IEEE Communications Letters, Available online 11 April 2022
DOI: 10.1109/LCOMM.2022.3166239

A Multi-Eavesdropper Scheme against RIS Secured LoS-dominated Channel

Zhuangkun Wei[1], Weisi Guo[1,2*], Bin Li[3]

***Abstract*—Reconfigurable intelligent surface (RIS) has been shown as a promising technique to increase the channel randomness for secret key generation (SKG) in low-entropy channels (e.g., static or line-of-sight (LoS)), without small-scale fading. In this letter, we show that even with the aid of RIS, collaborative eavesdroppers (Eves) can still estimate the legitimate Alice-Bob channel and erode their secret key rates (SKRs), since the RIS induced randomness is also reflected in the Eves' observations. Conditioned on Eves' observations, if the entropy of RIS-combined legitimate channel is zero, Eves are able to estimate it and its secret key. Leveraging this, we design a multi-Eve scheme against the RIS-secured LoS dominated scenarios, by using the multiple Eves' observations to reconstruct the RIS-combined legitimate channel. We further deduce a closed-form secret key leakage rate under our designed multi-Eve scheme, and demonstrate the results via simulations.**

***Index Terms*—Physical layer secret key, reconfigurable intelligent surface, eavesdropping, static channel, wireless communications.**

I. Introduction

Recent advances in reconfigurable intelligent surface (RIS) have been proved to significantly improve the wireless communication performances, and thereby motivated a plethora of applications in civilian and commercial domains. The introduction of RIS also provides an extra free-of-domain to increase the physical layer security (PLS) for wireless communication systems [1]. Related studies are categorized as key-less PLS [2]–[6] and physical layer secret key generation (PL-SKG) [7]–[11].

Key-less PLS leverages the superiority of the legitimate channels over the wiretap ones, by optimizing the key variables (e.g., RIS phases, beamforming vector, and trajectory of mobile legitimate nodes) to maximize the secrecy rate [3]–[6]. One challenge is that there is no guarantee of an existence of feasible solutions, if the eavesdroppers' (Eves') receiving beamforming vectors span for the full space, or other complex mission-layer constraints (e.g., avoiding obstacles) are added.

The second family is PL-SKG, which exploits random and reciprocal channel properties to generate secret key between legitimate nodes. In high entropy channel with rich small-scale scattering induced randomness (as shown by Fig. 1), robust PL-SKG can be guaranteed, and is able to prevent eavesdropping if Eves are half-wavelength away from the legitimate nodes [7]–[11].

This work was supported by the Engineering and Physical Sciences Research Council [grant number: EP/V026763/1].
[1]School of Aerospace, Transport, and Manufacturing, Cranfield University, UK. [2]The Alan Turing Institute, UK. [3]Department of Information Engineering, Beijing University of Posts and Telecommunications, China. *Corresponding Author: weisi.guo@cranfield.ac.uk.

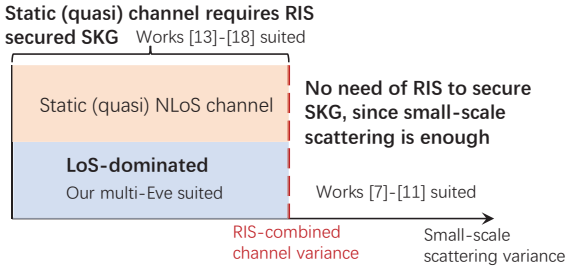

Fig. 1. Categories of current PL-SKG researches.

When it comes to the low-entropy scenarios where small-scale fading of legitimate channels is lack, e.g., static or line-of-sight (LoS) channels (as shown by Fig. 1), the physical layer secret key is easily decoded due to the lack of randomness [12]. To address this challenge, RIS has been deployed to generate channel randomness via reflective elements [13]–[18]. To be specific, by randomly assigning an RIS phase for each legitimate channel estimation round, the reciprocal randomness of legitimate channels can be artificially generated, enabling the shared key generation. However, most studies of the RIS-secured PL-SKG overlook that the RIS random phase is also contained in the Eves' received signals, which if properly utilized, will decrease the secret key rate (SKR). The work in [19] provides a collaborative eavesdropping scheme attacking RIS-secured static channel, but (i) [19] did not analyze the information theory behind their design (e.g., the secret key rate), and (ii) the required number of collaborative Eves is larger than the RIS elements (e.g., 10^2 [20]), which is infeasible in practice. A thorough comparison with [19] is performed in Simulation section.

In this work, we show an eavesdropping threat for RIS-secured PL-SKG from information theory aspect: Conditioned on Eves' received signals (observations) that contain the RIS random phase, if the entropy of RIS-combined legitimate channel is zero, Eves are able to estimate it and the secret key. Leveraging this, we design a multi-Eve scheme against the RIS-secured SKG in LoS-dominated scenarios, which exploits the multi-Eve path diversity to reconstruct the RIS-combined legitimate channel. We further deduce a closed-form secret key leakage rate under our designed multi-Eve scheme. Finally, we perform simulations to verify our design.

