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

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

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, $b$. 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 the SOP loss when binary phase shifts, i.e., $b = 1$, are utilized. It is found that increasing the number of RIS elements by 1.6 times provides the same SOP as that of an RIS with continuous-valued 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

A 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 nearly 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].

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 nearly passive BF. In order to maximize the theoretical secrecy, the authors of [6], [7], [8] investigated the joint optimization of the active and nearly passive BF 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 the SR, the 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 SOP of RIS-aided communication systems has been investigated in [11], [12], [13]. Both analytical and asymptotic analyses have been provided to reveal the impact of key system parameters on the SOP. In particular, the authors of [12] considered the SOP of an RIS-aided unmanned aerial vehicle (UAV) relay system. In [13], the authors analyzed the SOP and the probability of non-zero secrecy capacity of an RIS-aided device-to-device (D2D) communication system. However, most studies on the SOP considered RISs with continuous phase shifts, which entails a high implementation complexity. Even though discrete phase shifts have been considered in the context of RIS-aided communications, 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 assuming discrete phase shifts results in analytical expressions of the cascaded RIS channel that are 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 impact of assuming discrete phase shifts in a closed-form expression. 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 the SOP is characterized in the high-SNR regime. In particular, it is shown that the SOP decreases with slope $e^{-0.8N}$ 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 case of continuous phase control, we obtain that the SOP loss caused by using binary phase shifts, i.e., $b = 1$, can be compensated by deploying a larger RIS with size 1.6$N$.

The rest 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 Sections V and VI, respectively.

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

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. Nodes $S$, $D$, and $E$ are equipped with a single antenna for transmission and reception and all links experience Rayleigh fading. The channel coefficients of the S-RIS, RIS-D, RIS-E, and $S$-$E$ links are denoted by $h_1$, $g_1$, $p_1$, respectively, and $h_{SE} \sim CN(0, 1)$, where $CN$ is the complex Gaussian distribution. Since many channel estimation methods are available in the literature [3], [4] and the references therein, we assume that the channel coefficients of $h_1$ and $g_1$ are perfectly known to $S$. However, the channel gains of $p_1$ 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

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

(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 $n_D \sim CN(0, N_0)$ 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., $E[|x|^2] = 1$, where $E[.]$ 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 $\nu$ is the path loss exponent.

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

\[ \gamma_D = \frac{\eta^2 P \left| \sum_{i=1}^{N} h_i g_i e^{j\phi_i} \right|^2}{N_0 d_{SR}^2 d_{RD}^2}. \]  

(2)

In the case of continuous phase shifts, $\gamma_D$ 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 a complex number. This optimized phase compensates the phase shift introduced by the 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 $A = \{ 0, \frac{\pi}{\nu}, \ldots, \frac{(2^{m_b}) \pi}{\nu} \}$, where $m_b$ is the number of quantization bits. In this case, usually, the phase shift of the $i$th RIS element, $\phi_i^{\text{sub}} \in A$, is chosen as

\[ \phi_i^{\text{sub}} \triangleq \arg \min_{\phi_i \in A} | \phi_i - \phi_i^{\text{opt}} |. \]  

(3)

\(^1\)The direct link between $S$ and $E$ exists when the eavesdropper is not blocked by obstacles [11], [13].

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

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

\[ \gamma_D = \xi_{\text{SRD}} \sum_{i=1}^{N} h_i g_i e^{j\phi_i^{\text{sub}}} \left| x + n_D \right|^2, \]  

(4)

where $\xi_{\text{SRD}} \triangleq \frac{\eta^2 P}{N_0 d_{SR}^2 d_{RD}^2}$ denotes the average SNR.

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

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

(5)

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

\[ \gamma_E = \left( \frac{\xi_{\text{SRD}}}{\sqrt{\xi_{\text{SRD}}} + \eta \xi_{\text{SSE}}} \right)^2 \]  

(6)

where $\xi_{\text{SSE}} \triangleq \frac{\eta^2 P}{N_0 d_{SR}^2 d_{RD}^2}$ and $\xi_{\text{SSE}} \triangleq \frac{\eta^2 P}{N_0 d_{SR}^2 d_{RD}^2}$ 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 $\gamma_D$ and $\gamma_E$.

