlled through software, thereby realizing passive beamforming (BF) for improving the signal quality at intended receivers. Due to these merits, RISs have been considered for various wireless applications, e.g., in millimeter-wave (mmWave) [3] and Terahertz (THz) [4] communications, to enhance spectral and energy efficiencies [5].

Copyright (c) 2015 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

Wei Shi, Wei Xu, Jindan Xu, and Chunming Zhao are with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: {wshi, wxu, jdxu, cmzhao}@seu.edu.cn).

Marco Di Renzo is with Université Paris-Saclay, CNRS, CentraleSupélec, Laboratoire des Signaux et Systèmes, 3 Rue Joliot-Curie, 91192 Gif-sur-Yvette, France (e-mail: marco.di-renzo@universite-paris-saclay.fr).

In recent years, physical layer security (PLS) has gained considerable interest for securing wireless communications. As a complement to conventional cryptographic methods, PLS ensures secure communications by exploiting the dynamics of propagation channels. Since RISs have the ability of adjusting the propagation channels, their deployment empowers the design of PLS with an additional dimension by exploiting passive BF. In order to maximize the theoretical secrecy, literature [6]–[8] investigated joint optimization of the active and passive BFs at the transmitter and RIS, respectively. In [9], the average secrecy rate (SR) was characterized for an RIS-assisted two-way communication system through a lower bound. More recently in [10], the SR was further analyzed for a system where the RIS reflection is utilized as a multiplicative randomness against a wiretapper.

Besides the analysis of SR, secrecy outage probability (SOP) is another relevant performance measure to quantify the performance of PLS, especially for systems undergoing slow-varying channels. The SOP is defined as the probability that the instantaneous secrecy capacity falls below a target SR. The SOPs of RIS-aided communication systems have been investigated in [11]–[13]. Both analytical and asymptotic analyses have been provided to reveal the impacts of key system parameters on SOP. In particular, the work in [12] considered the SOP of an RIS-aided unmanned aerial vehicle (UAV) relay system. In [13], the authors analyzed the SOP as well as the probability of non-zero secrecy capacity of an RIS-aided device-to-device (D2D) communication system. However, most studies on SOP analysis considered RIS with continuous phase shifts, which leads to unaffordable high complexity in practice. Even though discrete phase shifts have been considered for RIS reflection optimizations, e.g., in [14] [15], few studies have been conducted on theoretical performance analysis with discrete RIS phase shifts especially in terms of SOP. Quantitative insight on RIS design has only been discovered for some non-security scenarios [16]. This is because discrete phase shifts make the performance expressions of the cascaded RIS channels much less tractable. In particular for secure communications, it can be even challenging to directly derive the corresponding cascaded channel distributions of both the legitimate user and eavesdropper.

In this work, we investigate the SOP of an RIS-assisted secure communication system and quantitatively characterize the impacts of discrete phase shifts in closed-form expressions. Concretely, we first derive the exact distributions of the received signal-to-noise-ratios (SNRs) at the legitimate user and the eavesdropper. Then, we present a closed-form expression for a tight upper bound of the SOP. Based on the obtained expressions, the asymptotic scaling law of SOP is characterized in high-SNR regimes. In particular, the SOP decreases with the slope of $e^{-0.8N}$ for large N and $b \geq 3$, where N is the number of RIS elements and b is the number of quantization bits. Compared with the ideally continuous phase control, we further obtain that the performance loss in terms of SOP caused by using binary phase shifts, i.e., $b=1$, can be compensated by deploying a larger RIS with size $1.6N$.

The remainder of this paper is organized as follows. The system model is introduced in Section II. In Section III, we derive the distribution of the received SNRs at the legitimate user and at the eavesdropper. In Section IV, we provide a closed-form expression for an upper bound of the SOP, and we study it in notable asymptotic regimes. Simulation results and conclusions are given in Section V and VI, respectively.

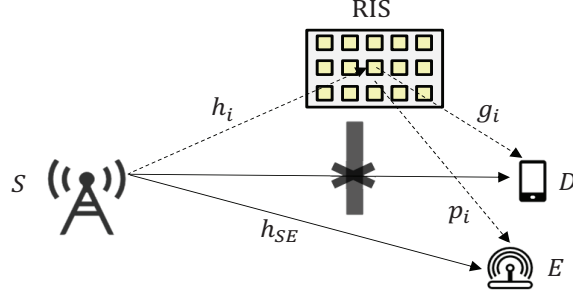


Fig. 1. The system model of an RIS-assisted secure communication.

II. SYSTEM MODEL

We consider an RIS-assisted secure communication system consisting of a source (S), an RIS with N reflecting elements, a legitimate user (D), and an eavesdropper (E), as illustrated in Fig. 1. The direct link between S and D is assumed to be blocked by obstacles, such as buildings, which is likely to occur at high frequency bands. In this scenario, the data transmission between S and D is ensured by the RIS. The eavesdropper is at a location where it can overhear the information from both S and the RIS.¹ Nodes S , D , and E are equipped with a single antenna for transmission and reception and all links experience Rayleigh fading.² The channel coefficients of the S -RIS, RIS- D , RIS- E , and S - E links are respectively denoted by h_i , g_i , p_i , and $h_{SE} \sim \mathcal{CN}(0, 1)$, where $\mathcal{CN}$ is the complex Gaussian distribution. By applying channel estimation methods in [3], [4] and the references therein, we assume that the channel coefficients of h_i and g_i are perfectly known to S . However, the channel gains of p_i and h_{SE} are not available to S , as the eavesdropper is usually a passive device that does not emit signals.