In this work, we use non-bold letters to represent scalars, bold lower-case letters for vectors, and bold capital letters for matrices. We use $\|\cdot\|_0$ and $\|\cdot\|_2$ to denote l_0-norm and l_2-norm. We use $diag(\cdot)$ to diagonalize a vector, and $det(\cdot)$ to compute

the determinant. The matrix transpose, conjugate transpose, and element-wise conjugate operators are $(\cdot)^T$, $(\cdot)^H$, and $(\cdot)^*$. $I(\cdot,\cdot)$ is mutual information and $H(\cdot)$ is information entropy.

II. RIS-secured LoS Channel Model

In this work, we consider an RIS-secured LoS-dominated Alice-Bob model. The legitimate Alice and Bob (with single-antenna) aim to generate secret key relying on the reciprocal channel between them. Here, we assume that the direct channels between Alice and Bob are LoS-dominated, and hence an RIS (an uniform planar array with $M \in \mathbb{N}^+$ elements) is deployed to generate the randomness by randomly shifting its reflecting phases [14]–[17].

The PL-SKG is realized by repeating the channel estimation round throughout the whole coherent time [14]. In each channel estimation round, RIS generates a random phase vector, i.e., $\mathbf{w} = [\exp(j\theta_1), \cdots, \exp(j\theta_M)]$ with $\theta_m \sim \mathcal{U}[0, 2\pi), m \in \{1, \cdots, M\}$, which remains unchanged during this round, but will change independently for next round [14]. Each channel estimation round includes an odd and an even time-slot. In the odd time-slot, Alice sends pilot $\mathbf{u}_A \in \mathbb{C}^{L\times 1}$ and Bob receives $\mathbf{y}_B$. Then in even time-slot, Bob sends pilot sequence $\mathbf{u}_B \in \mathbb{C}^{L\times 1}$ and the received signal at Alice is $\mathbf{y}_A$. The expressions of $\mathbf{y}_A$ and $\mathbf{y}_B$ are:

$$\begin{aligned} \mathbf{y}_A &= (h_{BA} + \mathbf{h}_{RA} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{BR}) \cdot \mathbf{u}_B + \boldsymbol{\epsilon}_A. \\ \mathbf{y}_B &= (h_{AB} + \mathbf{h}_{RB} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{AR}) \cdot \mathbf{u}_A + \boldsymbol{\epsilon}_B \end{aligned} \tag{1}$$

In Eq. (1), $h_{AB}, h_{BA} \in \mathbb{C}$, $\mathbf{h}_{AR}, \mathbf{h}_{BR} \in \mathbb{C}^{M\times 1}$ and $\mathbf{h}_{RA}, \mathbf{h}_{RB} \in \mathbb{C}^{1\times M}$ are the direct LoS-dominated channels from Alice to Bob, Bob to Alice, Alice to RIS, Bob to RIS, RIS to Alice and RIS to Bob, respectively. The expressions of these direct channels are detailed in the Simulation section. $\boldsymbol{\epsilon}_A$ and $\boldsymbol{\epsilon}_B$ are the complex Gaussian noises, i.e., $\boldsymbol{\epsilon}_A, \boldsymbol{\epsilon}_B \sim \mathcal{CN}(0, 2\sigma_\epsilon^2 \mathbf{I}_L)$ where $\mathbf{I}_L$ is the identity matrix of size $L \times L$.

The RIS-combined legitimate channel is estimated by Alice and Bob as:

$$\begin{aligned} \hat{h}_A &= \mathbf{u}_B^H \mathbf{y}_A / \|\mathbf{u}_B\|_2^2 = (h_{BA} + \mathbf{h}_{RA} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{BR}) + \hat{\epsilon}_A \\ \hat{h}_B &= \mathbf{u}_A^H \mathbf{y}_B / \|\mathbf{u}_A\|_2^2 = (h_{AB} + \mathbf{h}_{RB} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{AR}) + \hat{\epsilon}_B \end{aligned} \tag{2}$$

where $\hat{\epsilon}_A \sim \mathcal{CN}(0, 2\sigma_\epsilon^2/\|\mathbf{u}_B\|_2^2)$ and $\hat{\epsilon}_B \sim \mathcal{CN}(0, 2\sigma_\epsilon^2/\|\mathbf{u}_A\|_2^2)$ are the estimation errors. Then, the shared secret key can be generated by the small-scale scattering components in $\hat{h}_A$ and $\hat{h}_B$.

It is seen from Eqs. (1)-(2) that in the RIS-secured LoS-dominated Alice and Bob scenarios, the randomness is only from the RIS reflecting phase $\mathbf{w}$, i.e.,

$$h_{ARB} \triangleq \mathbf{h}_{RA} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{BR}. \tag{3}$$

However, such an RIS induced randomness $\mathbf{w}$ is also contained in the Eves' received signals (observations). This thereby enables the design of an eavesdropping scheme to reconstruct the RIS-combined legitimate channel h_{ARB}, and its secret key.

