Ergodic Secrecy Capacity 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 capacity (ESC) 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 ESC 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 ESC, and it is proved that the ESC 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 capacity.

I. INTRODUCTION

Reconfigurable intelligent surfaces (RISs) utilize a large number of passive reflecting elements to customize wireless communication environments [1]–[4]. In particular, the amplitude and phase shift of each reflecting element can be controlled, so that the received signal at the intended receiver can be strengthened through passive beamforming [5]. Due to the low-cost, high energy-efficiency and full-duplex advantages, RISs are regarded as a promising technology for the next-generation wireless communications and hence have recently received much academic and industrial attention [6]–[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 the 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. In particular, the authors of [13] proposed a joint beamforming and jamming scheme to enhance the secrecy rate, and the authors of [14] analyzed the secrecy outage probability at the RIS. However, these two works only considered a single eavesdropper and assumed continuous phase shifts at the reflecting elements of the RIS.

Different from these existing works, this letter investigates the ergodic secrecy capacity (ESC) 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 ESC for both non-colluding and colluding Eves. In order to provide insights, asymptotic analysis is also provided from the obtained ESC, and it is proved that, as the number of reflecting elements N goes to infinity, the ESC scales with $\log N$ for both non-colluding and colluding Eves. Numerical results are illustrated to verify that the analytical results and the scaling laws are accurate for large values of N.

Notation: $\mathbb{C}$ and $\mathbb{Z}$ denote the complex domain and integer set, respectively; for brevity, we denote $[1 : M] \triangleq \{1, \ldots, M\}$, 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

As shown in Fig. 1, we consider an RIS-assisted secure communication system with a source (S), an RIS (R) with N reflecting elements, a destination (D) and K Eves $(E_k, \forall k \in [1 : K])$. All nodes are assumed to be equipped with a single antenna. The channels $S \to D$, $S \to E_k$, $S \to R$, $R \to D$ and $R \to E_k$ 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
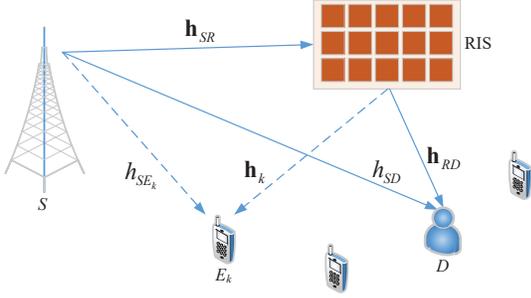
Fig. 1. RIS-assisted secrecy communication system.

$[\mathbf{h}_k]_n = g_{k,n}d_k^{-\frac{\alpha}{2}}$, where g_{SD}, g_{SE_k}, $g_{SR,n}$, $g_{RD,n}$, $g_{k,n} \sim \mathcal{CN}(0,1)$ denote the small-scale fading, d_{SD}, d_{SE_k}, d_{SR}, d_{RD} and d_k denote the distances $S \to D$, $S \to E_k$, $S \to R$, $R \to D$ and $R \to E_k$, 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

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

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

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, $\mathbf{\Phi} \triangleq \text{diag}(e^{j\phi_1}, \ldots, e^{j\phi_N})$ and $\phi_n \in [0,2\pi)$ is the nth phase shift at 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. Furthermore, in this letter, ϕ_n can only take a finite number of discrete values. In particular, the set of discrete phase shifts is denoted by $\mathcal{F} \triangleq \left\{0, \frac{2\pi}{2^b}, \ldots, \frac{(2^b-1)2\pi}{2^b}\right\}$, 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 quantization error is $\Theta_n = f_1(\phi_n^*) - \phi_n^*$, which is uniformly distributed in $\left[-\frac{\pi}{2^b}, \frac{\pi}{2^b}\right]$, similar to [15]–[18]. Accordingly, the received SNRs at D and E_k are formulated, respectively, as follows

$$\gamma_D = \rho\left|| h_{SD}| + \eta \sum_{n=1}^{N} |[\mathbf{h}_{SR}]_n[\mathbf{h}_{RD}]_n| e^{j\Theta_n}\right|^2$$