By assuming quasi-static flat fading channels, the signal received at D is expressed as

$$r_D = \sqrt{P} \left[\eta (d_{SR} d_{RD})^{-v/2} \sum_{i=1}^N h_i g_i e^{j\phi_i} \right] x + n_D, \quad (1)$$

where P denotes the transmit power at S , x is the transmit signal, $\eta \in (0, 1]$ is the RIS amplitude reflection coefficient with $\eta = 1$ corresponding to lossless reflection, $\{\phi_i\}_{i=1}^N$ represents the phase shift of the i th reflecting element of the RIS, and $n_D \sim \mathcal{CN}(0, N_0)$ is the additive white Gaussian noise (AWGN) with zero mean and variance N_0 . Without loss of generality, the signal power is normalized, i.e., $\mathbb{E}[|x|^2] = 1$ where $\mathbb{E}[\cdot]$ denotes the expectation of a random variable (RV). In addition, d_{SR} and d_{RD} are the distances of the S -RIS and RIS- D links, respectively, and v is the path loss exponent.

From (1), the received SNR at D is calculated as

$$\gamma_D = \frac{\eta^2 P \left| \sum_{i=1}^N h_i g_i e^{j\phi_i} \right|^2}{N_0 d_{SR}^v d_{RD}^v}. \quad (2)$$

In the case of ideally continuous phase shifts, γ_D is maximized by setting the phases of the RIS elements equal to $\phi_i = \phi_i^{\text{opt}} \triangleq -\angle(h_i g_i)$, where $\angle$ returns the phase of the complex number. This optimized phase compensates the

¹The direct link between S and E exists when the eavesdropper is not blocked by obstacles [11] [13].

²The RIS-related links can be modeled as Rayleigh fading, also as [11] [13], when the RIS is not optimally deployed to ensure strong LoS links.

phase shift introduced by fading channels. Due to hardware limitations, however, the phase shifts $\{\phi_i\}_{i=1}^N$ of the RIS elements are usually limited to a finite number of controllable discrete values. In particular, the set of discrete phase shifts is denoted by $\mathcal{A} \triangleq \left\{0, \frac{2\pi}{2^b}, \dots, \frac{(2^b-1)2\pi}{2^b}\right\}$, where b is the number of quantization bits. In this case, usually, the phase shift of the i th RIS element, $\phi_i^{\text{sub}} \in \mathcal{A}$, is chosen as

$$\phi_i^{\text{sub}} \triangleq \arg \min_{\phi \in \mathcal{A}} \{|\phi_i^{\text{opt}} - \phi|\}. \quad (3)$$

Then, the received SNR in the presence of the discrete phase shifts is rewritten as

$$\gamma_D = \bar{\gamma}_{SRD} \left| \sum_{i=1}^N h_i g_i e^{j\phi_i^{\text{sub}}} \right|^2, \quad (4)$$

where $\bar{\gamma}_{SRD} \triangleq \frac{\eta^2 P}{N_0 d_{SR}^v d_{RD}^v}$ denotes the average SNR.

The eavesdropper receives signals from the direct link from S and the reflected link from the RIS. Then, the received signal at E is written as

$$r_E = \sqrt{P} \left[\eta (d_{SR} d_{RE})^{-v/2} \sum_{i=1}^N h_i p_i e^{j\phi_i^{\text{sub}}} + d_{SE}^{-v/2} h_{SE} \right] x + n_E, \quad (5)$$

where d_{RE} and d_{SE} denote the distances of the RIS- E and S - E links, respectively, and $n_E \sim \mathcal{CN}(0, N_0)$ is the AWGN at E . Then, the received SNR at E is

$$\gamma_E = \left| \sqrt{\bar{\gamma}_{SRE}} \sum_{i=1}^N h_i p_i e^{j\phi_i^{\text{sub}}} + \sqrt{\bar{\gamma}_{SE}} h_{SE} \right|^2, \quad (6)$$

where $\bar{\gamma}_{SRE} \triangleq \frac{\eta^2 P}{N_0 d_{SR}^v d_{RE}^v}$ and $\bar{\gamma}_{SE} \triangleq \frac{\eta^2 P}{N_0 d_{SE}^v}$ represent the average SNRs of the S -RIS- E and S - E links, respectively.

III. DISTRIBUTIONS OF THE RECEIVED SNRS

In order to analyze the SOP of the system, we need to first characterize the distributions of γ_D and γ_E .

A. Distribution of γ_D

Let us denote the quantization error of phase shifts by $\Theta_i \triangleq \phi_i^{\text{sub}} - \phi_i^{\text{opt}}$, which is uniformly distributed [14] [15] [17], i.e., $\Theta_i \sim \mathcal{U}(-2^{-b}\pi, 2^{-b}\pi)$. Then, γ_D in (4) is rewritten as

$$\begin{aligned} \gamma_D &\stackrel{(a)}{=} \bar{\gamma}_{SRD} \left| \sum_{i=1}^N h_i g_i e^{j(\Theta_i + \phi_i^{\text{opt}})} \right|^2 \stackrel{(b)}{=} \bar{\gamma}_{SRD} \left| \sum_{i=1}^N |h_i| |g_i| e^{j\Theta_i} \right|^2 \\ &\stackrel{(c)}{=} \bar{\gamma}_{SRD} (X^2 + Y^2) \stackrel{(d)}{=} \gamma_{D_1} + \gamma_{D_2}, \end{aligned} \quad (7)$$

where (a) follows by the identity $\phi_i^{\text{sub}} = \Theta_i + \phi_i^{\text{opt}}$, (b) is obtained by using $\phi_i^{\text{opt}} = -\angle(h_i g_i)$, (c) follows by the definitions $X \triangleq \sum_{i=1}^N |h_i| |g_i| \cos \Theta_i$ and $Y \triangleq \sum_{i=1}^N |h_i| |g_i| \sin \Theta_i$, and (d) is obtained by defining $\gamma_{D_1} \triangleq \bar{\gamma}_{SRD} X^2$ and $\gamma_{D_2} \triangleq \bar{\gamma}_{SRD} Y^2$. Before deriving the distribution of γ_D , we introduce the following lemma.