III. Multi-Eavesdropper Scheme

In this section, we elaborate our design of an eavesdropping scheme by $S \in \mathbb{N}^+$ single-antenna Eves (see Fig. 2). Before we start, we list the assumptions as follows:

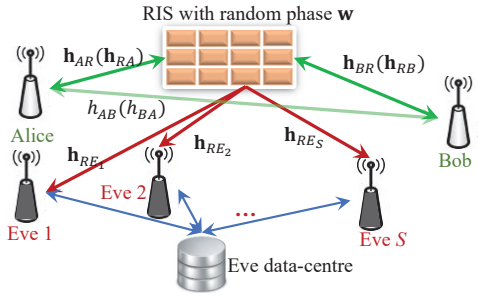

Fig. 2. Illustration of the RIS-secured LoS-dominated channel and our designed multi-Eve scheme to estimate the RIS-combined legitimate channel.

- All the direct channels are LoS-dominated, and are estimated by the LoS components, as one knows the positions (with localization error).
- The positions of Alice, Bob and RIS are known to Eves.

These two assumptions are common in LoS-dominated scenarios (e.g., open-area), where all the direct channels are LoS-dominated, and the radar and camera techniques can be used to locate the legitimate Alice and Bob. Then, the purpose of Eves is to estimate the RIS-combined random legitimate channel h_{ARB} for secret key via their observations.

A. Theory of Eavesdropping Threat

For Eve $s \in \{1, \cdots, S\}$, the observations at odd and even time-slot (sent by Alice and Bob respectively) are:

$$\begin{aligned} \mathbf{z}_s^{(odd)} &= (h_{AE_s} + \mathbf{h}_{RE_s} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{AR}) \cdot \mathbf{u}_A + \boldsymbol{\varepsilon}_s^{(odd)} \\ \mathbf{z}_s^{(even)} &= (h_{BE_s} + \mathbf{h}_{RE_s} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{BR}) \cdot \mathbf{u}_B + \boldsymbol{\varepsilon}_s^{(even)} \end{aligned} \tag{4}$$

where $\mathbf{h}_{RE_s} \in \mathbb{C}^{1\times M}$, $h_{AE_s}, h_{BE_s} \in \mathbb{C}$ are the LoS-donimated direct channels from RIS to Eve s, Alice to Eve s and Bob to Eve s, respectively. $\boldsymbol{\varepsilon}_s^{(odd)}, \boldsymbol{\varepsilon}_s^{(even)} \sim \mathcal{CN}(0, 2\sigma_\varepsilon^2 \mathbf{I}_L)$ are the noise vectors at odd and even time slots.

In Eq. (4), we see that Eves' observations contain the RIS induced channel randomness $\mathbf{w}$. This suggests that conditioned on these observations, when the entropy of RIS-combined legitimate channel is zero, then, Eves are able to reconstruct it. We have following relations:

$$\begin{aligned} & H\left(h_{BA} + h_{ARB} | \mathbf{z}_1^{(odd)}, \mathbf{z}_1^{(even)}, \cdots, \mathbf{z}_S^{(odd)}, \mathbf{z}_S^{(even)}\right) \\ \overset{(a)}{\approx} & H\left(\mathbf{h}_{RA} diag(\mathbf{h}_{BR}) \cdot \mathbf{w}; \begin{bmatrix} \mathbf{H}_{RE} \cdot diag(\mathbf{h}_{AR}) \\ \mathbf{H}_{RE} \cdot diag(\mathbf{h}_{BR}) \end{bmatrix} \cdot \mathbf{w}\right) \overset{(b)}{=} 0, \end{aligned} \tag{5}$$

where $\mathbf{H}_{RE} \triangleq [\mathbf{h}_{RE_1}^H \cdots \mathbf{h}_{RE_S}^H]^H$. In Eq. (5), (a) holds for (i) high signal-to-noise ratio (SNR) of Eves' observations, and (ii) LoS and other static direct channels, i.e., $H(h_{BA}) = 0$. (b) holds if there exists a vector $\mathbf{x} \in \mathbb{C}^{1\times 2N}$ satisfying:

$$\mathbf{h}_{RA} diag(\mathbf{h}_{BR}) = \mathbf{x} \cdot \begin{bmatrix} \mathbf{H}_{RE} \cdot diag(\mathbf{h}_{AR}) \\ \mathbf{H}_{RE} \cdot diag(\mathbf{h}_{BR}) \end{bmatrix}. \tag{6}$$

As such, Eqs. (5)-(6) give a guideline to design eavesdropping scheme for RIS-secured LoS-dominated and other static scenarios. The placement of S Eves should (i) ensure the existence of $\mathbf{x}$, and (ii) map the Eves' observations to the RIS-combined legitimate channel h_{ARB}.