A. Distribution of $\gamma_D$

Let us denote the quantization error of the phase shifts by $\Theta_1 = \phi_i^{\text{sub}} - \phi_i^{\text{opt}}$, which is uniformly distributed $[14], [15], [17]$, i.e., $\Theta_1 \sim U(-2^{\nu/2} \pi, 2^{\nu/2} \pi)$. Then, $\gamma_D$ in (4) is rewritten as

\[ \gamma_D = \xi_{\text{SRD}} \sum_{i=1}^{N} h_i g_i e^{j(\Theta_1 + \phi_i^{\text{opt}})} \left| x + n_D \right|^2, \]  

(7)

where (a) follows by using the identity $\phi_i^{\text{sub}} = \Theta_1 + \phi_i^{\text{opt}}$, (b) is obtained by using $\phi_i^{\text{opt}} = -\angle(h_i g_i)$, (c) follows by the definitions $X = \sum_{i=1}^{N} |h_i| |g_i| \cos \Theta_1$ and $Y = \sum_{i=1}^{N} |h_i| |g_i| \sin \Theta_1$, and (d) is obtained by defining $\gamma_D = \xi_{\text{SRD}} X^2$ and $\gamma_D = \xi_{\text{SRD}} Y^2$. Before deriving the distribution of $\gamma_D$, we introduce the following lemma.

Lemma 1: If $N$ is large, $\gamma_D$, and $\gamma_D$, are statistically independent. Also, the cumulative distribution function (CDF) of $\gamma_D$, and the probability density function (PDF) of $\gamma_D$, are respectively,

\[ F_{\gamma_D}(x) = 1 - \frac{1}{2} \text{erfc} \left( \frac{x + \sqrt{x}}{\beta} \right), \]  

(8)

\[ f_{\gamma_D}(y) = \lambda^\nu e^{-\lambda} \left( \frac{y - 1}{\mu} \right)^{\nu/2 - 1} \Gamma \left( \frac{\nu}{2} \right), \]  

(9)

where $\alpha = m_1 \sqrt{\xi_{\text{SRD}}}$, $\beta = \sqrt{2} \pi \sqrt{\xi_{\text{SRD}}}$, $m_1 = \frac{N_0}{\xi_{\text{SRD}}} \sin(2 \beta)$, $\sigma_1^2 = \frac{\pi}{4} \left[ 1 + \sin^2(2 \beta) \right] - \frac{N_0}{\xi_{\text{SRD}}} \sin^2(2 \beta)$, $\lambda = \frac{1}{\xi_{\text{SRD}}}$, and $\Gamma(\cdot)$ is the Gamma function [18, Eq. (8.310)].

Proof: The proof of the independence of $\gamma_D$, and $\gamma_D$, 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 $|h_l|$ and $|g_l|$ 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 $\text{Var}[Y] = \sigma_2^2$.

Then, it follows

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

(10)

where $\overset{d}{\sim}$ denotes the convergence in distribution by virtue of the CLT. $\gamma_{D_1}$ is a non-central $\chi^2$ RV and $\gamma_{D_2}$ is a central $\chi^2$ RV with one degree of freedom, where $\chi^2$ 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 $f_{\gamma_{D_1}}(\cdot)$ is obtained from [20, Eq. (2.3-28)]. The proof is then complete.

By applying Lemma 1 and (7), the CDF of $\gamma_D$ is equal to

$$F_{\gamma_D}(z) = \int_0^z f_{\gamma_{D_1}}(y) d\gamma_{D_1}(y)$$

(11)

where $D \overset{d}{\sim} \{(x, y) : x + y \leq z, x > 0, y > 0\}$, (d) follows from the independence of $\gamma_{D_1}$ and $\gamma_{D_2}$ in Lemma 1, and (e) is obtained by using (8) and (9).