Lemma 1: If N is large, γ_{D_1} and γ_{D_2} are statistically independent. Also, the cumulative distribution function (CDF) of γ_{D_1} and the probability density function (PDF) of γ_{D_2} are, respectively,

$$F_{\gamma_{D_1}}(x) = 1 - \frac{1}{2} \operatorname{erfc} \left(\frac{\alpha + \sqrt{x}}{\beta} \right) - \frac{1}{2} \operatorname{erfc} \left(\frac{\sqrt{x} - \alpha}{\beta} \right), \quad (8)$$

$$f_{\gamma_{D_2}}(y) = \frac{\lambda^\mu y^{\mu-1}}{\Gamma(\mu)} e^{-\lambda y}, \quad (9)$$

where $\alpha = m_1 \sqrt{\gamma_{SRD}}$, $\beta = \sqrt{2} \sigma_1 \sqrt{\gamma_{SRD}}$, $m_1 = \frac{N\pi}{4} \text{sinc}(2^{-b})$, $\sigma_1^2 = \frac{N}{2} [1 + \text{sinc}(2^{1-b})] - \frac{N\pi^2}{16} \text{sinc}^2(2^{-b})$, $\lambda = \frac{1}{2\sigma_2^2 \gamma_{SRD}}$, $\mu = \frac{1}{2}$, $\sigma_2^2 = \frac{N}{2} [1 - \text{sinc}(2^{1-b})]$, where $\text{sinc}(x) \triangleq \frac{\sin \pi x}{\pi x}$ and $\Gamma(\cdot)$ is the Gamma function [18, Eq. (8.310)].

Proof: The proof of the independence of γ_{D_1} and γ_{D_2} for large values of N is provided in Appendix A. Specifically, by applying the central limit theorem (CLT) [19], X and Y converge in distribution to Gaussian RVs for large N . Since $|h_i|$ and $|g_i|$ are independently distributed Rayleigh RVs with mean $\sqrt{\pi}/2$ and variance $(4-\pi)/4$, we obtain $\mathbb{E}[X] = m_1$, $\text{Var}[X] = \sigma_1^2$, $\mathbb{E}[Y] = 0$, and $\text{Var}[Y] = \sigma_2^2$. It follows

$$X \xrightarrow{d} \mathcal{N}(m_1, \sigma_1^2), \quad Y \xrightarrow{d} \mathcal{N}(0, \sigma_2^2), \quad (10)$$

where $\xrightarrow{d}$ denotes the convergence in distribution by virtue of the CLT. γ_{D_1} is a non-central χ^2 RV and γ_{D_2} is a central χ^2 RV with one degree of freedom, where χ^2 denotes the Chi-square distribution. Then, by using [20, Eq. (2.3-35)] and [21, Eq. (27)], $F_{\gamma_{D_1}}(\cdot)$ is derived. The PDF $f_{\gamma_{D_2}}(\cdot)$ is obtained from [20, Eq. (2.3-28)]. The proof completes. ■

By applying *Lemma 1* and (7), the CDF of γ_D equals

$$\begin{aligned} F_{\gamma_D}(z) &= \iint_D f_{\gamma_{D_1}, \gamma_{D_2}}(x, y) dx dy \\ &\stackrel{(d)}{=} \int_0^z f_{\gamma_{D_2}}(y) F_{\gamma_{D_1}}(z-y) dy \\ &\stackrel{(e)}{=} \int_0^z \frac{\lambda^\mu y^{\mu-1}}{\Gamma(\mu)} e^{-\lambda y} \times \left[1 - \frac{1}{2} \text{erfc}\left(\frac{\sqrt{z-y} + \alpha}{\beta}\right) \right. \\ &\quad \left. - \frac{1}{2} \text{erfc}\left(\frac{\sqrt{z-y} - \alpha}{\beta}\right) \right] dy, \end{aligned} \quad (11)$$

where $D \triangleq \{(x, y) : x + y \leq z, x > 0, y > 0\}$, (d) utilizes the independence of γ_{D_1} and γ_{D_2} in *Lemma 1*, and (e) is obtained by using (8) and (9).

B. Distribution of γ_E

Let us first consider the distribution of $Z \triangleq \sqrt{\gamma_{SRE}} \sum_{i=1}^N h_i p_i e^{j\phi_i^{\text{sub}}} + \sqrt{\gamma_{SE}} h_{SE}$. Then, γ_E in (6) can be calculated according to the relationship of $\gamma_E = |Z|^2$. The distribution of Z is provided in the following lemma.

Lemma 2: For large N , $Z \xrightarrow{d} \mathcal{CN}(0, N\bar{\gamma}_{SRE} + \bar{\gamma}_{SE})$, and the real and imaginary parts of Z are independent RVs with equal variance.

