Reconfigurable Intelligent Surface-Assisted Secret Key Generation Under Spatially Correlated Channels in Quasi-Static Environments

Vahid Shahiri, Hamid Behroozi, *Member, IEEE* and Ali Kuhestani, *Member, IEEE*, Kai-Kit Wong, *Fellow, IEEE*

***Abstract*—Physical layer key generation (PLKG) can significantly enhance the security of classic encryption schemes by enabling them to change their secret keys significantly faster and more efficiently. However, due to the reliance of PLKG techniques on channel medium, reaching a high key generation rate (KGR) is challenging in quasi-static environments. Recently, exploiting reconfigurable intelligent surface (RIS) as a means to induce randomness in quasi-static wireless channels has received significant research interest. However, the impact of spatial correlation between the RIS elements is rarely studied. To be specific, for the first time, in this contribution, we take into account a spatially correlated RIS which intends to enhance the KGR in a quasi-static medium. Closed-form analytical expressions for KGR are derived for the two cases of random phase shift (RPS) and equal phase shift (EPS) in the RIS elements. We also analyze the temporal correlation between the channel samples to ensure the randomness of the generated secret key sequence. It is shown that the EPS scheme can effectively exploit the inherent spatial correlation between the RIS elements and it leads to a higher KGR compared to the widely used RPS strategy. We further formulate an optimization problem in which we determine the optimal portion of time dedicated to direct and indirect channel estimation within a coherence time. We show the accuracy and the fast convergence of our proposed sequential convex programming (SCP) based algorithm and discuss the various parameters affecting spatially correlated RIS-assisted PLKG.**

***Index Terms*—Physical layer secret key generation, spatial correlation, reconfigurable intelligent surface (RIS), achievable key generation rate**

I. Introduction

WIRELESS communications medium is intrinsically prone to malicious eavesdropping attempts due to its broadcast nature. With the emergence of dense and widely distributed wireless networks, e.g., sixth generation mobile communications (6G) and Internet of Things (IoT), seeking a lightweight security approach which is able to combat the emerging modern threats has become crucial. Traditionally, the security is preserved by utilizing symmetric key cryptography (SKC) techniques such as stream ciphers, data encryption standard (DES) [1] and advanced encryption standard (AES) [2] or by using asymmetric key cryptography (AKC) methods such as Rivest-Shamir-Adleman (RSA) [3] scheme. These higher layer security schemes had tremendous contributions in maintaining the confidentiality of communications over the previous decades. However, these encryption methods need to get boosted with physical layer security (PLS) techniques to cope with the emerging threats in modern networks.

PLS solutions are comprised of two main categories, namely key-less and key-based techniques. Key-less research techniques are pioneered by Wyner in his seminal work [4] where he formulated the secrecy capacity. To be specific, in key-less techniques no encryption is involved and the information secrecy is achieved if and only if the legitimate receiver has better channel quality than the eavesdropper. So far, numerous key-less PLS techniques are proposed in the literature including secure beamforming [5], relay-based techniques [6], power allocation schemes [7], covert methods [8], [9], etc. However, key-less secure transmission usually requires complex code design and accurate channel state information (CSI) which may not be available mainly when a passive eavesdropper is considered [10], [11]. Accordingly, the key-based techniques which still exploit the merits of classical encryption schemes are widely considered in numerous studies with applications in IoT [12], relay channels [13], etc.

Classic encryption schemes suffer from two major drawbacks. Specifically, the AKC methods are not preferred in networks with limited resources in their nodes, e.g., in IoT. This is because AKC demands high computational resources due to its complex mathematical operations. Thus SKC is a more desirable option for IoT networks due to its low-complexity implementation [14]. However, SKC requires the encryption keys to be distributed among the nodes before they start transferring data. This key generation process requires a complicated structure to generate and distribute the common keys between the nodes of a widely distributed network. In these cases, physical layer key generation (PLKG) techniques can be utilized to generate and distribute the random keys between the nodes [10]. These techniques exploit the reciprocal characteristics of wireless channels as great sources of common randomness to generate random keys [15]. Another drawback is the vulnerability of classic schemes to quantum computer attacks [16]. The AKC methods rely on complex mathematical algorithms that are not scalable and thus are easily broken by a quantum computer. However, SKC schemes can be enhanced by increasing the length of the encryption keys [16]. PLKG techniques again come in handy here to help