B. Distribution of $\gamma_E$

Let us first consider the distribution of $Z \overset{d}{\sim} \mathcal{N}(\sum_{l=1}^N h_l e^{j\phi_l} + \mathcal{N}(0, \gamma_{SE}), \gamma_{SE})$. Then, $\gamma_E$ in (6) can be calculated according to the relation $\gamma_E = |Z|^2$. The distribution of $Z$ is provided in the following lemma.

Lemma 2: For large $N$, $Z \overset{d}{\sim} \mathcal{N}(0, \gamma_{SE} + \gamma_{SE})$, and the real and imaginary parts of $Z$ are independent RVs with equal variance.

Proof: See Appendix B.

As disclosed in Lemma 2, $\gamma_E$ has an exponential distribution with mean $N \gamma_{SE} + \gamma_{SE}$. Therefore, the PDF of $\gamma_E$ is

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

(12)

where $\epsilon = 1/(N \gamma_{SE} + \gamma_{SE})$.

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], [12], [13], [22], the SOP is defined as

$$\text{SOP} = \Pr\left(\ln(1 + \gamma_D) - \ln(1 + \gamma_E) < C_{th}\right) = \int_0^\infty F_{\gamma_D}(1 + x) \varphi - 1 f_{\gamma_E}(x) dx,$$

(13)

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

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

(14)

Remark 1: The SOP in (14) is tight when $N$ is large, because $\gamma_{D_1} \sim \gamma_{D_2}$ holds with high probability. The proof is provided in Appendix C.

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

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

(15)

where $I_1$ and $I_2$ are, respectively, defined as follows

$$I_1 = \frac{\text{erfc}\left(\frac{\sqrt{\varphi - 1} + \alpha}{\beta}\right)}{\text{erfc}\left(\frac{\sqrt{\varphi - 1} - \alpha}{\beta}\right)} \times \left[1 - \text{erfc}\left(\frac{B\sqrt{\varphi + 1}}{\sqrt{\varphi - 1}}\right)\right],$$

(16)

$$I_2 = \left[1 - \text{erfc}\left(-B\sqrt{\varphi + 1}/\sqrt{\varphi - 1}\right)\right],$$

(17)

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

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 application to the Internet of Things [23]. The target SR $C_{th}$ can be so small that $\varphi \to 1$. In this case, we obtain

$$\text{SOP} \overset{f}{\sim} \sqrt{\frac{1}{2\sigma_1^2 \gamma_{SRD}^2 + 1}} e^{-\frac{m_1^2 \gamma_{SRD} + \gamma_{SE}}{2\sigma_1^2 \gamma_{SRD}^2 + 1}} \frac{1}{k + \text{sinc}(2x) - \frac{2^6}{\pi^2} \text{sinc}^2(x)} e\left(-\frac{m_1^2 \gamma_{SRD}}{2\sigma_1^2 \gamma_{SRD}^2 + 1}\right),$$

(18)

where $f$ is obtained from (15) by setting $\varphi \to 1$, and (g) holds true in the high-SNR regime when $\gamma_{SRD} \gg \{\gamma_{SE}, \gamma_{SRD}^2\}$ and by using the following inequalities

$$2\sigma_1^2 \gamma_{SRD} = 1 + \text{sinc}(2x) - \frac{2^6}{\pi^2} \text{sinc}^2(x) / \gamma_{SRD} \geq \frac{\gamma_{SRD}}{2(\gamma_{SRD}^2 + \gamma_{SE})} \geq 1,$$

(19)

where $x \approx 2^{-b}$ and the inequality in (19) follows because $1 + \text{sinc}(2x) - \frac{2^6}{\pi^2} \text{sinc}^2(x) \geq \frac{1}{4}$ for $x \in (0, \frac{1}{4})$. The last equality in (18) is obtained by defining $k \equiv \gamma_{SRD} / (\gamma_{SRD}^2 + \frac{1}{4}\gamma_{SE})$.

By direct inspection of (18), we evince that SOP decreases if $\gamma_{SRD}$ increases, which implies that enhancing the average SNR at the legitimate user always improves the secrecy performance even for a limited number of discrete phase shifts. In particular, we have $\text{SOP} \to 0$ when $\gamma_{SRD} \to \infty$ while keeping $N, b$, $\gamma_{SRD}$, and $\gamma_{SE}$ fixed.

