

Ergodic Secrecy Rate of RIS-Assisted Communication Systems in the Presence of Discrete Phase Shifts and Multiple Eavesdroppers

Peng Xu, *Member, IEEE*, Gaojie Chen, *Senior Member, IEEE*, Gaofeng Pan, *Senior Member, IEEE*, and Marco Di Renzo, *Fellow, IEEE*

Abstract—This letter investigates the ergodic secrecy rate (ESR) of a reconfigurable intelligent surface (RIS)-assisted communication system in the presence of discrete phase shifts and multiple eavesdroppers (Eves). In particular, a closed-form approximation of the ESR is derived for both non-colluding and colluding Eves. The analytical results are shown to be accurate when the number of reflecting elements of the RIS N is large. Asymptotic analysis is provided to investigate the impact of N on the ESR, and it is proved that the ESR scales with $\log_2 N$ for both non-colluding and colluding Eves. Numerical results are provided to verify the analytical results and the obtained scaling laws.

Index Terms—Reconfigurable intelligent surface, discrete phase shifts, multiple eavesdroppers, ergodic secrecy rate.

I. INTRODUCTION

Reconfigurable intelligent surfaces (RISs) utilize a large number of passive reflecting elements to customize wireless communication environments [1]–[4]. Due to the low-cost, high energy-efficiency and full-duplex advantages, RISs are regarded as a promising technology for next-generation wireless communications and hence have recently received significant academic and industrial attention [5]–[8].

RISs have various potential applications in wireless communications, which include the design of secure wireless systems based on the concept of physical layer security (e.g., [9]–[14]). In [9]–[12], the authors investigated optimization problems to jointly design the beamforming vectors and phase shifts at the transmitter and RIS, respectively. In general, there exist two objectives for the design of the phase shifts at the RIS: (i) to strengthen the legitimate channels by co-phasing the reflected signals with the signal directly received from the transmitter; and (ii) to suppress the eavesdropping channels by setting the reflected signals at the eavesdroppers (Eves) to be in opposite

phase with respect to the signal from the transmitter. The key idea behind the optimization problems in existing works [9]–[12] lies in achieving a favorable trade-off between these two design objectives, which requires the knowledge of the instantaneous eavesdropping channel state information (CSI) at the transmitter and RIS. However, the instantaneous eavesdropping CSI is difficult to obtain in practice, since the Eves are usually passive and do not actively communicate with other nodes. Motivated by this consideration, the authors of [13] and [14] considered RIS-assisted secrecy communications without assuming the knowledge of the instantaneous eavesdropping CSI.

Different from these existing works, this letter investigates the ergodic secrecy rate (ESR) of RIS-assisted systems in the presence of discrete phase shifts and multiple Eves. In particular, by approximately characterizing the distribution of the received signal-to-noise-ratios (SNRs) at the Eves, we obtain a closed-form approximation of the ESR for both non-colluding and colluding Eves. The analysis of the ESR, in fact, is essentially different from the analysis of the ergodic rate without security constraints [15], since the phase shifts at the RIS lead to a different impact on the intended receiver and Eves. Moreover, based on passive beamforming, the received SNRs at the destination and Eves depend on phase quantization errors and cascaded channels, that are different from those in massive multiple-input multiple-output (MIMO) systems. In order to provide insights, asymptotic analysis is also provided, which shows that the ESR scales with $\log N$ for both non-colluding and colluding Eves. Numerical results are illustrated to verify that the analytical results are accurate for large values of N .

Notation: \mathbb{C} and \mathbb{Z} denote the complex domain and integer set, respectively; we denote $[1 : M] \triangleq \{1, \dots, M\}$, where M is a positive integer, and $[x]^+ \triangleq \max\{0, x\}$; \mathcal{CN} denotes the complex Gaussian distributions; $\mathbb{E}[\cdot]$ denotes the expectation of a random variable; $\log(\cdot)$ and $\ln(\cdot)$ denote the base-two and natural logarithms, respectively; and κ is Euler's constant.

II. SYSTEM MODEL AND PRELIMINARIES

We consider an RIS-assisted secure communication system with a source (S), an RIS (R) with N reconfigurable elements, a destination (D) and K Eves (E_k , $\forall k \in [1 : K]$). The reconfigurable elements of the RIS are arranged in a uniform array of tiny antennas spaced half of the wavelength apart. All nodes are assumed to be equipped with a single antenna¹.

¹RIS-aided transmission has several applications when multiple antennas are not available at either the transmitter or the receiver, e.g., in device-to-device communications [2].

The work of Peng Xu was supported in part by the Chongqing Natural Science Foundation Project under Grant cstc2019jcyj-msxmX0032, and in part by the National Natural Science Foundation of China under Grants 61701066 and 61971080. The work of Gaojie Chen was supported by EPSRC under Grant EP/R006377/1 (M3NETs). M. Di Renzo's work was supported in part by the European Commission through the H2020 ARIADNE project under grant agreement 675806.

P. Xu is with Chongqing Key Laboratory of Mobile Communications Technology, School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, 400065, China. (e-mail: xupeng@cqupt.edu.cn).