B. Design of Multi-Eve Scheme

Inspired by Eqs. (5)-(6), we design the multi-Eve scheme. Before the start, Eve data-centre virtually meshes the interested area for S Eve deployment into a $N_{\text{grid}} \in \mathbb{N}^+$ grid, and computes the LoS channel from RIS to each nth grid, i.e., $\mathbf{h}_{RG_n}^{(\text{LoS})} \in \mathbb{C}^{1\times M}$. We denote $\mathbf{H}_{\text{grid}} \triangleq [(\mathbf{h}_{RG_1}^{(\text{LoS})})^H, \cdots, (\mathbf{h}_{RG_{N_{\text{grid}}}}^{(\text{LoS})})^H]^H$. Then, with the known of the Alice's and Bob's positions, Eve data-centre will select optimal S grids as Eves' positions, which is implemented by the following three steps.

Step 1: Eve data-centre computes the LoS-dominated direct channels $\mathbf{h}_{AR}$ and $\mathbf{h}_{BR}$ by their LoS components, i.e., $\mathbf{h}_{AR}^{(\text{LoS})}$ and $\mathbf{h}_{BR}^{(\text{LoS})}$, given the known of the positions of Alice, Bob and RIS (see Eq. (19) in Simulation section).

Step 2: Eve data-centre selects a subset $\mathcal{S} \subset \{1, \cdots, N_{\text{grid}}\}$ for the positions of S Eves. This is pursued by the compressed sensing orthogonal matching pursuit (OMP) [21] of:

$$\mathbf{h}_{RA}^{(\text{LoS})} diag\left(\mathbf{h}_{BR}^{(\text{LoS})}\right) = \tilde{\mathbf{x}} \cdot \begin{bmatrix} \mathbf{H}_{\text{grid}} \cdot diag\left(\mathbf{h}_{AR}^{(\text{LoS})}\right) \\ \mathbf{H}_{\text{grid}} \cdot diag\left(\mathbf{h}_{BR}^{(\text{LoS})}\right) \end{bmatrix}, \quad s.t., \ \|\tilde{\mathbf{x}}\|_0 = 2S. \tag{7}$$

From Eq. (7), $\mathcal{S}$ can be selected as:

$$\mathcal{S} = \{n | \tilde{x}_n \neq 0, n \leq N_{\text{grid}}\} \bigcup \{n - N | \tilde{x}_n \neq 0, n > N_{\text{grid}}\}, \tag{8}$$

where $\tilde{x}_n$ is the nth element of $\tilde{\mathbf{x}}$. Then, Eve data-centre tells S Eves to adjust their positions to S selected grids. By this way, a small S (e.g., $S \leq 10$ in Fig. 4) is able to estimate the RIS combined legitimate channel, which is feasible when the number of RIS elements is large (e.g., $M \sim 10^2$ [20].)

Step 3: After gathered the observations from S Eves, Eve data-centre stacks them as $\boldsymbol{\zeta}^{(odd)} \triangleq [(\boldsymbol{\zeta}_1^{(odd)})^H, \cdots, (\boldsymbol{\zeta}_S^{(odd)})^H]^H$ and $\boldsymbol{\zeta}^{(even)} \triangleq [(\boldsymbol{\zeta}_1^{(even)})^H, \cdots, (\boldsymbol{\zeta}_S^{(even)})^H]^H$. Here, for each $s \in \mathcal{S}$, $\boldsymbol{\zeta}_s^{(odd)}$ and $\boldsymbol{\zeta}_s^{(even)}$ are:

$$\zeta_s^{(odd)} = \mathbf{u}_A^H \cdot \left(\mathbf{z}_s^{(odd)} - h_{AE_s}^{(\text{LoS})} \cdot \mathbf{u}_A\right) / \|\mathbf{u}_A\|_2^2$$
$$\zeta_s^{(even)} = \mathbf{u}_B^H \cdot \left(\mathbf{z}_s^{(even)} - h_{BE_s}^{(\text{LoS})} \cdot \mathbf{u}_B\right) / \|\mathbf{u}_B\|_2^2.$$

where $h_{AE_s}^{(\text{LoS})}$ and $h_{BE_s}^{(\text{LoS})}$ are computed by their LoS component. Then, the RIS-combined legitimate channel h_{ARB} can be estimated by the sub-vector of the non-zero elements in $\tilde{\mathbf{x}}$, denoted as $\hat{\mathbf{x}}$, and the stacked observations, i.e.,

$$\hat{h}_E = \hat{\mathbf{x}} \cdot \begin{bmatrix} \boldsymbol{\zeta}^{(odd)} \\ \boldsymbol{\zeta}^{(even)} \end{bmatrix} = h_{ARB} + \boldsymbol{\eta} \cdot \mathbf{w} + \tilde{\mathbf{x}} \cdot \boldsymbol{\varepsilon} \tag{9}$$

where $\boldsymbol{\eta}$ of size $1 \times M$ is the deviation vector by taking $\hat{\mathbf{x}}$ into Eq. (6). $\boldsymbol{\varepsilon} \triangleq [\varepsilon_1^{(odd)}, \cdots, \varepsilon_S^{(odd)}, \varepsilon_1^{(even)}, \cdots, \varepsilon_S^{(even)}]^T$, with independent elements $\varepsilon_s^{(odd)} \sim \mathcal{CN}(0, 2\sigma_\varepsilon^2/\|\mathbf{u}_A\|_2^2)$ and $\varepsilon_s^{(even)} \sim \mathcal{CN}(0, 2\sigma_\varepsilon^2/\|\mathbf{u}_B\|_2^2)$ is the stacked noise component.