V. Shahiri and H. Behroozi are with the Electrical Engineering Department, Sharif University of Technology, Tehran, Iran. E-mail: vahid.shahiri@ee.sharif.edu, behroozi@sharif.edu

A. Kuhestani is with the Electrical and Computer Engineering Department, Qom University of Technology, Qom, Iran. Email: kuhestani@qut.ac.ir

Kai-Kit Wong is with the Department of Electronic and Electrical Engineering, University College London, UK. (e-mail: kai-kit.wong@ucl.ac.uk).

the SKC generate long random sequences of keys to boost its strength in combating quantum computer attacks [10].

Generally, the PLKG process comprises four phases, i.e., random sharing, quantization, information reconciliation and privacy amplification [15]. During the random sharing phase, the two parties exchange pilots in a time-division duplex (TDD) mode to estimate the channel coefficients and exploit them as their source of common randomness. These real value coefficients are then converted to binary sequences through the quantization process [17]. Generally, the mismatches occur during the channel estimation process of the parties. The two nodes use methods such as cosets of binary linear codes to compensate for these mismatches in the information reconciliation phase [18]. Finally, in the privacy amplification phase, the possible leakage of the generated keys to the eavesdroppers in the previous steps is wiped out [19]. These four steps highlight that PLKG relies on the reciprocity of physical medium characteristics to generate identical keys in two nodes and its security is guaranteed by the inherent randomness in the physical medium.

The randomness of the generated key is a vital requirement guaranteed by the temporal decorrelation between the sampled channel coefficients [20]. Temporal decorrelation can be achieved in wireless networks with mobility in their nodes or surroundings. However, this requirement is not fulfilled in static environments such as IoT networks [21]. Moreover, the mobility level in the wireless medium may not be adequate to generate secret keys at a high rate. Accordingly, [21]–[23] have proposed various solutions to overcome the slow rate of PLKG in static environments. Specifically, in [21] the end users deploy random pilot constellations to induce randomness in the received signals. The authors in [22], induce randomness in multiple-input-multiple-output (MIMO) by designing random precoding vectors. In [23], the correlated eavesdropper channel is scrambled by utilizing artificial noise. All these studies focus on inducing randomness at user ends to enhance the key generation rate (KGR).

Very recently, increasing the rate of channel randomness by reconfigurable intelligent surface (RIS) has received extensive research interest [24]–[30]. Specifically, In [24], the authors initially proposed exploiting the random shifts in RIS elements to induce randomness in the wireless channel and increase the KGR in quasi-static environments. They argue that this method paves the way to the perfectly secure one-time pad (OTP) communications. A four-step protocol is designed in [25] to add randomness in a quasi-static environment. In the proposed protocol, the direct and reflective paths are estimated at each coherence time of the channel and their randomness is also exploited to enhance the KGR. In [26], the authors proposed an attack model consisting of several eavesdroppers which aim to jeopardize the RIS-assisted PLKG in a quasi-static line-of-sight (LoS) dominated channel. In [27], the potential of RIS-induced randomness in millimeter wave communications is studied. The authors in [28] have considered designing pilot signals based on random matrix theory for RIS-assisted PLKG in quasi-static environments. This method avoids the leakage of generated secret keys to the eavesdropper caused due to using globally known pilot signals. In [29], the theoretical boundaries for KGR by assuming discrete phase shifts in RIS elements are studied. Finally, the authors in [30] have performed the first practical study on RIS-assisted PLKG in quasi-static environments. They showed that their implemented scheme achieves 97.39 bps KGR while passing standard randomness tests. In our proposed system model, we consider the practical issue of spatial correlation present between the RIS elements. We note that none of the above studies has considered spatial correlation in RIS in their system models.