G. Chen is with School of Engineering, University of Leicester, Leicester LE1 7RH, U.K. (e-mail: gaojie.chen@leicester.ac.uk).

G. Pan is with the School of Information and Electronics Engineering, Beijing Institute of Technology, Beijing 100081, China, and he is also with Computer, Electrical and Mathematical Sciences and Engineering Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia. (e-mail: gaofeng.pan.cn@ieee.org).

M. Di Renzo is with Université Paris-Saclay, CNRS and CentraleSupélec, Laboratoire des Signaux et Systèmes, Gif-sur-Yvette, France. (e-mail: marco.direnzo@centralesupelec.fr).

The channels $S \rightarrow D$, $S \rightarrow E_k$, $S \rightarrow R$, $R \rightarrow D$ and $R \rightarrow E_k$ are denoted by $h_{SD} \in \mathbb{C}$, $h_{SE_k} \in \mathbb{C}$, $\mathbf{h}_{SR} \in \mathbb{C}^{N \times 1}$, $\mathbf{h}_{RD} \in \mathbb{C}^{N \times 1}$ and $\mathbf{h}_k \in \mathbb{C}^{N \times 1}$, respectively. These channels are modeled as $h_{SD} = g_{SD}d_{SD}^{-\frac{\alpha}{2}}$, $h_{SE_k} = g_{SE_k}d_{SE_k}^{-\frac{\alpha}{2}}$, $[\mathbf{h}_{SR}]_n = g_{SR,n}d_{SR}^{-\frac{\alpha}{2}}$, $[\mathbf{h}_{RD}]_n = g_{RD,n}d_{RD}^{-\frac{\alpha}{2}}$ and $[\mathbf{h}_k]_n = g_{k,n}d_k^{-\frac{\alpha}{2}}$, where g_{SD} , g_{SE_k} , $g_{SR,n}$, $g_{RD,n}$, $g_{k,n} \sim \mathcal{CN}(0, 1)$ denote the small-scale fading², d_{SD} , d_{SE_k} , d_{SR} , d_{RD} and d_k denote the distances $S \rightarrow D$, $S \rightarrow E_k$, $S \rightarrow R$, $R \rightarrow D$ and $R \rightarrow E_k$, respectively, $\forall n \in [1 : N]$, $k \in [1 : K]$, and α is the pass-loss exponent. Then, the received signal at D and E_k can be written as

$$y_D = \sqrt{P}(\eta \mathbf{h}_{SR}^T \Phi \mathbf{h}_{RD} + h_{SD})x_S + n_D, \quad (1)$$

$$y_{E_k} = \sqrt{P}(\eta \mathbf{h}_{SR}^T \Phi \mathbf{h}_k + h_{SE_k})x_S + n_{E_k}, \quad (2)$$

respectively, where x_S is the transmitted signal, $\mathbb{E}(|x_S|^2) = 1$, P is the transmit power, n_D and $n_{E_k} \sim \mathcal{CN}(0, \delta^2)$ are the additive white Gaussian noises at D and E_k , respectively, $\eta \in (0, 1]$ is the amplitude reflection coefficient, $\Phi \triangleq \text{diag}(e^{j\phi_1}, \dots, e^{j\phi_N})$ and $\phi_n \in [0, 2\pi)$ is the phase shift of the n th element of the RIS.

We assume that the RIS does not have access to the instantaneous eavesdropping CSI, so that it cannot design ϕ_n in order to suppress the received SNRs at the Eves. However, the RIS is assumed to know the instantaneous legitimate CSI. Under these assumptions, the optimal value of ϕ_n that maximizes the received SNR at D is $\phi_n^* = \theta_{SD} - \theta_{SR,n} - \theta_{RD,n}$, where θ_{SD} , $\theta_{SR,n}$ and $\theta_{RD,n}$ denote the phases of g_{SD} , $g_{SR,n}$ and $g_{RD,n}$, respectively. Due to hardware limitations, ϕ_n can only take a finite number of discrete values. In particular, the set of discrete phase shifts is denoted by $\mathcal{F} \triangleq \{0, \frac{2\pi}{2^b}, \dots, \frac{(2^b-1)2\pi}{2^b}\}$, where b denotes the number of quantization bits. Accordingly, we set $\phi_n = f_1(\phi_n^*)$, where the function $f_1(\phi_n^*)$ maps ϕ_n^* to the nearest point in \mathcal{F} , i.e.,

$$f_1(\phi_n^*) = \hat{\phi}_i, \text{ if } |\phi_n^* - \hat{\phi}_i| \leq |\phi_n^* - \hat{\phi}_j|, \hat{\phi}_i, \hat{\phi}_j \in \mathcal{F}, \forall j \neq i. \quad (3)$$