As such, the designed multi-Eves can decode the secret key via the reconstructed RIS-combined legitimate channel. The computational complexity is measured via the number of multiplications, i.e., $O(SMN_{\text{grid}}+LS)$, including $(N_{\text{grid}}+2)M$ for step 1, $2SMN_{\text{grid}}$ for the OMP in step 2, and $6LS+2S$ for step 3. The designed multi-Eve scheme has a larger computational complexity as opposed to the legitimate channel estimation at Alice and Bob, i.e., $O(SMN_{\text{grid}} + LS) > O(L)$.

C. Secret Key Leakage Analysis

In this part, we analyze the secret key leakage rate of our designed multi-Eve scheme, which is defined as $I(\hat{h}_E; \hat{h}_A)$ (or $I(\hat{h}_E; \hat{h}_B)$). We express $I(\hat{h}_E; \hat{h}_A)$ via the information entropy, i.e.,

$$I\left(\hat{h}_E; \hat{h}_A\right) = H\left(\hat{h}_E\right) + H\left(\hat{h}_A\right) - H\left(\hat{h}_E, \hat{h}_A\right). \tag{10}$$

To compute Eq. (10), we need to derive the probability distribution of $\hat{h}_E$ and $\hat{h}_A$, and also their correlation.

We firstly compute the distribution of legitimate channel:

$$h_{ARB} \sim \mathcal{CN}(0, 2\iota^2). \tag{11}$$

where $\iota^2 \triangleq \|\mathbf{h}_{RA} \cdot diag(\mathbf{h}_{BR})\|_2^2/2$. The reason of using a complex Gaussian distribution is central limit theorem, given the large number of RIS elements (e.g., $M \sim 10^2$). The mean and variance are computed given the distribution of $\mathbf{w}$.

Then, according to Eq. (2) and Eq. (9), we have:

$$[\hat{h}_A, \hat{h}_E] \sim \mathcal{CN}\left([h_{BA}, 0], 2\boldsymbol{\Sigma}_{\hat{h}_A, \hat{h}_E}\right) \tag{12}$$

$$\boldsymbol{\Sigma}_{\hat{h}_A, \hat{h}_E} = \begin{bmatrix} \iota^2 + \sigma_\epsilon^2/\|\mathbf{u}_B\|_2^2 & \iota^2 + \varpi/2 \\ \iota^2 + \varpi^*/2 & \iota^2 + \varsigma^2 \end{bmatrix}, \tag{13}$$

where $\boldsymbol{\Sigma}_{\hat{h}_A, \hat{h}_E}$ is the co-variance matrix of $\hat{h}_A$ and $\hat{h}_E$, with $\varpi \triangleq \mathbf{h}_{RA} diag(\mathbf{h}_{BR}) \boldsymbol{\eta}^H$. ς^2 is the variance of estimation error of the RIS-combined legitimate channel h_{ARB} from Eves:

$$\begin{aligned} \varsigma^2 \triangleq & \|\tilde{\mathbf{x}}_{1:S}\|_2^2 \cdot \sigma_\varepsilon^2/\|\mathbf{u}_A\|_2^2 + \|\tilde{\mathbf{x}}_{S+1:2S}\|_2^2 \cdot \sigma_\varepsilon^2/\|\mathbf{u}_B\|_2^2 \\ & + Re[\varpi] + \|\boldsymbol{\eta}\|_2^2/2. \end{aligned} \tag{14}$$

where $Re[\varpi]$ is the real-part of ϖ.

With the help of Eqs. (12)-(13), we use the formula, i.e., $H(X, \cdots, X_D) = 1/2 \log_2((2\pi e)^D det(\boldsymbol{\Sigma}))$ with $\boldsymbol{\Sigma}$ the co-variance matrix of random variables $X_1, \cdots, X_D$ ($D \in \mathbb{N}^+$), to compute the information entropy in Eq. (10), i.e.,

$$H\left(\hat{h}_A\right) = \frac{1}{2} \log_2 2\pi e \left(\iota^2 + \sigma_\epsilon^2/\|\mathbf{u}_B\|_2^2\right), \tag{15}$$

$$H\left(\hat{h}_E\right) = \frac{1}{2} \log_2 2\pi e \left(\iota^2 + \varsigma^2\right), \tag{16}$$

$$H(\hat{h}_E, \hat{h}_A) = \frac{1}{2} \log_2 4\pi^2 e^2 det\left(\boldsymbol{\Sigma}_{\hat{h}_A, \hat{h}_E}\right). \tag{17}$$