In another research line, the RIS is deployed to enhance the KGR by assisting the transceivers in conveying their signals [31]–[34]. Specifically, the authors in [31] have derived the minimum achievable KGR and developed an optimization framework for the RIS reflecting coefficients to maximize the derived secret key capacity lower bound. In [32], the KGR expression for the RIS-assisted PLKG is deduced. The authors in [33], have considered a scenario in which a base station intends to generate secret keys with multiple user terminals (UTs) when the direct path is blocked and the signals are conveyed with an RIS. The two cases of independent and correlated channels between the UTs are studied and KGR maximization frameworks have been proposed for the two cases. Moreover, in [34], the KGR improvement through deploying RIS when the two nodes are equipped with multiple antennas is considered. The authors have proposed an optimization algorithm to maximize KGR by designing the RIS passive beamforming. Additionally, [35] and [36] view the RIS as an attacker to the PLKG schemes. In [35], after studying the constructive aspects of deploying RIS in PLKG, i.e. in quasi-static and wave-blockage environments, the authors argue that an attacker can utilize the IRS to perform jamming and leakage attacks. Furthermore, the authors in [36], proposed an attack model in which an RIS reduces the wireless channel reciprocity by rapidly changing the RIS reflection coefficients in the uplink and downlink channel probing steps. A method to detect and counteract this attack is also proposed.

All the reviewed studies on RIS-assisted PLKG assume independent reflective channels in RIS. Recently, the spatial correlation between the RIS elements is modeled in [37]. The authors argue that any RIS deployed in a two-dimensional rectangular grid is subject to spatially correlated fading. This property holds for any practical RIS since it is by definition two-dimensional. The model has been widely used to consider the practical aspects of RIS deployment [38]–[43]. For the first time in this contribution, we investigate the impact of spatial correlation between the RIS elements in PLKG for quasi-static environments. The presence of spatial correlation in RIS elements makes our mathematical analysis of KGR challenging compared to the state-of-the-art. Furthermore, we offer an optimization framework for KGR which basically explores the intrinsic limitation in deploying the RIS to reach OTP encryption in quasi-static wireless environments. The main contributions of this paper are summarized as follows:

- We consider a spatially correlated RIS which randomly changes the phases of its elements to induce artificial randomness in the quasi-static environment. This is the first time that the spatial correlation between the RIS

elements is considered in such an application.

- We study the two cases of random phase shift (RPS) for all the elements and equal phase shift (EPS) in every change of the phase of the elements and extract the KGR for each of these cases. It is the first time that the random equal phase shift in each phase change is considered in an RIS aided PLKG scenario for quasi-static environments. It is shown that the EPS scheme effectively exploits the inherent spatial correlation in the RIS elements. This scheme results in better KGR and improved randomness in the generated secret key sequence. However, the widely used RPS strategy mimics the behavior of the hypothetically independent channel model for the RIS and fails to exploit the spatial correlation between the RIS elements.
- Due to the presence of spatial correlation, it is not possible to directly incorporate the central limit theorem (CLT). Accordingly, we present a mathematical framework which finally leads to deriving a closed-form expression for KGR.
- To glean further insights, we derive the temporal correlation between the two channel samples for both of the above cases. We show that unlike the results presented in the literature, when the realistic RIS model is deployed, it is needed to subtract the direct channel from the indirect channel samples to generate a random secret key.
- We propose to generate secret keys from both direct and indirect probings and formulate an optimization problem to derive the optimum choice of dedicated time to direct and indirect probings and the optimum number of times that the RIS should change the phase of its arrays to maximize KGR. We propose a sequential convex programming (SCP) algorithm which is shown to be accurate and fast converging.

The symbols used in this paper are listed in Table I. The remainder of this paper is organized as follows. In Section II, we introduce our system model and the main parameters used. In Section III, we calculate the correlation between the channel samples used for PLKG for both EPS and RPS schemes. The expression for the upper bound of KGR with spatially correlated RIS is derived in Section IV. Moreover, we formulate our optimization problem to maximize the KGR in Section V. Our numeric results are presented in Section VI, while our conclusions are offered in Section VII.