Therefore, the phase quantization error is $\Theta_n = f_1(\phi_n^*) - \phi_n^*$, which is uniformly distributed in $[-\frac{\pi}{2^b}, \frac{\pi}{2^b}]$, similar to [15], [17]. According to (1) and (2), the received SNRs at D and E_k can be formulated, respectively, as follows

$$\begin{aligned} \gamma_D &= \rho \left| h_{SD} + \eta \sum_{n=1}^N [\mathbf{h}_{SR}]_n [\mathbf{h}_{RD}]_n e^{j\Theta_n} \right|^2 \\ &= \rho \left| d_{SD}^{-\frac{\alpha}{2}} |g_{SD}| + \eta d_{SR}^{-\frac{\alpha}{2}} d_{RD}^{-\frac{\alpha}{2}} \sum_{n=1}^N |g_{SR,n} g_{RD,n}| e^{j\Theta_n} \right|^2, \quad (4) \end{aligned}$$

$$\begin{aligned} \gamma_{E_k} &= \rho \left| h_{SE_k} + \eta \sum_{n=1}^N [\mathbf{h}_{SR}]_n [\mathbf{h}_k]_n e^{j\psi_{k,n}} \right|^2 \\ &= \rho \left| d_{SE_k}^{-\frac{\alpha}{2}} |g_{SE_k}| + \eta d_{SR}^{-\frac{\alpha}{2}} d_k^{-\frac{\alpha}{2}} \sum_{n=1}^N |g_{SR,n} g_{k,n}| e^{j\psi_{k,n}} \right|^2, \quad (5) \end{aligned}$$

where $\psi_{k,n} \triangleq f_2(\phi_n^*, \theta_{SR,n}) + \theta_{k,n}$, $\theta_{k,n}$ is the phase of $g_{k,n}$ and the function $f_2(\phi_n^*, \theta_{SR,n})$ is defined as follows

$$f_2(\phi_n^*, \theta_{SR,n}) \triangleq f_1(\phi_n^*) + \theta_{SR,n}. \quad (6)$$

²Since the elements of the RIS are spaced half of the wavelength apart and we assume that the location of the RIS cannot be optimized to ensure strong line-of-sight links, we have, as a first approximation similar to [14]–[16], that the channels can be modeled as independent and identically distributed, and follow a Rayleigh distribution.

The ESR³ can be expressed as follows

$$R_s = [R_D - R_E]^+, \quad (7)$$

where $R_D = \mathbb{E}_{\gamma_D}[\log(1 + \gamma_D)]$ and R_E denote the ergodic rates from S to D and from S to the Eves, respectively. Given $\{\Theta_n\}_{n=1}^N$, an approximated expression of R_D can be found in [15, Eq. (13)]. By averaging over $\{\Theta\}_{n=1}^N$, R_D can be calculated as shown in (8) at the top of the next page, where $A_1 \triangleq \eta^2 d_{SR}^{-\alpha} d_{RD}^{-\alpha}$, $A_2 \triangleq \frac{\sqrt{\pi} \eta 2^b}{4} d_{SD}^{-\frac{\alpha}{2}} d_{SR}^{-\frac{\alpha}{2}} d_{RD}^{-\frac{\alpha}{2}} \sin \frac{\pi}{2^b}$ and $A_3 \triangleq \frac{\eta^2 2^{2b}}{32} d_{SR}^{-\alpha} d_{RD}^{-\alpha} (1 - \cos \frac{2\pi}{2^b})$.

Remark 1: The analysis of the ESR for the considered RIS-assisted system relies only on the knowledge of the statistical eavesdropping CSI, which can be obtained by using several methods, such as those used in [19].

In the following sections, R_E is calculated for non-colluding and colluding Eves, respectively.

III. NON-COLLUDING EVES

In the non-colluding case, R_E can be expressed as follows

$$R_E = \max_{k \in [1:K]} R_{E_k}, \quad (9)$$

where $R_{E_k} \triangleq \mathbb{E}_{\gamma_{E_k}}[\log(1 + \gamma_{E_k})]$. In order to derive R_{E_k} , the distribution of γ_{E_k} in (5) needs to be computed.

A. Distribution of γ_{E_k}

Before deriving the distribution of γ_{E_k} , we introduce the following lemma.

Lemma 1: The phase $\psi_{k,n}$, $k \in [1 : K]$, $n \in [1 : N]$, in (5) has the following properties:

- a) $\psi_{k,n}$ is uniformly distributed in $[0, 2\pi)$;
- b) $\psi_{k,n}$ is independent of $f_2(\phi_n^*, \theta_{SR,n})$ defined in (6);
- c) $\psi_{k,i}$ is independent of $\psi_{k,j}$, $\forall i \neq j$, $i, j \in [1 : N]$.

Proof: See Appendix A. ■

Based on Lemma 1, the distribution of γ_{E_k} in (5) is provided in the following lemma.

Lemma 2: When N is large, γ_{E_k} can be approximated with an exponential random variable with mean $\lambda_{E_k} = \rho(d_{SE_k}^{-\alpha} + NB_k)$, where $B_k \triangleq \eta^2 d_{SR}^{-\alpha} d_k^{-\alpha}$.