Finally, by taking Eqs. (15)-(17) into Eq. (10), we derive the secret key leakage rate, i.e.,

$$I\left(\hat{h}_E; \hat{h}_A\right) = -\frac{1}{2} \log_2 \left(1 - \frac{|\iota^2 + \varpi/2|^2}{(\iota^2 + \varsigma^2)(\iota^2 + \sigma_\epsilon^2/\|\mathbf{u}_B\|_2^2)}\right). \tag{18}$$

From Eq. (18), it is seen that the secret key leakage rate $I(\hat{h}_E; \hat{h}_A)$ will increase with the decrease of the variance of Eves' channel estimation error, i.e., ς^2. Specially, when such estimation error is less than that of Bob, i.e., $\varsigma^2 < \sigma_\epsilon^2/\|\mathbf{u}_A\|_2^2$, the secret key leakage rate will exceed the mutual information between Alice's and Bob's estimated channels, i.e., $I(\hat{h}_E; \hat{h}_A) > I(\hat{h}_A; \hat{h}_B)$. This is further shown by simulations.

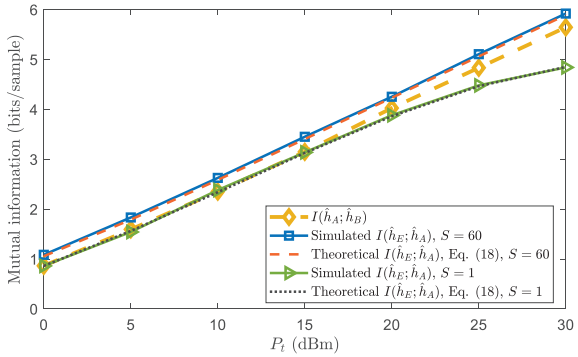

Fig. 3. Secret key leakage rate of multi-Eve v.s. transmitted power.

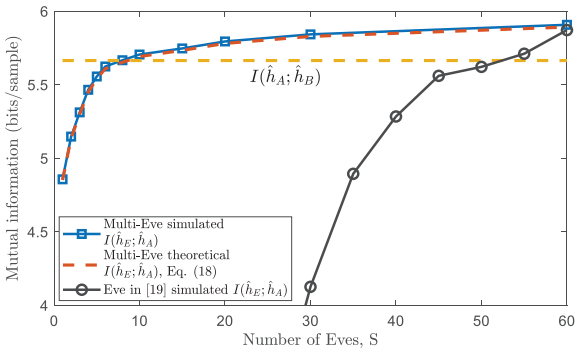

Fig. 4. Secret key leakage rate v.s. number of Eves.

IV. Experimental Simulations

In this section, we evaluate our designed multi-Eve scheme. The RIS-secured LoS-dominated channel model is configured in the following. In a 3D space, Alice, Bob and RIS are located at $(0, 0, 50)$, $(0, 80, 40)$, and $(10, 50, 20)$, with unit m. The number of RIS elements is assigned as $M = M_x \times M_y = 10 \times 10 = 100$. The area for Eve deployment is $\{[0, 50], [10, 70], 0\}$ with unit m, which Eve data-centre meshes by $N_{\text{grid}} = 30 \times 30$ grids. The length of pilot signals is $L = 50$. The received signal noise for Alice, Bob and Eves are set as $\sigma_\epsilon^2 = \sigma_\varepsilon^2 = -110dBm$. All the LoS-dominated direct channels are formulated according to [18], [22], i.e.,

$$\begin{aligned}
\mathbf{h}_{Ra} &= \mathbf{h}_{Ra}^{(\text{LoS})} + \boldsymbol{\psi}_{Ra}, \\
\mathbf{h}_{Ra}^{(\text{LoS})} &= \sqrt{C_0 d_{Ra}^{-\alpha_{Ra}}}[\exp(ju0), \cdots, \exp(ju(M_x-1))] \\
&\quad \otimes [\exp(jv0), \cdots, \exp(jv(M_y-1))], \\
h_{ab} &= \mathbf{h}_{ab}^{(\text{LoS})} + \psi_{ab}, \\
h_{ab}^{(\text{LoS})} &= \sqrt{C_0 d_{ab}^{-\alpha_{ab}}}, \ a \neq b \in \{A, B, E_1, \cdots, E_N\}. \quad (19)
\end{aligned}$$

In Eq. (19), $\boldsymbol{\psi}_{Ra}$ and ψ_{ab} are complex Gaussian random variables accounting for NLoS component and LoS channel estimating error. $u \triangleq \pi \cos(el_{Ra})$ and $v \triangleq \pi \sin(el_{Ra}) \sin(az_{Ra})$ with el_{Ra}, az_{Ra}, and d_{Ra} the elevation angle, the azimuth angle, and the distance. $C_0 = -30$dBw is the path loss at the reference distance (i.e., 1m), and $\alpha_{Ra} = \alpha_{ab} = 2.3$ are the path-loss exponents.