Proof: See Appendix B. ■

As disclosed in *Lemma 2*, γ_E has an exponential distribution with mean $N\bar{\gamma}_{SRE} + \bar{\gamma}_{SE}$. Therefore, the PDF of γ_E is

$$f_{\gamma_E}(x) = \epsilon e^{-\epsilon x}, \quad x \geq 0 \quad (12)$$

where $\epsilon = 1/(N\bar{\gamma}_{SRE} + \bar{\gamma}_{SE})$.

IV. THEORETICAL ANALYSIS OF THE SOP

A. SOP Analysis

The SOP is an essential performance metric to quantify the performance of PLS, which is defined as the probability that the instantaneous secrecy capacity falls below a target positive SR C_{th} . From [11]–[13] [22], the SOP is calculated as

$$\begin{aligned} \text{SOP} &= \Pr(\ln(1 + \gamma_D) - \ln(1 + \gamma_E) < C_{\text{th}}) \\ &= \int_0^\infty F_{\gamma_D}((1+x)\varphi - 1) f_{\gamma_E}(x) dx, \end{aligned} \quad (13)$$

where $\varphi \triangleq e^{C_{\text{th}}}$. It is still difficult to compute (13) because the CDF of γ_D in (11) involves an intractable integral. Thus, instead of seeking for a closed-form expression for the SOP, we derive an upper bound as follows

$$\text{SOP} < \int_0^\infty F_{\gamma_{D_1}}((1+x)\varphi - 1) f_{\gamma_E}(x) dx = \overline{\text{SOP}}. \quad (14)$$

Remark 1: Note that $\overline{\text{SOP}}$ in (14) is tight when N is large, because $\gamma_{D_1} \gg \gamma_{D_2}$ holds with high probability, whose proof is provided in Appendix C.

Lemma 3: The upper bound in (14) can be expressed as

$$\overline{\text{SOP}} = 1 - \frac{1}{2}(I_1 + I_2), \quad (15)$$

where I_1 and I_2 are respectively defined as follows

$$\begin{aligned} I_1 &= \text{erfc}\left(\frac{\sqrt{\varphi-1}+\alpha}{\beta}\right) - \frac{2\sqrt{A}}{\beta} e^{AB^2 + \frac{(\varphi-1)\epsilon}{\varphi} \frac{\alpha^2}{\beta^2}} \\ &\quad \times \left[1 - \text{erf}\left(B\sqrt{A} + \frac{\sqrt{\varphi-1}}{2\sqrt{A}}\right)\right], \end{aligned} \quad (16)$$

$$\begin{aligned} I_2 &= \text{erfc}\left(\frac{\sqrt{\varphi-1}-\alpha}{\beta}\right) - \frac{2\sqrt{A}}{\beta} e^{AB^2 + \frac{(\varphi-1)\epsilon}{\varphi} \frac{\alpha^2}{\beta^2}} \\ &\quad \times \left[1 - \text{erf}\left(-B\sqrt{A} + \frac{\sqrt{\varphi-1}}{2\sqrt{A}}\right)\right], \end{aligned} \quad (17)$$

where $A = \frac{\beta^2 \varphi}{4(\beta^2 \epsilon + \varphi)}$ and $B = \frac{2\alpha}{\beta^2}$.

Proof: See Appendix D. ■

B. Asymptotic SOP Analysis

We consider application scenarios characterized by a low transmission rate but high security requirements, such as for the Internet of Things [23]. The target SR C_{th} can be so small that $\varphi \rightarrow 1$. In this case, we obtain

$$\begin{aligned} \overline{\text{SOP}} &\xrightarrow{(f)} \sqrt{\frac{1}{2\sigma_1^2 \tilde{\gamma}_{\text{SRD}} \epsilon + 1}} e^{-\frac{m_1^2 \tilde{\gamma}_{\text{SRD}} \epsilon}{2\sigma_1^2 \tilde{\gamma}_{\text{SRD}} \epsilon + 1}} \xrightarrow{(g)} \sqrt{\frac{1}{2\sigma_1^2 \tilde{\gamma}_{\text{SRD}} \epsilon}} e^{-\frac{m_1^2}{2\sigma_1^2}} \\ &= \sqrt{\frac{1}{k[1 + \text{sinc}(2x) - \frac{\pi^2}{8} \text{sinc}^2(x)]}} e^{-\frac{1}{\frac{16[1 + \text{sinc}(2x)]}{\pi^2 \text{sinc}^2(x)} - 2} N}, \end{aligned} \quad (18)$$

where (f) is obtained from (15) by setting $\varphi \rightarrow 1$, and (g) holds true in the high-SNR regime when $\bar{\gamma}_{SRD} \gg \{\bar{\gamma}_{SRE}, \bar{\gamma}_{SE}\}$ and by using the following inequalities

$$\begin{aligned} 2\sigma_1^2 \bar{\gamma}_{SRD} \epsilon &= \frac{1 + \text{sinc}(2x) - \frac{\pi^2}{8} \text{sinc}^2(x)}{\bar{\gamma}_{SRE} + \bar{\gamma}_{SE}/N} \bar{\gamma}_{SRD} \\ &\geq \frac{\bar{\gamma}_{SRD}}{2(\bar{\gamma}_{SRE} + \bar{\gamma}_{SE})} \gg 1, \end{aligned} \quad (19)$$

where $x \triangleq 2^{-b}$ and the inequality in (19) follows by $1 + \text{sinc}(2x) - \frac{\pi^2}{8} \text{sinc}^2(x) \geq \frac{1}{2}$ for $x \in (0, \frac{1}{2}]$. The last equality in (18) is obtained by defining $k \triangleq \bar{\gamma}_{SRD} / (\bar{\gamma}_{SRE} + \frac{1}{N} \bar{\gamma}_{SE})$.