Proof: Define $G_k \triangleq \sum_{n=1}^N |g_{SR,n} g_{k,n}| e^{j\psi_{k,n}}$, $k \in [1 : K]$. Based on [20, Lemma 2] and the fact that $\{\psi_{k,n}\}_{n=1}^N$ are independent and identically distributed uniform random variables in $[0, 2\pi)$ as proved in Lemma 1, $G_k \sim \mathcal{CN}(0, N)$ as $N \rightarrow \infty$. Furthermore, since g_{SE_k} is independent of G_k , we have

$$d_{SE_k}^{-\frac{\alpha}{2}} |g_{SE_k}| + \eta d_{SR}^{-\frac{\alpha}{2}} d_k^{-\frac{\alpha}{2}} G_k \sim \mathcal{CN}(0, d_{SE_k}^{-\alpha} + NB_k),$$

as $N \rightarrow \infty$. Recalling that $\gamma_{E_k} = \rho \left| d_{SE_k}^{-\frac{\alpha}{2}} |g_{SE_k}| + \sqrt{B_k} G_k \right|^2$ in (5), the proof follows. ■

Remark 2: The authors of [15] approximated R_D based on the fact that Jensen's inequality is tight, rather than an upper bound, if $\frac{\text{Var}[\gamma_D]}{\mathbb{E}^2[\gamma_D]} \rightarrow 0$, as $N \rightarrow \infty$. However, Lemma 2 shows that Jensen's inequality cannot be applied for approximating R_E , since $\frac{\text{Var}[\gamma_{E_k}]}{\mathbb{E}^2[\gamma_{E_k}]} \rightarrow 1$, as $N \rightarrow \infty$.

³We assume that the RIS appropriately customizes the wireless channel but we consider that the distribution of the signal transmitted by S is always Gaussian. It is worth mentioning that the information-theoretic characterization of RIS-assisted transmission and the calculation of the optimal input distribution in the presence of an RIS is an open issue that is currently under active research [18]. This is, however, beyond the scope of this letter.

$$\begin{aligned}
R_D &\approx \log \left(1 + \rho \left(N \eta^2 d_{SR}^{-\alpha} d_{RD}^{-\alpha} + d_{SD}^{-\alpha} + \frac{\pi^{\frac{3}{2}} \eta}{4} d_{SD}^{-\frac{\alpha}{2}} d_{SR}^{-\frac{\alpha}{2}} d_{RD}^{-\frac{\alpha}{2}} \sum_{n=1}^N \mathbb{E}_{\Theta_n} [\cos \Theta_n] + \frac{\pi^2 \eta^2}{8} d_{SR}^{-\alpha} d_{RD}^{-\alpha} \sum_{i=1}^{N-1} \sum_{k=i+1}^N \mathbb{E}_{\Theta_i, \Theta_k} [\cos(\Theta_k - \Theta_i)] \right) \right) \\
&= \log \left(1 + \rho N A_1 + \rho d_{SD}^{-\alpha} + \rho N A_2 + \rho N(N-1) A_3 \right), \tag{8}
\end{aligned}$$

B. Ergodic Secrecy Rate

The ESR for non-colluding Eves is summarized in the following theorem.

Theorem 1: When N is large, the ESR for non-colluding Eves can be expressed as follows

$$R_s \approx \left[R_D + \frac{1}{\ln 2} \max_{k \in [1:K]} e^{\frac{1}{\lambda_{E_k}}} \text{Ei} \left(-\frac{1}{\lambda_{E_k}} \right) \right]^+, \tag{10}$$

where $\text{Ei}(x) \triangleq -\int_{-x}^{\infty} \frac{e^{-t}}{t} dt$, $x < 0$, is the exponential integral function [21, Eq. 8.211].

Proof: When N is large, based on Lemma 2, R_{E_k} in (9) can be approximated as follows

$$\begin{aligned}
R_{E_k} &\approx \int_0^{\infty} \log(1+x) \frac{1}{\lambda_{E_k}} e^{-\frac{x}{\lambda_{E_k}}} dx = \frac{1}{\ln 2} \int_0^{\infty} \frac{e^{-\frac{x}{\lambda_{E_k}}}}{1+x} dx \\
&= -\frac{e^{\frac{1}{\lambda_{E_k}}}}{\ln 2} \text{Ei} \left(-\frac{1}{\lambda_{E_k}} \right), \tag{11}
\end{aligned}$$

where the last equality is based on [21, Eq. 3.352.4]. Combining (7), (9) and (11), the theorem is proved. ■

C. Asymptotic Analysis

To obtain insights from the obtained ESR, its asymptotic behavior is analyzed in the following corollary.

Corollary 1: As $N \rightarrow \infty$, $R_s \rightarrow \log N + \log A_3 + \frac{\kappa}{\ln 2} - \max_{k \in [1:K]} \log B_k$, which implies that the ESR for non-colluding Eves scales with $\log N$.