A. Secret Key Leakage Rate

We first evaluate the secret key leakage rate of our designed multi-Eve scheme, i.e., $I(\hat{h}_E; \hat{h}_A)$, under perfect LoS link. In Fig. 3, it is firstly seen that with the increase of the transmitted power P_t, both the secret key and leakage rates increase, since the rates rely on the accuracy of channel estimation, which increases as the transmitted power grows. Then, we see that the secret key leakage rate of our scheme, i.e., $I(\hat{h}_E; \hat{h}_A)$ is close to the mutual information of Alice's and Bob's estimated channels, i.e., $I(\hat{h}_A; \hat{h}_B)$. This can be further observed from Fig. 4. As the number of Eves, i.e., S grows, $I(\hat{h}_E; \hat{h}_A)$ increases and even exceeds $I(\hat{h}_A; \hat{h}_B)$ (e.g., when $S = 10$ Eves are used). This is because a larger number of Eves' observations leads to a smaller estimation error of the RIS-combined legitimate channel by Eves, which subsequently gives rise to a larger $I(\hat{h}_E; \hat{h}_A)$. When such estimation error is smaller than that of legitimate nodes, i.e., $\varsigma^2 < \sigma_\epsilon^2 / \|\mathbf{u}_A\|_2^2$, we have $I(\hat{h}_E; \hat{h}_A) > I(\hat{h}_A; \hat{h}_B)$, as explained in Eq. (18).

In Fig. 4, we also compare our designed multi-Eve scheme with the cooperative eavesdropping scheme in [19]. It is seen that our multi-Eve scheme can use a smaller number of Eves to achieve a comparable secret key leakage rate with [19], e.g., $S = 10$ v.s. $S = 60$ Eves for a same $I(\hat{h}_E; \hat{h}_A) = 5.62$. We explain this gap from the theoretical perspective we leveraged. Our multi-Eve scheme maps the S Eves' observations to the low-dimensional space of RIS-combined legitimate channel, i.e., $h_{ARB} \in \mathbb{C}$. This thereby leads to a smaller number of Eves, as opposed to the scheme in [19], which tries to find an over-determined equation from Eves' observations to the high-dimensional RIS phase space $\mathbb{C}^M$.

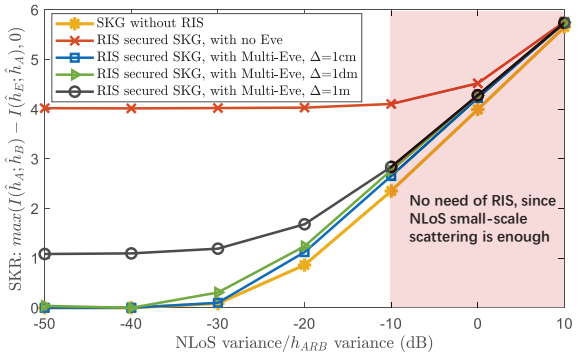

Fig. 5. Performance with LoS channel estimating error and NLoS component.

B. With LoS Channel Estimation Error and NLoS Component

We then test our designed multi-Eve scheme with (i) the direct LoS channel estimation error caused by cm, dm and m levels of localization errors, and (ii) the small-scale NLoS fading components. In Fig. 5, x-coordinate is the variance ratio between the small-scale NLoS component and the RIS-combined legitimate channel h_{ARB}, while y-coordinate is the secret key rate, i.e., $\max\{I(\hat{h}_A; \hat{h}_B) - I(\hat{h}_E; \hat{h}_A), 0\}$.

It is firstly seen that with the increase of the NLoS component variance, the SKRs of all SKG scenarios (with and without RIS and our designed multi-Eve) increase, since a

larger variance of NLoS component means more sufficient small-scale randomness for key generation. When the variance of NLoS component approaches to that of the RIS-combined legitimate channel (red zone), there is no need to use RIS for PL-SKG, since the NLoS small-scale scattering induced randomness is enough for key generation, e.g., the gap between SKGs with and without RIS (red and yellow curves) is close.

Then, it is seen that our proposed multi-Eve scheme can neutralize the security gain induced by RIS. For example, when the NLoS variance is low (e.g., NLoS variance / RIS-combined channel variance is less than $-30dB$), the SKR is improved from 0 (yellow curve) to 4 (red curve) by using RIS to increase the phase randomness. However, under our proposed multi-Eve scheme, such SKRs decrease back to 0, with LoS channel estimation errors caused by dm (green curve) and cm (blue curve) levels of localization errors. This therefore suggests the eavesdropping ability of our proposed multi-Eve scheme against the RIS-secured SKG.