II. System Model

In our proposed secret key generation (SKG) system model, Alice and Bob as legitimate users, aim to generate identical secret keys over the public channel in the presence of a passive eavesdropper (Eve), as shown in Fig. 1. Alice, Bob and Eve are all equipped with a single antenna. Due to the relatively large coherence time in the channel between Alice and Bob, an RIS (Rose) assists them with increasing the KGR. Alice and Bob probe the channel in TDD mode to acquire correlated measurements of the shared channel to extract secret keys. Through this process, Eve strives to obtain information on the generated secret key by listening to Alice and Bob's transmissions over the public channel. The RIS with the spatial correlation between its elements acts as a trusted node trying to enhance the KGR by randomly shifting the phase of its elements. By doing this, the RIS is able to induce a virtual fast fading channel and introduce artificial randomness to the propagation environment.

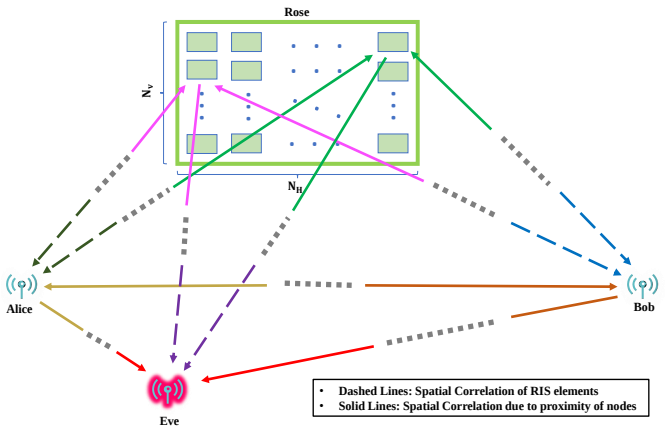

Fig. 1: System model: A spatially correlated RIS aids Alice and Bob to generate secret keys from the quasi-static wireless channel in the presence of a passive eavesdropper. Lines with the same colors represent correlated paths.

We assume the channels between the nodes are block-fading Rayleigh channels with coherence time T_c. This means through the time interval T_c, the channel coefficients remain constant. As shown in Fig. 2, to fully exploit the randomness induced by RIS, we design a protocol consisting of two steps, namely the direct channel estimation and the aggregate randomly configured sub-reflecting channel estimation. Specifically, we first estimate the direct channel to exploit its randomness. Moreover, these measurements will also be used in step two to mitigate the influence of the direct channel. Later in Section III, we will show this can lead to have a negligible correlation between two probings of Alice and Bob. We assume that the time assigned for direct channel probing by each of the legitimate parties is equal to $T_d = T_{los}/2$, $(T_{los} < T_c)$.

We further assume that the RIS has N reflecting elements and during step two for each channel coherence time, it changes the phase of these elements P times. Accordingly, the effective coherence time of the resulting propagation medium becomes $T_e = \frac{T_r}{P}$, where T_r is the time assigned for key generation from aggregate randomly configured sub-reflecting channel, $(T_r < T_c)$. This means to generate identical secret keys, Alice and Bob should exchange pilot signals during the time interval T_e in which the propagation environment parameters are the same for both of them. They send pilots during each time slot which is equal to $T_s = \frac{T_e}{2}$ and take turns in sending pilot signals, i.e. Alice sends pilots in even time slots, and Bob sends his pilots in odd time slots. After all, the pilot exchange phase in step two takes $T_r = PT_e = 2PT_s$ long. The remaining $T_m = T_c - T_{los} - T_r$ time is dedicated to exchanging the data encrypted by using keys generated from