$$= \rho\left|d_{SD}^{-\frac{\alpha}{2}}|g_{SD}| + \eta d_{SR}^{-\frac{\alpha}{2}}d_{RD}^{-\frac{\alpha}{2}} \sum_{n=1}^{N} |g_{SR,n}g_{RD,n}| e^{j\Theta_n}\right|^2, \quad (4)$$

$$\gamma_{E_k} = \rho\left| h_{SE_k} + \eta \sum_{n=1}^{N} |[\mathbf{h}_{SR}]_n[\mathbf{h}_k]_n| e^{j\psi_{k,n}}\right|^2$$

$$= \rho\left|d_{SE_k}^{-\frac{\alpha}{2}}g_{SE_k} + \eta d_{SR}^{-\frac{\alpha}{2}}d_k^{-\frac{\alpha}{2}} \sum_{n=1}^{N} |g_{SR,n}g_{k,n}| e^{j\psi_{k,n}}\right|^2, \quad (5)$$

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

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

The ESC can be expressed as follows [19]

$$C_s = [C_D - C_E]^+, \quad (7)$$

where $C_D = \mathbb{E}_{\gamma_D}[\log(1 + \gamma_D)]$ and C_E denote the ergodic capacities from S to D and the Eves, respectively. Given $\{\Theta_n\}_{n=1}^N$, an approximated expression of C_D can be found in [16, Eq. (13)]. By averaging over $\{\Theta\}_{n=1}^N$, C_D can be calculated as shown in (8) at the top of the next page.

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

III. Non-Colluding Eves

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

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

where $C_{E_k} \triangleq \mathbb{E}_{\gamma_{E_k}}[\log(1 + \gamma_{E_k})]$. In order to derive C_{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 1: 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 as 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 2: 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 (i.i.d.) uniform random variables in $[0,2\pi)$ as proved in Lemma 1, $G_k \sim \mathcal{CN}(0,N)$ as $N \to \infty$. Furthermore, since g_{SE_k} is independent of G_k, we have

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

as $N \to \infty$. 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.

B. Ergodic Secrecy Capacity

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

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

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

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

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

$$= \log\left(1+\rho N A_1+\rho d_{SD}^{-\alpha}+\rho N A_2+\rho N(N-1)A_3\right), \tag{8}$$

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 $A_3 \triangleq \frac{\eta^2 2^{2b}}{32}d_{SR}^{-\alpha}d_{RD}^{-\alpha}\left(1-\cos\frac{2\pi}{2^b}\right)$.

Proof 3: When N is large, based on Lemma 2, C_{E_k} in (9) can be approximated as follows

$$C_{E_k} \approx \int_0^\infty \log(1+x)\frac{1}{\lambda_{E_k}}e^{-\frac{x}{\lambda_{E_k}}}\,dx = \frac{1}{\ln 2}\int_0^\infty \frac{e^{-\frac{x}{\lambda_{E_k}}}}{1+x}\,dx$$

$$= -\frac{e^{\frac{1}{\lambda_{E_k}}}}{\ln 2}\mathrm{Ei}\left(-\frac{1}{\lambda_{E_k}}\right), \tag{11}$$

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 ESC, its asymptotic behavior is analyzed in the following corollary.

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

Proof 4: From (8), we have

$$C_D \approx \log\left(\rho A_3 N^2\left(\frac{1}{\rho A_3 N^2}+\frac{A_1}{A_3 N}+\frac{d_{SD}^{-\alpha}}{A_3 N^2}+\frac{A_2-A_3}{A_3 N}+1\right)\right)$$

$$\to 2\log N + \log\rho + \log A_3, \text{ as } N \to \infty. \tag{12}$$

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

$$C_{E_k} \overset{(a)}{\approx} \frac{e^{\frac{1}{\lambda_{E_k}}}}{\ln 2}\left(-\kappa+\ln(\lambda_{E_k})+\sum_{i=1}^{\infty}\frac{(-1)^{i+1}}{i\cdot i!\cdot\lambda_{E_k}^i}\right)$$

$$\overset{(b)}{\to} \log(\lambda_{E_k})-\frac{\kappa}{\ln 2}$$

$$\overset{(c)}{=} \log(N\rho B_k)+\log\left(1+\frac{d_{SE_k}^{-\alpha}}{NB_k}\right)-\frac{\kappa}{\ln 2}$$

$$\to \log N+\log\rho+\log B_k-\frac{\kappa}{\ln 2}, \text{ as } N \to \infty. \tag{13}$$

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

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

Remark 1: Compared with the scaling law $2\log N$ for non-secrecy transmission with discrete phase shifts [15], [16], Corollary 1 shows that the ESC has a different scaling law that is equal to $\log N$.