Proof: From (8), we have

$$\begin{aligned}
R_D &\approx \log \left(\rho A_3 N^2 \left(\frac{1}{\rho A_3 N^2} + \frac{A_1}{A_3 N} + \frac{d_{SD}^{-\alpha}}{A_3 N^2} + \frac{A_2 - A_3}{A_3 N} + 1 \right) \right) \\
&\rightarrow 2 \log N + \log \rho + \log A_3, \text{ as } N \rightarrow \infty. \tag{12}
\end{aligned}$$

In addition, R_{E_k} in (11) can be further expressed as follows

$$\begin{aligned}
R_{E_k} &\stackrel{(a)}{\approx} \frac{e^{\frac{1}{\lambda_{E_k}}}}{\ln 2} \left(-\kappa + \ln(\lambda_{E_k}) + \sum_{i=1}^{\infty} \frac{(-1)^{i+1}}{i \cdot i! \cdot \lambda_{E_k}^i} \right) \\
&\stackrel{(b)}{\rightarrow} \log(\lambda_{E_k}) - \frac{\kappa}{\ln 2} \\
&\stackrel{(c)}{=} \log(N \rho B_k) + \log \left(1 + \frac{d_{SE_k}^{-\alpha}}{N B_k} \right) - \frac{\kappa}{\ln 2} \\
&\rightarrow \log N + \log \rho + \log B_k - \frac{\kappa}{\ln 2}, \text{ as } N \rightarrow \infty. \tag{13}
\end{aligned}$$

where (a) is based on (11) and [21, Eq. 8.214.1], (b) holds since $1/\lambda_{E_k} \rightarrow 0$ as $N \rightarrow \infty$, and (c) is based on the definition of λ_{E_k} in Lemma 2.

Combining (7), (9), (12) and (13), the corollary follows. ■

Remark 3: Compared with the scaling law $2 \log N$ for non-secrecy transmission with discrete phase shifts [15], Corollary 1 shows that the ESR scales with $\log N$.

IV. COLLUDING EVES

When the Eves are colluding, they can combine their received signals for information interception. Based on [22], R_E in (7) can be expressed as follows

$$R_E = \mathbb{E}_{\{\gamma_{E_k}\}_{k=1}^K} \log \left(1 + \sum_{k=1}^K \gamma_{E_k} \right). \tag{14}$$

Since common random variables $\{g_{SR,n}\}_{n=1}^N$ are present in every γ_{E_k} as shown in (5), $\{\gamma_{E_k}\}_{k=1}^K$ are correlated random variables. However, the following lemma shows that such correlation is negligible for large values of N .

Lemma 3: γ_{E_i} is independent of γ_{E_j} if $N \rightarrow \infty$, $i, j \in [1:K]$, $i \neq j$.

Proof: Let us define $H_{E_k} \triangleq d_{SE_k}^{-\frac{\alpha}{2}} g_{SE_k} + \sqrt{B_k} \sum_{n=1}^N |g_{SR,n} g_{k,n}| e^{j\psi_{k,n}}$. Thus, $\gamma_{E_k} = \rho |H_{E_k}|^2$. According to Lemma 1-a), $\mathbb{E}[e^{j\psi_{k,n}}] = 0$ and $\mathbb{E}[H_{E_k}] = 0$, $\forall k \in [1:K]$. Moreover, since $\psi_{i,n}$ is independent of $\psi_{j,m}$ if $i \neq j$ or $n \neq m$, we have $\mathbb{E}[H_{E_i} H_{E_j}] = 0$, $\forall i \neq j$. Therefore, the covariance of H_{E_i} and H_{E_j} is zero. Furthermore, based on Lemma 2, $\{H_k\}_{k=1}^K$ are uncorrelated complex Gaussian variables if $N \rightarrow \infty$, and hence $\{H_k\}_{k=1}^K$ are independent of each other. This completes the proof. ■

A. Ergodic Secrecy Rate

Based on Lemma 2 and Lemma 3, the ESR is provided in the following theorem.

Theorem 2: When N is large, and $\lambda_{E_i} \neq \lambda_{E_j}$, $\forall i \neq j$, $i, j \in [1:N]$, the ESR for colluding Eves can be approximated as follows

$$R_s \approx \left[R_D + \frac{1}{\ln 2} \sum_{i=1}^K e^{\frac{1}{\lambda_{E_i}}} \text{Ei} \left(-\frac{1}{\lambda_{E_i}} \right) \prod_{j=1, j \neq i}^K \frac{\lambda_{E_i}}{\lambda_{E_i} - \lambda_{E_j}} \right]^+. \tag{15}$$

Proof: Based on Lemma 2 and Lemma 3, if $\lambda_{E_i} \neq \lambda_{E_j}$, $\forall i \neq j$, $\sum_{k=1}^K \gamma_{E_k}$ has the following probability density function (PDF) [23]:

$$f_{\sum_{k=1}^K \gamma_{E_k}}(x) = \sum_{i=1}^K \frac{1}{\lambda_{E_i}} e^{-\frac{x}{\lambda_{E_i}}} \prod_{j=1, j \neq i}^K \frac{\lambda_{E_i}}{\lambda_{E_i} - \lambda_{E_j}}. \tag{16}$$

Combining (11), (14) and (16), we obtain

$$R_E \approx -\frac{1}{\ln 2} \sum_{i=1}^K e^{\frac{1}{\lambda_{E_i}}} \text{Ei} \left(-\frac{1}{\lambda_{E_i}} \right) \prod_{j=1, j \neq i}^K \frac{\lambda_{E_i}}{\lambda_{E_i} - \lambda_{E_j}}. \tag{17}$$

Recalling (7), the theorem is proved. ■

Remark 4: Theorem 2 corresponds to the case that the Eves lie in different locations, so that $\{\gamma_{E_k}\}_{k=1}^K$ have different means. When the Eves are clustered relatively closely together, $\{\gamma_{E_k}\}_{k=1}^K$ have the same (or a very similar) mean. In this case, the ESR can be analyzed in a similar way, whose details are not provided due to space limitations.