Table I: List of symbols

Symbol	Description	Symbol	Description
T_c	Coherence time of wireless quasi-static channel	T_m	Encrypted data exchange time
T_{los}	Direct channel probing time	T_d	Direct channel probing time for each party
T_r	Aggregate randomly configured sub-reflecting channel probing time	T_s	Time slot duration for probing the randomly induced channel
T_e	Effective coherence time of the randomly configured channel	T_p	Direct and aggregate randomly configured sub-reflecting channels probing time
P	Number of times the phase of the RIS elements change within a coherence time	N	Number of RIS elements
P_a	Transmit power of Alice	P_b	Transmit power of Bob
h_{ij}	Direct channel coefficient between nodes i and j	$\mathbf{n}_{i,j}$	Noise vector in receiver i at phase j during the step 1
$\mathbf{x}_d$	Public pilot used for the direct channel probing	$\mathbf{x}_r$	Public pilot used for the randomly configured sub-reflecting channel probing
σ_{ij}^2	Variance of the channel between nodes i and j	σ_i^2	Variance of noise at node i
$\hat{h}_{ij}$	Estimated direct channel between nodes i and j during the step 1	$\hat{n}_{i,j}/\hat{\sigma}_{i,j}^2$	Channel estimation noise term/variance at node i in phase j during the step 1
$\mathbf{h}_{ri}$	Sub-reflective channel vector between node i and RIS	$\mathbf{n}_i^p$	Noise vector for receiver i in p-th round of phase change during the step 2
$\mathbf{\Phi}^p$	Diagonal phase shift matrix of RIS in p-th round of phase change	ϕ_i^p	Phase of i-th element of RIS in p-th round of phase change
$\hat{h}_i^p$	Estimated aggregate direct and sub-reflecting channels in p-th round of phase change	$\hat{n}_i^p/\hat{\sigma}_i^2$	Aggregate direct and sub-reflecting channels estimation noise term/variance at node i
h_i^p	Estimated aggregate sub-reflecting channel in p-th round of phase change	$\hat{z}_i^p/\hat{\sigma}_{z_i}^2$	Aggregate sub-reflecting channel estimation noise term/variance at node i
$\mathbf{R}_{ij}$	Correlation matrix of RIS elements and node i	ρ^t	Maximum permissible correlation
d_H/d_V	vertical height/ horizontal width of RIS elements	N_H/N_V	Elements per row/column of RIS

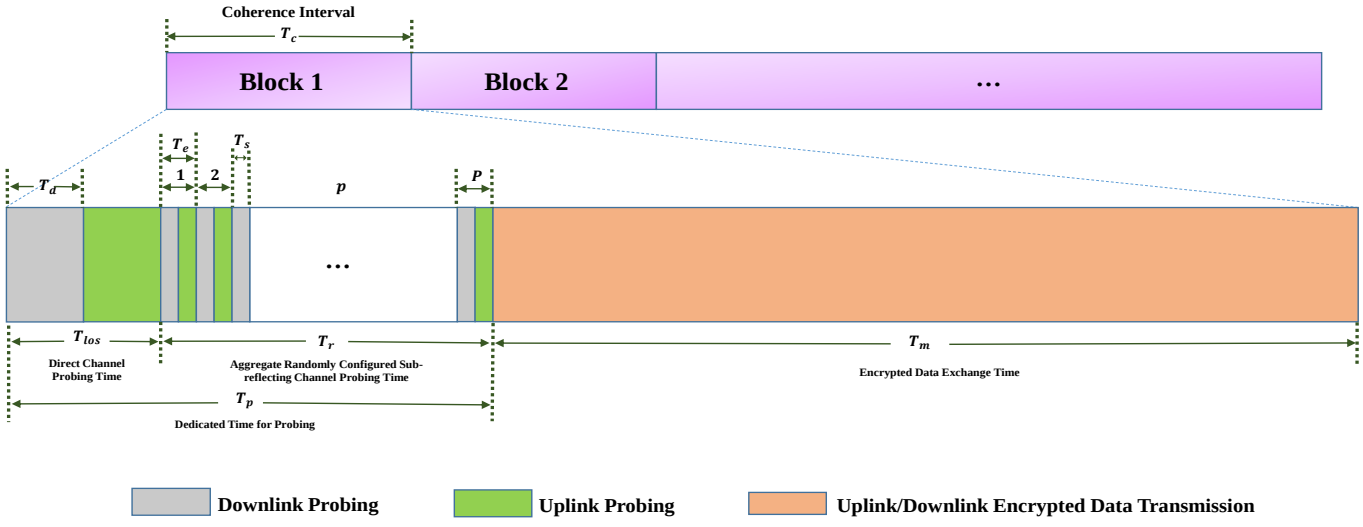

Fig. 2: Time slot allocation for the spatially correlated RIS-assisted SKG.

the previous two steps.