By direct inspection of (18), we evince that $\overline{SOP}$ decreases if $\bar{\gamma}_{SRD}$ increases, which means that enhancing the average SNR at the legitimate user always improves the secrecy performance even for a limited number of discrete phase shift status. In particular, we have $\overline{SOP} \rightarrow 0$ when $\bar{\gamma}_{SRD} \rightarrow \infty$ while keeping N , b , $\bar{\gamma}_{SRE}$, and $\bar{\gamma}_{SE}$ fixed.

Besides, inspired by [24], we have the following remark to show the impact of the RIS location on SOP.

Remark 2: The SOP improves when $\{d_{SR}, d_{RD}\}$ decreases and d_{RE} increases. For large N , it is further found that the asymptotic SOP hardly changes with a moderate variation of d_{SR} . This behavior is also explained from the fact that reducing the distance from the source to RIS increases the received SNRs for both the legitimate user and the eavesdropper. Therefore, in the case that the location of the eavesdropper is unknown, we should prioritize deploying the RIS closer to the legitimate user than to the source.

Proof: From (18), we see that the location of the RIS is only reflected in the parameter $k = \frac{d_{RD}^{-v}}{d_{RE}^{-v} + \frac{1}{N} \left(\frac{d_{SE}}{d_{SR}}\right)^{-v}}$, and the asymptotic SOP in (18) decreases as k grows. ■

Moreover, the high-SNR expression in (18) is also useful for understanding the asymptotic secrecy performance given the number of control bits of discrete phase shifts. Some relevant case studies are reported as follows.

Case 1: Under the assumption of continuous-valued phase shifts, i.e., $b = +\infty$, the SOP in (18) reduces to

$$\overline{SOP} \Big|_{b=+\infty} \rightarrow \sqrt{\frac{8}{k(16 - \pi^2)}} e^{-\frac{\pi^2}{32 - 2\pi^2} N}. \quad (20)$$

Case 2: Under the assumption of 1-bit binary phase shifts, i.e., $b = 1$, the SOP in (18) reduces to

$$\overline{SOP} \Big|_{b=1} \rightarrow \sqrt{\frac{2}{k}} e^{-\frac{N}{2}}. \quad (21)$$

Case 3: Under the assumption of $b \geq 3$, we prove in Appendix E that the quantization noise, which is due to the use of discrete phase shifts, is one order-of-magnitude smaller than the SOP of the continuous phase shifts disclosed in Case 1.

Remark 3: According to Case 1 and Case 2, the SOP tends to $\overline{SOP}|_{b=+\infty} \rightarrow \sqrt{8\bar{\gamma}_{SRE}/[(16 - \pi^2)\bar{\gamma}_{SRD}]} e^{-0.8N}$ and $\overline{SOP}|_{b=1} \rightarrow \sqrt{2\bar{\gamma}_{SRE}/\bar{\gamma}_{SRD}} e^{-0.5N}$ for sufficiently large N . We see that the SOP loss due to the 1-bit quantization, compared to the ideal continuous-valued phase shifts, can be asymptotically compensated by increasing the number of RIS elements by about 1.6 times.

Proof: Let N_1 and N_2 denote the numbers of RIS elements corresponding to $b = +\infty$ and $b = 1$, respectively. By solving $\overline{SOP}|_{b=1} \leq \overline{SOP}|_{b=+\infty}$, it follows that $N_2 \geq \frac{\pi^2}{16 - \pi^2} N_1 - \ln \frac{4}{16 - \pi^2} \approx 1.6N_1$. This completes the proof. ■

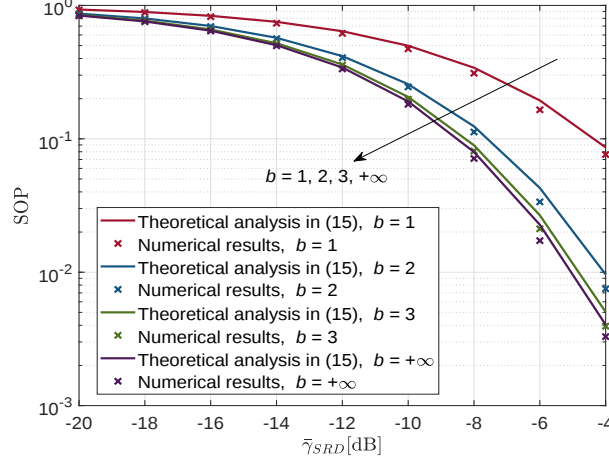


Fig. 2. SOP versus $\bar{\gamma}_{SRD}$ for different values of b .

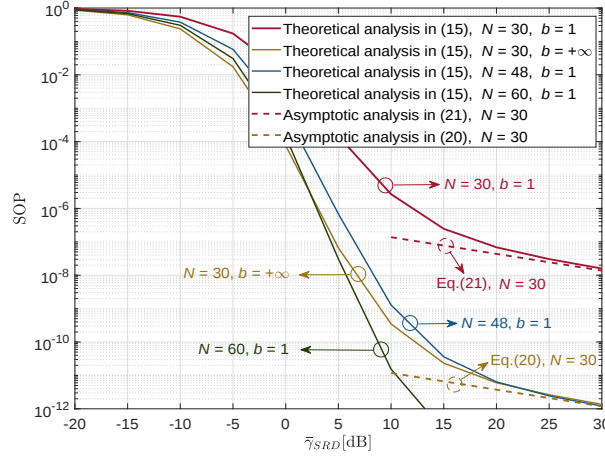


Fig. 3. SOP versus $\bar{\gamma}_{SRD}$ for different values of N .