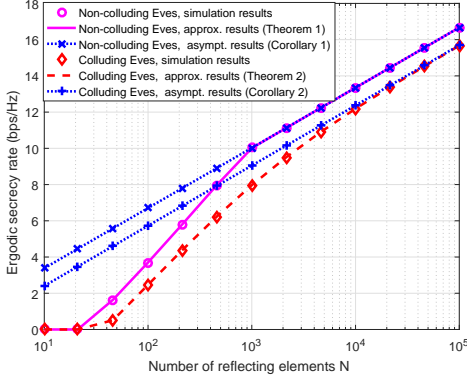


Fig. 1. Ergodic secrecy rate vs. N , for $K = 5$.

B. Asymptotic Analysis

The asymptotic behavior of the obtained ESR for colluding Eves is provided in the following corollary.

Corollary 2: As $N \rightarrow \infty$, $R_s \rightarrow \log N + \log A_3 + \frac{\kappa}{\ln 2} - \sum_{i=1}^K \log B_i \prod_{j=1, j \neq i}^K \frac{B_i}{B_i - B_j}$, which implies that the ESR for colluding Eves also scales with $\log N$.

Proof: From (11), (13) and (17), we have

$$\begin{aligned} R_E &\rightarrow \sum_{i=1}^K \left(\log N + \log \rho - \frac{\kappa}{\ln 2} + \log B_i \right) \prod_{j=1, j \neq i}^K \frac{\lambda_{E_i}}{\lambda_{E_i} - \lambda_{E_j}} \\ &\stackrel{(a)}{\rightarrow} \sum_{i=1}^K \left(\log N + \log \rho - \frac{\kappa}{\ln 2} + \log B_i \right) \prod_{j=1, j \neq i}^K \frac{B_i}{B_i - B_j} \\ &\stackrel{(b)}{=} \log N + \log \rho - \frac{\kappa}{\ln 2} + \sum_{i=1}^K \log B_i \prod_{j=1, j \neq i}^K \frac{B_i}{B_i - B_j}, \end{aligned} \quad (18)$$

where (a) holds since $\lambda_{E_k} = \rho N B_k \left(1 + \frac{d_{SE_k}^{-\alpha}}{N B_k} \right) \rightarrow \rho N B_k$ as $N \rightarrow \infty$, and (b) is based on the fact that $\sum_{i=1}^K \prod_{j=1, j \neq i}^K \frac{B_i}{B_i - B_j} = 1$, as proved in [23, Chapter 5].

Combining (7), (12), (14) and (18), the proof follows. ■

Remark 5: Comparing Corollaries 1 and 2, we evince that only the last terms for the asymptotic ESR are different, i.e., $\max_{k \in [1:K]} \log B_k$ and $\sum_{i=1}^K \log B_i \prod_{j=1, j \neq i}^K \frac{B_i}{B_i - B_j}$ for non-colluding and colluding Eves, respectively. In addition, the ESRs for both non-colluding and colluding Eves have the same scaling law, i.e., $\log N$.

C. Large Number of Eves

To obtain more insights from the obtained ESR, we provide a simplified expression of R_s for large values of K in the following corollary.

Corollary 3: When N and $K \rightarrow \infty$, the ESR for colluding Eves can be approximated as follows

$$R_s \approx \left[R_D - \log \left(1 + \sum_{k=1}^K \lambda_{E_k} \right) \right]^+. \quad (19)$$

Proof: Based on Lemma 3, $\text{Var} \left[\sum_{k=1}^K \gamma_{E_k} \right] \rightarrow \sum_{k=1}^K \lambda_{E_k}^2$ as $N \rightarrow \infty$. Thus, $\frac{\text{Var} \left[\sum_{k=1}^K \gamma_k \right]}{(\mathbb{E} \left[\sum_{k=1}^K \gamma_k \right])^2} \rightarrow \frac{\sum_{k=1}^K \lambda_{E_k}^2}{(\sum_{k=1}^K \lambda_{E_k})^2} \rightarrow 0$ as N and $K \rightarrow \infty$. According to [24, Theorem 4], R_E in (14) can be

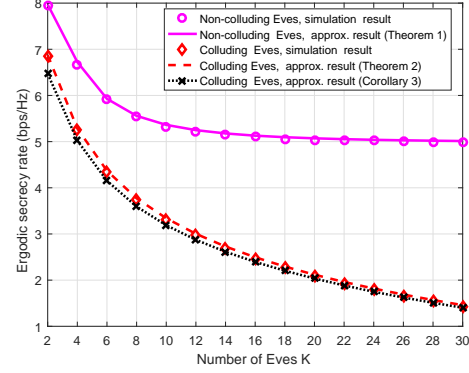


Fig. 2. Ergodic secrecy rate vs. K , for $N = 250$.