A. Step 1: Direct Channel Estimation

We estimate the direct channel in this step to exploit its variation from block to block in secret key generation. Additionally, the direct channel remains constant during each time slot. Thus, a strong direct channel can hinder our efforts in generating a random key sequence from the aggregate randomly configured sub-reflecting RIS channel. To estimate the direct channel, Alice and Bob turn off the RIS and exchange public pilots with each other. Eve also receives these pilot signals. The transmitted pilot signal by Alice is received by Bob and Eve as

$$\mathbf{y}_{i,1} = \sqrt{P_a} h_{ai} \mathbf{x}_d + \mathbf{n}_{i,1}, \quad , i \in \{b, e\}, \tag{1}$$

while the pilot signal received by Alice and Eve sent by Bob is

$$\mathbf{y}_{i,2} = \sqrt{P_b} h_{bi} \mathbf{x}_d + \mathbf{n}_{i,2}, \quad , i \in \{a, e\}. \tag{2}$$

In (1) and (2), $\mathbf{x}_d \in \mathbb{C}^{T_d \times 1}$ is the public pilot signal, where T_d is also assumed to be the length of the pilot signal in the direct channel probing. Additionally, P_a and P_b are the

transmit power of Alice and Bob and $h_{ai} \sim \mathcal{CN}(0, \sigma_{ai}^2)$ and $h_{bi} \sim \mathcal{CN}(0, \sigma_{bi}^2)$ are the direct channel coefficients from Alice to i, $i = \{b, e\}$ and from Bob to i, $i = \{a, e\}$, respectively. Moreover, $\mathbf{n}_{i,1}\mathbf{n}_{i,2} \sim \mathcal{CN}(\mathbf{0}, \sigma_i^2\mathbf{I})$ are the independent and identically distributed (i.i.d.) complex additive white Gaussian noise vectors. We assume the receivers exploit the least squares (LS) method to obtain CSI. Accordingly, the CSI measured by Bob and Eve can be written as

$$\hat{h}_{ai} = \frac{\mathbf{x}_d^H \mathbf{y}_{i,1}}{\sqrt{P_a}||\mathbf{x}_d||^2} = h_{ai} + \underbrace{\frac{1}{\sqrt{P_a T_d}} n_{i,1}}_{\hat{n}_{i,1}}, \quad i \in \{b, e\}, \quad (3)$$

while the CSI measured by Alice and Eve is

$$\hat{h}_{bi} = \frac{\mathbf{x}_d^H \mathbf{y}_{i,2}}{\sqrt{P_b}||\mathbf{x}_d||^2} = h_{bi} + \underbrace{\frac{1}{\sqrt{P_b T_d}} n_{i,2}}_{\hat{n}_{i,2}}, \quad i \in \{a, e\}. \quad (4)$$

We note that $\hat{n}_{i,1} \sim \mathcal{CN}(0, \hat{\sigma}_{i,1}^2 = \sigma_i^2/(P_a T_d))$ and $\hat{n}_{i,2} \sim \mathcal{CN}(0, \hat{\sigma}_{i,2}^2 = \sigma_i^2/(P_b T_d))$ are estimation noise terms and $\hat{\sigma}_{ai}^2 = \sigma_{ai}^2 + \sigma_i^2/(P_a T_d)$ and $\hat{\sigma}_{bi}^2 = \sigma_{bi}^2 + \sigma_i^2/(P_b T_d)$ denote the variance of the estimated channels. Moreover, $||.||^2$ denotes the Euclidean norm of a vector.