V. Conclusion

PL-SKG leverages the reciprocal channel randomness, and provides an additional layer of security for wireless communications. In low-entropy channel with a lack of small-scale fading and randomness (e.g., static or LoS scenarios), RIS has been proved to be able to generate randomness for sufficient key generation. However, current studies overlook that the RIS-induced randomness is also contained in the Eves' received signals, which thereby paves the way for a design of sophisticated eavesdropping scheme to estimate the RIS-combined legitimate random channel and further decode the secret key relying on it.

In this letter, we designed the cooperative multi-Eve scheme against the RIS-secured PL-SKG in LoS-dominated scenarios. The scheme estimates the RIS-combined legitimate channel by making the entropy of legitimate channel conditioned on Eves' signals approaches to zero. The theoretical secret key leakage rate of our designed scheme was deduced. Shown by the numerical results, our multi-Eve scheme can use less than 10 collaborative Eves to estimate the legitimate channel secured by 100 RIS elements. This therefore demonstrates the eavesdropping capacity of our designed multi-Eve scheme against the RIS-secured PL-SKG. In future work, more researches should be conducted on collaborative eavesdropper cases when proposing appropriate RIS-secured PL-SKG schemes.

References

[1] H.-M. Wang, X. Zhang, and J.-C. Jiang, "Uav-involved wireless physical-layer secure communications: Overview and research directions," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 32–39, 2019.

[2] C. Huang, G. Chen, and K.-K. Wong, "Multi-agent reinforcement learning-based buffer-aided relay selection in irs-assisted secure cooperative networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4101–4112, 2021.

[3] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 375–388, 2021.

[4] W. Wang, X. Liu, J. Tang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, "Beamforming and jamming optimization for irs-aided secure noma networks," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2021.

[5] X. Pang, N. Zhao, J. Tang, C. Wu, D. Niyato, and K.-K. Wong, "Irs-assisted secure uav transmission via joint trajectory and beamforming design," *IEEE Transactions on Communications*, pp. 1–1, 2021.

[6] W. Jiang, B. Chen, J. Zhao, Z. Xiong, and Z. Ding, "Joint active and passive beamforming design for the irs-assisted mimome-ofdm secure communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 10, pp. 10 369–10 381, 2021.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[8] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[9] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *2006 IEEE International Symposium on Information Theory*, 2006, pp. 2593–2597.

[10] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[11] X. Wu, Y. Song, C. Zhao, and X. You, "Secrecy extraction from correlated fading channels: An upper bound," in *2009 International Conference on Wireless Communications Signal Processing*, 2009, pp. 1–3.

[12] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020.

[13] G. Li, L. Hu, P. Staat, H. Elders-Boll, C. Zenger, C. Paar, and A. Hu, "Reconfigurable intelligent surface for physical layer key generation: Constructive or destructive?" *arXiv preprint arXiv:2112.10043*, 2021.

[14] X. Hu, L. Jin, K. Huang, X. Sun, Y. Zhou, and J. Qu, "Intelligent reflecting surface-assisted secret key generation with discrete phase shifts in static environment," *IEEE Wireless Communications Letters*, vol. 10, no. 9, pp. 1867–1870, 2021.

[15] X. Lu, J. Lei, Y. Shi, and W. Li, "Intelligent reflecting surface assisted secret key generation," *IEEE Signal Processing Letters*, vol. 28, pp. 1036–1040, 2021.

[16] Z. Ji, P. L. Yeoh, G. Chen, C. Pan, Y. Zhang, Z. He, H. Yin, and Y. Li, "Random shifting intelligent reflecting surface for otp encrypted data transmission," *IEEE Wireless Communications Letters*, vol. 10, no. 6, pp. 1192–1196, 2021.

[17] P. Staat, H. Elders-Boll, M. Heinrichs, R. Kronberger, C. Zenger, and C. Paar, "Intelligent reflecting surface-assisted wireless key generation for low-entropy environments," *arXiv preprint arXiv:2010.06613*, 2020.

[18] Z. Ji, P. L. Yeoh, D. Zhang, G. Chen, Y. Zhang, Z. He, H. Yin, and Y. li, "Secret key generation for intelligent reflecting surface assisted wireless communication networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 1030–1034, 2021.

[19] Z. Wei and W. Guo, "Random matrix based physical layer secret key generation in static channels," *arXiv preprint arXiv:2110.12785*, 2021.

[20] C. Pan, H. Ren, K. Wang, J. F. Kolb, M. Elkashlan, M. Chen, M. Di Renzo, Y. Hao, J. Wang, A. L. Swindlehurst, X. You, and L. Hanzo, "Reconfigurable intelligent surfaces for 6g systems: Principles, applications, and research directions," *IEEE Communications Magazine*, vol. 59, no. 6, pp. 14–20, 2021.

[21] T. Zhang, "Sparse recovery with orthogonal matching pursuit under rip," *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 6215–6221, 2011.

[22] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5394–5409, 2019.