V. NUMERICAL RESULTS

In this section, Monte-Carlo simulations are illustrated to validate our analysis. The tested parameters are set to $\bar{\gamma}_{SE} = -5$ dB and $\bar{\gamma}_{SRE} = 0$ dB.

Fig. 2 shows the impact of b on the SOP when $N = 30$ and $C_{th} = 0.05$. We observe that the analytical results in (15) match well with the numerical curves. Monte-Carlo simulations are illustrated for values of the SOP no smaller than 10^{-3} due to the limited number of channel realizations simulated. As stated in Case 3, the gap between $b = 3$ and $b = +\infty$ in Fig. 2 does appear negligible for high SNRs.

In Fig. 3, we consider a larger $C_{th} = 0.2$ to verify the effectiveness of the asymptotic analysis. We plot the SOP for $N = 30$ by setting $b = 1$ and $b = +\infty$. As expected, the asymptotic expressions in (20) and (21) are quite tight in the high-SNR regime. Then, we plot the SOP for $b = 1$ by setting $N = 48$ (i.e., which is equal to 1.6×30) and $N = 60$ (2×30). We see that the setup $N = 48$ with $b = 1$ provides, in the high-SNR regime, the same SOP as

the setup $N = 30$ with $b = +\infty$, which validates the obtained guideline in *Remark 3*.

VI. CONCLUSION

This paper studied the SOP of an RIS-assisted communication system with discrete phase shifts. The main contribution is to unveil the achievable scaling law of SOP with respect to N and b . Specifically, the increased number of RIS elements was quantified to compensate the performance loss caused by binary phase shifts.

APPENDIX A

PROOF OF THE INDEPENDENCE OF γ_{D_1} AND γ_{D_2}

By taking into account that the distribution of Θ_i is symmetric around its mean value, which is equal to zero, we have $\mathbb{E}[XY] = 0$ [25]. Then, the covariance of X and Y is

$$\text{Cov}[X, Y] = \mathbb{E}[XY] - \mathbb{E}[X] \mathbb{E}[Y] = \mathbb{E}[XY] = 0, \quad (22)$$

which indicates that X and Y are uncorrelated RVs.

For large values of N , $\sum_{i=1}^N |h_i| |g_i| e^{j\Theta_i}$ is approximately a complex Gaussian RV by virtue of the CLT, and its real part X and imaginary part Y are jointly Gaussian RVs. Since two uncorrelated Gaussian RVs are independent as well, it follows that γ_{D_1} and γ_{D_2} are independent.

APPENDIX B

PROOF OF LEMMA 2

First, we note that h_i and ϕ_i^{sub} are dependent RVs since ϕ_i^{sub} and $\phi_i^{\text{opt}} = -\angle(h_i g_i)$ are correlated RVs. Since $\phi_i^{\text{sub}} = \Theta_i + \phi_i^{\text{opt}}$, the RV Z can be rewritten as

$$Z = \sqrt{\gamma_{SRE}} \sum_{i=1}^N |h_i| |p_i| e^{j(\angle p_i - \angle g_i + \Theta_i)} + \sqrt{\gamma_{SE}} h_{SE}, \quad (23)$$

where $\angle p_i$ and $\angle g_i$ are uniformly distributed in $[0, 2\pi)$. The RV Θ_i depends on the phase error at the RIS, and $\angle p_i$ and $\angle g_i$ depend on the positions of the eavesdropper and the legitimate user, respectively. Since the RV $p_i = |p_i| e^{j\angle p_i}$ is independent of the three RVs $|h_i|$, $\angle g_i$, and Θ_i and has zero mean, we obtain $\mathbb{E}[|h_i| |p_i| e^{j(\angle p_i - \angle g_i + \Theta_i)}] = 0$, and $\text{Var}[|h_i| |p_i| e^{j(\angle p_i - \angle g_i + \Theta_i)}] = 1$. For large values of N , $\sum_{i=1}^N |h_i| |p_i| e^{j(\angle p_i - \angle g_i + \Theta_i)} \xrightarrow{d} \mathcal{CN}(0, N)$ by virtue of the CLT, and then $Z \xrightarrow{d} \mathcal{CN}(0, N\gamma_{SRE} + \gamma_{SE})$.

Since p_i is a circularly-symmetric Gaussian RV, we have $\Pr(e^{j\angle p_i}) = \Pr(e^{j\angle p_i} e^{j(-\angle g_i + \Theta_i)})$. Thus, $|p_i| e^{j(\angle p_i - \angle g_i + \Theta_i)}$ is a zero-mean circularly-symmetric complex Gaussian RV as well. This implies that the real and imaginary parts of Z are uncorrelated and hence independent since they are Gaussian distributed. Also, they have zero means and the same variance.

APPENDIX C

PROOF OF REMARK 1

Since the RV $\gamma_{D_2}/\gamma_{D_1}$ is nonnegative, we obtain

$$\Pr\left(\frac{\gamma_{D_2}}{\gamma_{D_1}} < 0.1\right) \stackrel{(h)}{\geq} 1 - \frac{\mathbb{E}\left[\frac{\gamma_{D_2}}{\gamma_{D_1}}\right]}{0.1} \stackrel{(i)}{=} 1 - \frac{\mathbb{E}[\gamma_{D_2}]}{0.1\mathbb{E}[\gamma_{D_1}]}, \quad (24)$$

where (h) is obtained by applying the Markov inequality [19], and (i) comes from the fact that γ_{D_1} and γ_{D_2} are independent.