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

Remark 2: The SOP improves when $\{d_{SR}, d_{RD}\}$ decreases and $d_{SE}$ increases. For large values of $N$, the asymptotic SOP slightly changes for moderate variations of $d_{SR}$. This behavior is also explained by the fact that, in the considered regime, reducing the distance from the source to the RIS increases the received SNRs for both the legitimate user and the eavesdropper. Therefore, when the location of the eavesdropper is...
unknown, it is convenient to deploy the RIS closer to the legitimate user than to the source.

**Proof:** From (18), we see that the location of the RIS affects only the parameter \( k = \frac{d_{\text{RIS}}}{d_{\text{RIS}} + (\frac{\Delta x}{\Delta y})^2} \), and the asymptotic SOP in (18) decreases as \( k \) increases. For large values of \( N \), in addition, the second addend in the denominator is negligible.

The high-SNR expression in (18) is also useful for understanding the asymptotic secrecy performance as a function of the number of quantization bits of the 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

\[
\text{SOP}
\] 

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

\[
\text{SOP}
\]

**Case 3:** Under the assumption \( b \geq 3 \), 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-valued phase shifts in Case 1.

**Remark 3:** According to Case 1 and Case 2, the SOP tends to \( \text{SOP}_{|b=+\infty} \rightarrow \sqrt{\gamma_{SE}} \/(|16 - \pi|) \) and \( \text{SOP}_{|b=1} \rightarrow \sqrt{\gamma_{SE}} \gamma_{SE}^{0.5N} \) for sufficiently large values of \( N \). 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 \( \text{SOP}_{|b=1} \leq \text{SOP}_{|b=+\infty} \), it follows that \( N_{2} \geq \frac{\pi^{2}}{16 - \pi} N_{1} - \ln \frac{4}{16 - \pi} \approx 1.6N_{1} \). This completes the proof.

V. NUMERICAL RESULTS

In this section, Monte-Carlo simulations are illustrated to validate the obtained analytical results. The simulation parameters are set to \( \gamma_{SE} = -5 \text{ dB} \) and \( \gamma_{SE} = 0 \text{ dB} \).

Fig. 2 shows the impact of \( b \) on the SOP when \( N = 30 \) and \( C_{\text{th}} = 0.05 \). 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 is negligible for high values of the SNR.

In Fig. 3, we consider a larger \( C_{\text{th}} = 0.2 \) to verify the effectiveness of the asymptotic analysis. We plot the SOP for \( N = 30 \) by setting \( b = 1 \) and \( b = +\infty \). We see that 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 \( 1.6 \times 30 \)) and \( N = 60 \) (2 x 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 design guidelines 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 the SOP with respect to \( N \) and \( b \). Specifically, the increase of the number of RIS elements to compensate for the performance loss caused by binary phase shifts was quantified.

**APPENDIX A**

**PROOF OF THE INDEPENDENCE OF \( \gamma_{D_{1}} \) AND \( \gamma_{D_{2}} \)**

By taking into account that the distribution of \( \Theta_{i} \) 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

\[ \text{Cov}[X,Y] = \mathbb{E}[XY] - \mathbb{E}[X] \mathbb{E}[Y] = \mathbb{E}[XY] = 0, \]  

which indicates that \( X \) and \( Y \) are uncorrelated RVs.

For large values of \( N \), the \( \sum_{i=1}^{N} \) 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 \( \gamma_{D_{1}} \) and \( \gamma_{D_{2}} \) are independent.