approximated as $R_E \approx \log \left(1 + \mathbb{E} \left[\sum_{k=1}^K \gamma_k \right] \right)$. This completes the proof. ■

V. NUMERICAL RESULTS

In this section, numerical results are provided to verify the analytical results stated in the theorems and corollaries. For illustrative purposes, we set $\alpha = 3$, $b = 3$ bits, $P = 20$ dBm, $\sigma^2 = -96$ dBm and $\eta = 0.8$. In addition, S , R and D are located at $(0, 0)$ m, $(100, 0)$ m and $(90, 20)$ m, respectively. As for the Eves, E_k is located at $(\frac{90k}{K}, -20)$ m, $k \in [1:K]$. For the considered simulation setup, the ESR is zero in the absence of RIS. In this case, in fact, the ESR for non-colluding Eves can be expressed as $R_s = [f_3(d_{SD}) - \max_{k \in [1:K]} f_3(d_{SE_k})]^+$, where $f_3(x) \triangleq \frac{1}{\ln 2} \int_0^\infty e^{-\frac{t}{\rho x^{-\alpha}}}/(1+t) dt$, $x > 0$. Therefore, $R_s = 0$ since $f_3(x)$ is a decreasing function of x and $d_{SD} \geq d_{SE_k}$ in the considered network configuration, $\forall k \in [1:K]$.

Fig. 1 shows the impact of the number of reconfigurable elements N on the ESR, when the number of Eves is $K = 5$. We observe that the approximated analytical results in Theorems 1 and 2 match well with Monte Carlo simulations almost for all values of N . This is because the ESR is zero for small values of N , and starts to be positive for large values of N , i.e., $N \geq 46$ in the considered case. We also observe that the ESR increases with N . For example, the ESRs are about 3.7 bps/Hz and 2.5 bps/Hz for non-colluding and colluding Eves, respectively, if $N = 100$. In addition, the analytical results obtained in Corollaries 1 and 2 asymptotically approach the simulations as N becomes sufficiently large, which confirms the scaling laws. The setup with non-colluding Eves provides a larger secrecy rate since only the “best” Eve determines the ESR. There exists a constant gap of about 1 bps/Hz between the ESRs for non-colluding and colluding Eves if N exceeds 10^4 .

In Fig. 2, the ESR as a function of the number of Eves K for $N = 250$ is shown. The figure confirms the findings in Corollary 3 for colluding Eves, and we observe that the approximation in (19) becomes tighter as K increases. The ESR for non-colluding Eves is less affected by K . We observe, in particular, that there exists an ESR floor of about 5 bps/Hz for large values of K . This is because the ESR for non-colluding Eves is determined by the nearest Eve to the source. In the considered simulation setup, the nearest Eve is located at around $(0, -20)$ m, when K is large.

VI. CONCLUSIONS

This letter investigated the ESR of an RIS-assisted communication system in the presence of discrete phase shifts and multiple Eves. We obtained an approximated closed-form expression of the ESR and unveiled that the ESR scales with $\log N$ in the presence of both non-colluding and colluding Eves. An interesting future direction is to analyze the ESR of RIS-assisted systems in the presence of multi-antenna transmitters. For example, the recent research works in [16], [25] could be generalized in order to take into account security constraints.

APPENDIX A PROOF OF LEMMA 1

Let us denote $X_{1,n} \triangleq f_2(\phi_n^*, \theta_{SR,n})$, $X_{2,n} \triangleq \theta_{k,n}$ and $Y_n \triangleq \psi_{k,n}$. Accordingly, $Y_n = X_{1,n} + X_{2,n}$ as shown in Section II. We note that the random phases $X_{1,n}$, $X_{2,n}$ and Y_n have a uniform circular distribution.

Given $X_{1,n} = x_1$, $\forall x_1 \in [0, 2\pi)$, $Y_n = x_1 + X_{2,n}$ is uniformly distributed in $[x_1, x_1 + 2\pi) = [x_1, 2\pi) \cup [2\pi, x_1 + 2\pi)$. Since Y_n has a circular uniform distribution, $[2\pi, x_1 + 2\pi)$ is equivalent to $[0, x_1)$. Thus, Y_n is uniformly distributed in $[0, 2\pi)$, which proves Lemma 1-a).