Furthermore, $\frac{\mathbb{E}[\gamma_{D_2}]}{\mathbb{E}[\gamma_{D_1}]}$ is calculated as

$$\frac{\mathbb{E}[\gamma_{D_2}]}{\mathbb{E}[\gamma_{D_1}]} = \frac{\sigma_2^2}{m_1^2 + \sigma_1^2} = \frac{8[1 - \text{sinc}(2x)]}{(N-1)\pi^2 \text{sinc}^2(x) + 8[1 + \text{sinc}(2x)]}, \quad (25)$$

where $x = 2^{-b} \in (0, \frac{1}{2}]$ and it is easy to check that $\frac{\mathbb{E}[\gamma_{D_2}]}{\mathbb{E}[\gamma_{D_1}]}$ is increasing as x grows by calculating its first order derivative. It follows

$$\frac{\mathbb{E}[\gamma_{D_2}]}{\mathbb{E}[\gamma_{D_1}]} \leq \frac{\mathbb{E}[\gamma_{D_2}]}{\mathbb{E}[\gamma_{D_1}]} \Big|_{x=\frac{1}{2}} = \frac{2}{N+1}. \quad (26)$$

Therefore, (24) is further expressed as

$$\Pr\left(\frac{\gamma_{D_2}}{\gamma_{D_1}} < 0.1\right) \geq 1 - \frac{\mathbb{E}[\gamma_{D_2}]}{0.1\mathbb{E}[\gamma_{D_1}]} = 1 - \frac{20}{N+1}. \quad (27)$$

When N is large, we finally obtain $\Pr\left(\frac{\gamma_{D_2}}{\gamma_{D_1}} < 0.1\right) \rightarrow 1$, which means that $\gamma_{D_1} \gg \gamma_{D_2}$ holds with high probability.

APPENDIX D

PROOF OF LEMMA 3

By inserting (8) and (12) in (14), the upper bound of the SOP can be rewritten as

$$\begin{aligned} \overline{SOP} &= \int_0^\infty \left[1 - \frac{1}{2} \text{erfc} \left(\frac{\alpha + \sqrt{(1+x)\varphi - 1}}{\beta} \right) \right. \\ &\quad \left. - \frac{1}{2} \text{erfc} \left(\frac{\sqrt{(1+x)\varphi - 1} - \alpha}{\beta} \right) \right] \epsilon e^{-\epsilon x} dx \\ &= 1 - \frac{1}{2} \left(\int_0^\infty \text{erfc} \left(\frac{\alpha + \sqrt{(1+x)\varphi - 1}}{\beta} \right) \epsilon e^{-\epsilon x} dx \right. \\ &\quad \left. + \int_0^\infty \text{erfc} \left(\frac{\sqrt{(1+x)\varphi - 1} - \alpha}{\beta} \right) \epsilon e^{-\epsilon x} dx \right) \\ &= 1 - \frac{1}{2} (I_1 + I_2). \end{aligned} \quad (28)$$

The integral I_1 is calculated by using the integration by parts method. We have

$$\begin{aligned}
I_1 &= \int_0^\infty \operatorname{erfc} \left(\frac{\sqrt{(1+x)\varphi-1} + \alpha}{\beta} \right) \epsilon e^{-\epsilon x} dx \\
&= -\operatorname{erfc} \left(\frac{\sqrt{(1+x)\varphi-1} + \alpha}{\beta} \right) e^{-\epsilon x} \Big|_{x=0}^\infty \\
&\quad + \int_0^\infty e^{-\epsilon x} d \left(\operatorname{erfc} \left(\frac{\sqrt{(1+x)\varphi-1} + \alpha}{\beta} \right) \right) \\
&= \operatorname{erfc} \left(\frac{\sqrt{\varphi-1} + \alpha}{\beta} \right) - \frac{1}{\sqrt{\pi}\beta} J_1,
\end{aligned} \tag{29}$$

where J_1 is expressed as

$$\begin{aligned}
J_1 &= \int_0^\infty \varphi e^{-\epsilon x} \frac{e^{-\left(\sqrt{(1+x)\varphi-1} + \alpha\right)^2/\beta^2}}{\sqrt{(1+x)\varphi-1}} dx \\
&= 2e^{\frac{(\varphi-1)\epsilon}{\varphi} - \frac{\alpha^2}{\beta^2}} \int_{\sqrt{\varphi-1}}^\infty e^{-\left(\frac{1}{\beta^2} + \frac{\epsilon}{\varphi}\right)t^2 - \frac{2\alpha}{\beta^2}t} dt \\
&= 2e^{\frac{(\varphi-1)\epsilon}{\varphi} - \frac{\alpha^2}{\beta^2}} \sqrt{\pi A} e^{AB^2} \left[1 - \operatorname{erf} \left(B\sqrt{A} + \frac{\sqrt{\varphi-1}}{2\sqrt{A}} \right) \right],
\end{aligned} \tag{30}$$

$t = \sqrt{(1+x)\varphi-1}$, and the last equality is obtained by using [18, Eq. (3.322)], where $A = \frac{\beta^2\varphi}{4(\beta^2\epsilon+\varphi)}$ and $B = \frac{2\alpha}{\beta^2}$. Further, by substituting (30) into (29), I_1 is obtained as shown in (16). Analogously, I_2 is calculated by replacing α in (16) with $-\alpha$, which yields the desired result in (17).