**APPENDIX B**

**PROOF OF LEMMA 2**

First, we note that \( h_{i} \) and \( \phi^{\text{sub}}_{i} \) are dependent RVs since \( \phi^{\text{sub}}_{i} = -\angle(h_{i}g_{i}) \) are correlated RVs. Since \( \phi^{\text{sub}}_{i} = \Theta_{i} + \phi^{\text{sub}}_{i} \), the RV \( Z \) can be rewritten as

\[ Z = \sqrt{\gamma_{SE}} \sum_{i=1}^{N} |h_{i}| |g_{i}| \phi^{\text{sub}}_{i} + \phi^{\text{sub}}_{i} + \sqrt{\gamma_{SE}} h_{SE}, \]  

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
where $\angle p_i$ and $\angle g_i$ are uniformly distributed in $[0, 2\pi)$. The RV $\Theta_i$ 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 $\Theta_i$ and has zero mean, we obtain $E[|h_i||p_i|e^{j(\angle p_i - \angle g_i + \Theta_i)}] = 0$, and $\text{Var}[|h_i||p_i|e^{j(\angle p_i - \angle g_i + \Theta_i)}] = 1$. For large values of $N$, $\sum_{i=1}^{\infty} |h_i||p_i|e^{j(\angle p_i - \angle g_i + \Theta_i)} \to d\mathcal{CN}(0, N)$ by virtue of the CLT, and then $Z \to d\mathcal{CN}(0, N\gamma_{\text{SBE}} + \gamma_{\text{SR}})$.

Since $p_i$ is a circularly-symmetric Gaussian RV, we have $\Pr(e^{j\angle p_i}) = \Pr(e^{j(\angle p_i - \angle g_i + \Theta_i)})$. 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**

Since the RV $\gamma_{D2}/\gamma_{D1}$ is nonnegative, we obtain

$$\Pr \left( \frac{\gamma_{D2}}{\gamma_{D1}} < 0.1 \right) \geq 1 - \frac{E \left[ \gamma_{D2} \right]}{0.1} = 1 - \frac{E \left[ \gamma_{D1} \right]}{0.1E \left[ \gamma_{D1} \right]},$$

(24)

where (h) is obtained by applying the Markov inequality [19], and (i) comes from the fact that $\gamma_{D1}$ and $\gamma_{D2}$ are independent.

Furthermore, $\frac{E \left[ \gamma_{D2} \right]}{E \left[ \gamma_{D1} \right]}$ is calculated as

$$\frac{E \left[ \gamma_{D2} \right]}{E \left[ \gamma_{D1} \right]} = \frac{\sigma^2}{m_2 + \sigma^2} = \frac{8(1 - \text{sinc}^2(2x))}{(N-1)\pi^2 \text{sinc}^2(x) + 8(1+\text{sinc}(2x))},$$

(25)

where $x = 2^{-b} \in (0, \frac{1}{2}]$ and it can be shown that $\frac{E \left[ \gamma_{D2} \right]}{E \left[ \gamma_{D1} \right]}$ is increasing as $x$ grows by calculating its first-order derivative. Then, if follows

$$\frac{E \left[ \gamma_{D2} \right]}{E \left[ \gamma_{D1} \right]} \leq \frac{E \left[ \gamma_{D2} \right]}{E \left[ \gamma_{D1} \right]}_{x=\frac{1}{2}} = \frac{2}{N + 1},$$

(26)

Therefore, (24) can be further expressed as

$$\Pr \left( \frac{\gamma_{D2}}{\gamma_{D1}} < 0.1 \right) \geq 1 - \frac{E \left[ \gamma_{D2} \right]}{0.1E \left[ \gamma_{D1} \right]} = 1 - \frac{20}{N + 1}.\tag{27}$$

When $N$ is large, we obtain $\Pr(\frac{\gamma_{D2}}{\gamma_{D1}} < 0.1) \to 1$, which implies that $\gamma_{D1} \gg \gamma_{D2}$ 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

$$\text{SOP} = \int_0^\infty \left[ 1 - \frac{1}{2} \text{erfc} \left( \frac{\alpha + \sqrt{(1 + x)} \varphi - 1}{\beta} \right) - \frac{1}{2} \text{erfc} \left( \frac{\sqrt{(1 + x)} \varphi - 1 - \alpha}{\beta} \right) \right] e^{-\epsilon x} dx$$