Since $X_{1,n}$ and $X_{2,n}$ are independent, their joint PDF is

$$f_{X_{1,n}, X_{2,n}}(x_1, x_2) = f_{X_{1,n}}(x_1) f_{X_{2,n}}(x_2) = \frac{1}{2\pi} f_{X_{1,n}}(x_1). \quad (20)$$

We can construct the following Jacobian matrix

$$J_{X_{1,n}, Y_n}(x_1, x_2) = \begin{bmatrix} \frac{\partial x_1}{\partial x_1} & \frac{\partial x_1}{\partial x_2} \\ \frac{\partial y}{\partial x_1} & \frac{\partial y}{\partial x_2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \quad (21)$$

Thus, the joint PDF of $X_{1,n}$ and Y_n can be written as

$$\begin{aligned} f_{X_{1,n}, Y_n}(x_1, y) &= \frac{f_{X_{1,n}, X_{2,n}}(x_1, x_2)}{\det(J_{X_{1,n}, Y_n}(x_1, x_2))} = \frac{1}{2\pi} f_{X_{1,n}}(x_1) \\ &= f_{X_{1,n}}(x_1) f_{Y_n}(y), \end{aligned} \quad (22)$$

which implies that Y_n is independent of $X_{1,n}$. Thus, Lemma 1-b) is proved.

For $\forall i \neq j$ and $i, j \in [1 : N]$, we have $Y_i = X_{1,i} + X_{2,i}$ and $Y_j = X_{1,j} + X_{2,j}$. Although the same random phase θ_{SD} is present in both Y_i and Y_j as shown in Section II, Y_i is still independent of Y_j , due to the following two facts: (i) Y_i and Y_j are independent of $X_{1,i}$ and $X_{1,j}$, respectively, according to Lemma 1-b); (ii) $X_{2,i}$ is independent of $X_{2,j}$. Therefore, Lemma 1-c) is proved.

REFERENCES

- [1] M. Di Renzo, *et al.*, "Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–20, May 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 in Commun.*, vol. 38, no. 11, pp. 2450–2525, Nov. 2020.
- [3] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, Aug. 2019.
- [4] M. Di Renzo, *et al.*, "Reconfigurable intelligent surfaces vs. relaying: Differences, similarities, and performance comparison," *IEEE Open J. Commun. Society*, vol. 1, pp. 798–807, June 2020.
- [5] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Nov. 2019.
- [6] Y. Liu, *et al.*, "Reconfigurable intelligent surfaces: Principles and opportunities," *arXiv:2007.03435*, year=2020.
- [7] C. Pan, *et al.*, "Multicell mimo communications relying on intelligent reflecting surfaces," *IEEE Trans. Wireless Commun.*, vol. 19, no. 8, pp. 5218–5233, Aug. 2020.
- [8] C. Pan, *et al.*, "Intelligent reflecting surface aided mimo broadcasting for simultaneous wireless information and power transfer," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1719–1734, Aug. 2020.
- [9] 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, May 2019.
- [10] Z. Chu, W. Hao, P. Xiao, and J. Shi, "Intelligent reflecting surface aided multi-antenna secure transmission," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, Sep. 2020.
- [11] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jan. 2020.
- [12] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2637–2652, Nov. 2020.
- [13] H. Wang, J. Bai, and L. Dong, "Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI," *IEEE Sig. Process. Lett.*, vol. 27, pp. 1300–1304, Jul. 2020.
- [14] L. Yang, Y. Jinxia, W. Xie, M. Hasna, T. Siftsis, and M. Di Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Vehi. Technol.*, doi: 10.1109/TVT.2020.3007521, 2020.
- [15] D. Li, "Ergodic capacity of intelligent reflecting surface-assisted communication systems with phase errors," *IEEE Commun. Lett.*, vol. 24, no. 8, pp. 1646–1650, Aug. 2020.
- [16] X. Qian, M. Di Renzo, J. Liu, A. Kammoun, and M. S. Alouini, "Beamforming through reconfigurable intelligent surfaces in single-user MIMO systems: SNR distribution and scaling laws in the presence of channel fading and phase noise," *IEEE Wireless Commun. Lett.*, doi: 10.1109/LWC.2020.3021058, 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.*, doi: 10.1109/LWC.2020.3031084, 2020.
- [18] R. Karasik, O. Simeone, M. Di Renzo, and S. Shamai Shitz, "Beyond max-snr: Joint encoding for reconfigurable intelligent surfaces," in *IEEE Int. Symp. Inf. Theory (ISIT)*, Los Angeles, CA, USA, Jun. 2020, pp. 2965–2970.
- [19] B. Shang, L. Liu, J. Ma and P. Fan, "Unmanned aerial vehicle meets vehicle-to-everything in secure communications," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 98–103, Oct. 2019.
- [20] Z. Ding, R. Schober, and H. V. Poor, "On the impact of phase shifting designs on IRS-NOMA," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1596–1600, Oct. 2020.
- [21] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. New York, NY, USA: Academic, 2000.
- [22] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics and Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.
- [23] S. M. Ross, *Introduction to probability models*, 10th ed. Academic, Amsterdam, 2010.
- [24] S. Sanayei and A. Nosratinia, "Opportunistic beamforming with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 2765–2771, Aug. 2007.
- [25] A. Zappone, M. Di Renzo, F. Shams, X. Qian, and M. Debbah, "Overhead-aware design of reconfigurable intelligent surfaces in smart radio environments," *IEEE Trans. Wireless Commun.*, doi: 10.1109/TWC.2020.3023578, 2020.