IV. COLLUDING EVES

When the Eves are colluding, they can combine their received signals for information interception. Thus, the C_E in (7) can be expressed as follows

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

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 $N \to \infty$, $i,j \in [1:K]$, $i \neq j$.

Proof 5: See Appendix B.

A. Ergodic Secrecy Capacity

Based on Lemma 2 and Lemma 3, the ESC 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 ESC for colluding Eves can be approximated as follows

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

Proof 6: Based on 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) [22]:

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

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

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

Recalling (7), we prove the theorem.

Remark 2: 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 that $\{\gamma_{E_k}\}_{k=1}^K$ have the same mean, the ESC can be analyzed in a similar way, whose details are not provided due to space limitations.

B. Asymptotic Analysis

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

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

Proof 7: From (11), (13) and (17), we have

$$C_E \to \sum_{i=1}^{K}\left(\log N+\log\rho-\frac{\kappa}{\ln 2}+\log B_i\right)\prod_{j=1,j\neq i}^{K}\frac{\lambda_{E_i}}{\lambda_{E_i}-\lambda_{E_j}}$$

$$\overset{(a)}{\to} \sum_{i=1}^{K}\left(\log N+\log\rho-\frac{\kappa}{\ln 2}+\log B_i\right)\prod_{j=1,j\neq i}^{K}\frac{B_i}{B_i-B_j}$$

$$\overset{(b)}{=} \log N+\log\rho-\frac{\kappa}{\ln 2}+\sum_{i=1}^{K}\log B_i\prod_{j=1,j\neq i}^{K}\frac{B_i}{B_i-B_j}, \tag{18}$$

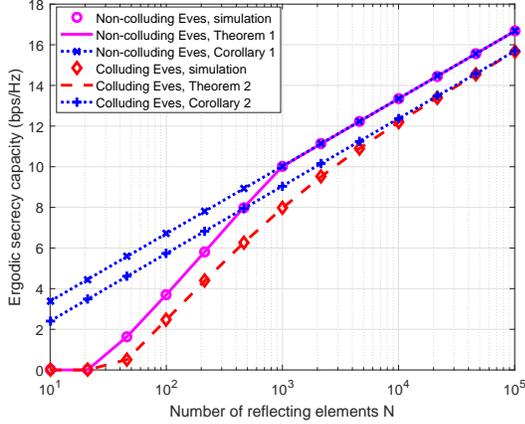Fig. 2. Ergodic secrecy capacity vs. N, for $K = 5$.

Fig. 3. Ergodic secrecy capacity vs. K, for $N = 250$.

where (a) holds since $\lambda_{E_k} = \rho N B_k \left(1 + \frac{d_{SE_k}^{-\alpha}}{N B_k} \right) \to \rho N B_k$ as $N \to \infty$, 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 [22, Chapter 5].

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

Remark 3: Comparing Corollaries 1 and 2, we evince that only the last terms for the asymptotic ESC 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 ESCs for both non-colluding and colluding Eves have the same scaling law $\log N$.

C. Large Number of Eves

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

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

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

Proof 8: Based on Lemma 3, $\text{Var} \left[\sum_{k=1}^{K} \gamma_{E_k} \right] \to \sum_{k=1}^{K} \lambda_{E_k}^2$ as $N \to \infty$. Thus, $\frac{\text{Var}\left[\sum_{k=1}^{K} \gamma_k \right]}{\left(\mathbb{E}\left[\sum_{k=1}^{K} \gamma_k \right] \right)^2} \to \frac{\sum_{k=1}^{K} \lambda_{E_k}^2}{\left(\sum_{k=1}^{K} \lambda_{E_k} \right)^2} \to 0$ as N and $K \to \infty$. According to [23, Theorem 4], C_E in (14) can be approximated as follows

$$C_E \approx \log \left(1 + \mathbb{E}\left[\sum_{k=1}^{K} \gamma_k \right] \right). \tag{20}$$

This completes the proof.