$$= 1 - \frac{1}{2} \left( \int_0^\infty \text{erfc} \left( \frac{\alpha + \sqrt{(1 + x)} \varphi - 1}{\beta} \right) e^{-\epsilon x} dx \right)$$

$$+ \int_0^\infty \text{erfc} \left( \frac{\sqrt{(1 + x)} \varphi - 1 - \alpha}{\beta} \right) e^{-\epsilon x} dx$$

$$= 1 - \frac{1}{2} \left( I_1 + I_2 \right). \tag{28}$$

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

$$I_1 = \int_0^\infty \text{erfc} \left( \frac{\sqrt{(1 + x)} \varphi - 1 + \alpha}{\beta} \right) e^{-\epsilon x} dx$$

$$= -\epsilon x \left. \text{erfc} \left( \frac{\sqrt{(1 + x)} \varphi - 1 + \alpha}{\beta} \right) \right|_x=0$$

$$+ \int_0^\infty e^{-\epsilon x} d \left( \text{erfc} \left( \frac{\sqrt{(1 + x)} \varphi - 1 + \alpha}{\beta} \right) \right)$$

$$= \epsilon x \left. \text{erfc} \left( \frac{\sqrt{(1 + x)} \varphi - 1 + \alpha}{\beta} \right) \right|_x=0 - \frac{1}{\sqrt{\pi} \beta} J_1,$$

(29)

where $J_1$ is expressed as

$$J_1 = \int_0^\infty \frac{e^{-\epsilon x}}{\sqrt{(1 + x)} \varphi - 1} dx$$

$$= \frac{2e^{-\epsilon x}}{\sqrt{(1 + x)} \varphi - 1} \int_0^\infty e^{-\left( \frac{1}{\pi \beta^2} + \frac{1}{\beta} \right) x^2} dx$$

$$= 2e^{-\epsilon x} \sqrt{\pi \beta} \left[ 1 - \text{erf} \left( B\sqrt{\beta A + \frac{\sqrt{\pi^2 - 1}}{2\sqrt{A}}} \right) \right]. \tag{30}$$

$t = \sqrt{(1 + x)} \varphi - 1$, and the last equality is obtained by using [18, Eq. (3.32)], where $A = \frac{\beta^2}{4(\beta^2 + 1)}$ and $B = \frac{\beta}{\sqrt{2\beta}}$. Further, by substituting (30) into (29), $I_1$ is obtained as shown in (16). Analogously, $I_2$ is calculated by replacing $\alpha$ 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

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

$$\text{e}^{-rac{8\text{sinc}^2(x)}{1 - \text{sinc}^2(x)}} = c_3 + c_4 x^2 + O \left( x^4 \right), \tag{32}$$

where $c_1 = \sqrt{\frac{8 k}{(k-\pi^2)^2}}$, $c_2 = \frac{\pi^2}{6} c_1$, and $c_3 = \frac{\pi^2}{32} - \frac{\pi^2}{2}.\tag{33}$

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

$$\text{SOP} \rightarrow \left( c_1 + c_2 x^2 + O \left( x^4 \right) \right) \left( e^{-c_3 x^2} + O \left( x^4 \right) \right)$$

$$= c_1 e^{-c_3 x^2} + c_2 e^{-c_3 x^2} x^2 + O \left( x^4 \right).$$

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., $c_2 e^{-c_3 x^2} x^2$. If we assume that the performance loss is one order of magnitude smaller than Case 1 for $b = +\infty$, we obtain $(c_2 e^{-c_3 x^2})/(c_1 e^{-c_3 x^2}) < 1/10$, 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, 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. Wang, 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. 4732–4745, 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, May 09, 2022, 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, Sep. 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. Fan, 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] Y. Wang, Z. Gao, M. Di Renzo, and M.-S. Alouini, “On the monotonicity of the generalized Marcum and Nuttall Q-functions,” IEEE Trans. Inf. Theory, vol. 55, no. 8, pp. 3701–3710, Aug. 2009.

[12] 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.

[13] N. Wang, P. Wang, A. Alipour-Fard, 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.

[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. Grahlhteyn and J. 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-Fard, 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.