APPENDIX E

PROOF OF CASE 3

We apply the Taylor expansion to the SOP in (18). More precisely, around $x = 0$ and for small values of $x = 2^{-b} < 1$, we have

$$\sqrt{\frac{1}{k[1 + \operatorname{sinc}(2x) - \frac{\pi^2}{8} \operatorname{sinc}^2(x)]}} = c_1 + c_2 x^2 + O(x^4), \tag{31}$$

$$e^{-\frac{1}{\frac{16[1 + \operatorname{sinc}(2x)]}{\pi^2 \operatorname{sinc}(x)} - 2} N} = e^{-c_3 N} + O(x^4), \tag{32}$$

where $c_1 = \sqrt{\frac{8}{k(16-\pi^2)}}$, $c_2 = \frac{\pi^2}{6}c_1$, and $c_3 = \frac{\pi^2}{32-2\pi^2}$.

By substituting (31) and (32) in (18), the SOP is further rewritten as

$$\begin{aligned}
\overline{SOP} &\rightarrow (c_1 + c_2 x^2 + O(x^4)) (e^{-c_3 N} + O(x^4)) \\
&= c_1 e^{-c_3 N} + c_2 e^{-c_3 N} x^2 + O(x^4).
\end{aligned} \tag{33}$$

Since the first term in (33) is the SOP for $b = +\infty$ as given in Case 1, the performance loss due to finite values of b is dominated by the second term in (33), i.e., $c_2 e^{-c_3 N} x^2$. If we restrict that the performance loss is one order of magnitude smaller than Case 1 for $b = +\infty$, it gives $(c_2 e^{-c_3 N} x^2) / (c_1 e^{-c_3 N}) < 1/10$, which implies $x < \sqrt{3/(5\pi^2)}$ and equivalently $b \geq 3$.

REFERENCES

- [1] 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, Aug. 2019.
- [2] M. Di Renzo *et al.*, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2450–2525, Nov. 2020.
- [3] S. Liu, Z. Gao, J. Zhang, M. Di Renzo, and M.-S. Alouini, "Deep denoising neural network assisted compressive channel estimation for mmWave intelligent reflecting surfaces," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9223–9228, Aug. 2020.
- [4] Z. Wan, Z. Gao, F. Gao, M. Di 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.
- [5] W. Shi, W. Xu, X. You, C. Zhao, and K. Wei, "Intelligent reflection enabling technologies for integrated and green Internet-of-Everything beyond 5G: Communication, sensing, and security," *IEEE Wireless Commun.*, early access. doi: 10.1109/MWC.018.2100717.
- [6] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1488–1492, Sept. 2019.
- [7] L. Dong, H.-M. Wang, J. Bai, and H. Xiao, "Double intelligent reflecting surface for secure transmission with inter-surface signal reflection," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2912–2916, Mar. 2021.
- [8] G. Zhou, C. Pan, H. Ren, K. Wang, and Z. Peng, "Secure wireless communication in RIS-aided MISO system with hardware impairments," *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1309–1313, Jun. 2021.
- [9] L. Lv, Q. Wu, Z. Li, N. Al-Dhahir, and J. Chen, "Secure two-way communications via intelligent reflecting surfaces," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 744–748, Mar. 2021.
- [10] J. Luo, F. Wang, S. Wang, H. Wang, and D. Wang, "Reconfigurable intelligent surface: Reflection design against passive eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 3350–3364, May 2021.
- [11] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. Di Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12296–12300, Oct. 2020.
- [12] W. Wang, H. Tian, and W. Ni, "Secrecy performance analysis of IRS-aided UAV relay system," *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2693–2697, Dec. 2021.
- [13] M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, "Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1443–1447, May 2021.
- [14] 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.
- [15] A. Papazafeiropoulos, C. Pan, P. Kourtessis, S. Chatzinotas, and J. M. Senior, "Intelligent reflecting surface-assisted MU-MISO systems with imperfect hardware: Channel estimation and beamforming design," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 2077–2092, Mar. 2022.
- [16] H. Zhang, B. Di, L. Song, and Z. Han, "Reconfigurable intelligent surfaces assisted communications with limited phase shifts: How many phase shifts are enough?," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4498–4502, Apr. 2020.
- [17] P. Xu, G. Chen, Z. Yang, and M. Di Renzo, "Reconfigurable intelligent surfaces-assisted communications with discrete phase shifts: How many quantization levels are required to achieve full diversity?," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 358–362, Feb. 2021.
- [18] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.
- [19] H. Pishro-Nik, *Introduction to Probability, Statistics and Random Processes*, Gaithersburg, MD, USA: Kappa Research, 2014.
- [20] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed., New York, NY, USA: McGraw-Hill, 2008.
- [21] V. M. Kapinas, S. K. Mihos, and G. K. Karagiannidis, "On the monotonicity of the generalized Marcum and Nuttall Q-functions," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3701–3710, Aug. 2009.
- [22] M. ElKashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.
- [23] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.
- [24] S. Zeng, H. Zhang, B. Di, Z. Han, and L. Song, "Reconfigurable intelligent surface (RIS) assisted wireless coverage extension: RIS orientation and location optimization," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 269–273, Jan. 2021.

- [25] I. Trigui, W. Ajib, W.-P. Zhu, and M. Di Renzo, "Performance evaluation and diversity analysis of RIS-assisted communications over generalized fading channels in the presence of phase noise," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 593–607, 2022.