V. NUMERICAL RESULTS

In this section, numerical results are provided to verify the analytical results in the obtained theorems and corollaries. The simulation results are averaged over 10^4 channel realizations. 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 $\left(\frac{90k}{K}, -20 \right)$ m, $k \in [1 : K]$. For the considered simulation configuration, the ESC is zero
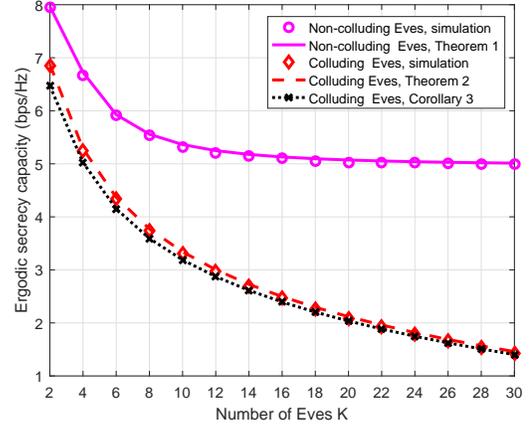
in the absence of the RIS. In this case, in fact, the ESC for non-colluding Eves can be expressed as follows

$$C_s = \left[\mathbb{E}_{h_{SD}}[1 + \rho |h_{SD}|^2] - \max_{k \in [1:K]} \mathbb{E}_{h_{SE_k}}[1 + \rho |h_{SE_k}|^2] \right]^+$$
$$= \left[f_3(d_{SD}) - \max_{k \in [1:K]} f_3(d_{SE_k}) \right]^+, \tag{21}$$

where $f_3(x) \triangleq \frac{1}{\ln 2} \int_0^\infty e^{-\frac{t}{\rho x^{-\alpha}}} / (1 + t) \mathrm{d}t$, $x > 0$. Therefore, $C_s = 0$ in (21), since $f_3(x)$ is a decreasing function of x and $d_{SD} \geq d_{SE_k}$ in the considered simulation configuration, $\forall k \in [1 : K]$.

Fig. 2 shows the impact of the number of reflecting elements N on the ESC, when the number of Eves is $K = 5$. We can observe that the ESC increases with N. For example, the ESCs are about 3.7 bps/Hz and 2.5 bps/Hz for non-colluding and colluding Eves, respectively, if $N = 100$. We observe that the approximated analytical results in Theorems 1 and 2 match well with Monte Carlo simulations. In addition, the asymptotic analytical results obtained in Corollaries 1 and 2 asymptotically approach the simulations as N becomes sufficiently large, which confirms the scaling laws in Corollaries 1 and 2. The setup with non-colluding Eves provides a larger secrecy capacity since only the "best" Eve determines the ESC. There exists a constant gap of about 1 bps/Hz between the ESCs for non-colluding and colluding Eves if N exceeds 10^4.

In Fig. 3, the ESC is shown as a function of the number of Eves K, by assuming $N = 250$. This figure confirms the findings in Corollary 3 for colluding Eves, and we observe that the approximation in (19) becomes tighter as K increases. The ESCs for both non-colluding and colluding Eves decrease with K. However, the ESC for non-colluding Eves is less affected by K. We observe, in particular, that there exists an ESC floor of about 5 bps/Hz for large values of K. This is because the ESC 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 ESC 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 ESC for both non-colluding and colluding Eves, which were demonstrated to be accurate for large values of the number of RIS reflecting elements. By analyzing the asymptotic behaviors of the obtained ESC, we unveiled that the ESC scales with $\log N$ in the presence of both non-colluding and colluding Eves. Numerical results were provided to verify the accuracy of the analytical results and the scaling laws.

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[1] [15].

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

$$f_{X_{1,n}, X_{2,n}}(x_1, x_2) = f_{X_{1,n}}(x_1) f_{X_{2,n}}(x_2) = \frac{1}{2\pi} f_{X_{1,n}}(x_1). \quad (22)$$

We can construct the following Jacobian matrix

$$J_{X_{1,n}, Y_n}(x_1, x_2) = \begin{bmatrix} \frac{\partial x_1}{\partial x_1}, & \frac{\partial x_1}{\partial x_2} \\ \frac{\partial y}{\partial x_1}, & \frac{\partial y}{\partial x_2} \end{bmatrix} = \begin{bmatrix} 1, & 0 \\ 1, & 1 \end{bmatrix}. \quad (23)$$

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

$$\begin{aligned} f_{X_{1,n}, Y_n}(x_1, y) &= \frac{f_{X_{1,n}, X_{2,n}}(x_1, x_2)}{\det(J_{X_{1,n}, Y_n}(x_1, x_2))} = \frac{1}{2\pi} f_{X_{1,n}}(x_1) \\ &= f_{X_{1,n}}(x_1) f_{Y_n}(y), \end{aligned} \quad (24)$$

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.

APPENDIX B
PROOF OF LEMMA 3

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), $\mathbb{E}\left[e^{j\psi_{k,n}}\right] = 0$ and

$$\mathbb{E}\left[H_{E_k}\right] = 0, \ \forall k \in [1 : K]. \quad (25)$$

Moreover, since $\psi_{i,n}$ is independent of $\psi_{j,m}$ if $i \neq j$ or $n \neq m$, we have

$$\mathbb{E}[H_{E_i} H_{E_j}] = 0, \ \forall i \neq j. \quad (26)$$

From (25) and (26), the covariance of H_{E_i} and H_{E_j} can be expressed as follows

$$\text{Cov}(H_{E_i} H_{E_j}) = \mathbb{E}[H_{E_i} H_{E_j}] - \mathbb{E}[H_{E_i}]\mathbb{E}[H_{E_j}] = 0. \quad (27)$$

[1] A random phase X that follows a circular distribution fulfills the property that all the realization points $\{x + 2M\pi\}_{\forall M \in \mathbb{Z}}$ of X are equivalent to the point x, where $x \in [0, 2\pi)$.

Based on Lemma 2 and (27), $\{H_k\}_{k=1}^K$ are uncorrelated complex Gaussian variables if $N \to \infty$, and hence $\{H_k\}_{k=1}^K$ are independent of each other. This completes the proof.

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] ——, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and road ahead," *arXiv:2004.09352*.

[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. 116 753–116 773, 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] ——, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Nov. 2020.

[7] Z. Abdullah, G. Chen, S. Lambotharan, and J. A. Chambers, "A hybrid relay and intelligent reflecting surface network and its ergodic performance analysis," *IEEE Wireless Commun. Lett. (Early Access)*.

[8] Y. Liu, *et al.* "Reconfigurable intelligent surfaces: Principles and opportunities." *arXiv:2007.03435*.

[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. (Early Access)*, 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. Tsiftsis, and M. Di Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Vehi. Technol. (Early Access)*, 2020.

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

[16] 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.

[17] T. Wang, G. Chen, J. P. Coon, and M. Badiu, "Study of intelligent reflective surface assisted communications with one-bit phase adjustments," *in proc. IEEE Globecom, Taiwan, China*, pp. 1–6, 2020.

[18] 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?" *arXiv: 2008.05317*.

[19] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," *IEEE Trans. Vehi. Technol.*, vol. 65, no. 8, pp. 6146–6158, Aug. 2016.

[20] Z. Ding, R. Schober, and H. V. Poor, "On the impact of phase shifting designs on IRS-NOMA," *IEEE Wireless Commun. Lett. (Early Access)*.

[21] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. New York, NY, USA: Academic, 2000.

[22] S. M. Ross, *Introduction to probability models*, 10th ed. Academic, Amsterdam, 2010.

[23] S. Sanayei and A. Nosratinia, "Opportunistic beamforming with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 2765–2771, Aug. 2007.