B. Step 2: Aggregate Randomly Configured Sub-Reflecting Channel Estimation

At this step, during the pilot exchange phase the transmitted pilot of Alice is received by Bob and Eve as

$$\mathbf{y}_{i,1}^p = \sqrt{P_a}(h_{ai} + \mathbf{h}_{ri}^H \mathbf{\Phi}^p \mathbf{h}_{ar})\mathbf{x}_r + \mathbf{n}_i^p, \quad i \in \{b, e\}, \quad (5)$$

where $\mathbf{x}_r \in \mathbb{C}^{T_s \times 1}$ is the public pilot signal and T_s is the pilot signal length. Additionally, $\mathbf{h}_{ar} \in \mathbb{C}^{N \times 1}$ is the channel vector for Alice-Rose link and $\mathbf{h}_{ri} \in \mathbb{C}^{N \times 1}$ is the channel from Rose to the receiver i. Let $\mathbf{\Phi}^p = \text{diag}[e^{j\phi_1^p}, ..., e^{j\phi_N^p}]$ be the diagonal phase shift matrix of RIS with size N in the p-th round of channel probing. We note that in the EPS scheme, we have the equal phase shifts in a given p, i.e., $\phi_1^p = ... = \phi_N^p$ while this equality does not hold in the RPS scheme. Moreover, it is possible to configure the phase shifts by uniformly quantizing the interval $[0, 2\pi)$, i.e., $\{0, \frac{2\pi}{2^B}, ..., \frac{(2^B-1)2\pi}{2^B}\}$, where B is the number of quantization bits. In (5), $\mathbf{n_i}^p \sim \mathcal{CN}(\mathbf{0}, \sigma_i^2\mathbf{I})$ is the i.i.d. complex additive white Gaussian noise vector.

Similarly, in the subsequent time slot Bob sends his probing sequence and the received signal at Alice and Eve is

$$\mathbf{y}_{i,2}^p = \sqrt{P_b}(h_{bi} + \mathbf{h}_{ri}^H \mathbf{\Phi}^p \mathbf{h}_{br})\mathbf{x}_r + \mathbf{n}_i^p, \quad i \in \{a, e\} \quad (6)$$

where $\mathbf{h}_{br} \in \mathbb{C}^{N \times 1}$ denotes the channel from Bob to Rose. Accordingly, the equivalent estimated channels at each node can be calculated based on observations in (5) and (6) as

$$\hat{h}_a^p = \frac{\mathbf{x}_r^H \mathbf{y}_{a,2}^p}{\sqrt{P_b}||\mathbf{x}_r||^2} = h_{ba} + \mathbf{h}_{ra}^H \mathbf{\Phi}^p \mathbf{h}_{br} + \underbrace{\frac{1}{\sqrt{P_b T_s}} n_a^p}_{\hat{n}_a^p}, \quad (7a)$$

$$\hat{h}_b^p = \frac{\mathbf{x}_r^H \mathbf{y}_{b,1}^p}{\sqrt{P_a}||\mathbf{x}_r||^2} = h_{ab} + \mathbf{h}_{rb}^H \mathbf{\Phi}^p \mathbf{h}_{ar} + \underbrace{\frac{1}{\sqrt{P_a T_s}} n_b^p}_{\hat{n}_b^p}, \quad (7b)$$

$$\hat{h}_{ae}^p = \frac{\mathbf{x}_r^H \mathbf{y}_{e,1}^p}{\sqrt{P_a}||\mathbf{x}_r||^2} = h_{ae} + \mathbf{h}_{re}^H \mathbf{\Phi}^p \mathbf{h}_{ar} + \underbrace{\frac{1}{\sqrt{P_a T_s}} n_{ae}^p}_{\hat{n}_{ae}^p}, \quad (7c)$$

$$\hat{h}_{be}^p = \frac{\mathbf{x}_r^H \mathbf{y}_{e,2}^p}{\sqrt{P_b}||\mathbf{x}_r||^2} = h_{be} + \mathbf{h}_{re}^H \mathbf{\Phi}^p \mathbf{h}_{br} + \underbrace{\frac{1}{\sqrt{P_b T_s}} n_{be}^p}_{\hat{n}_{be}^p}, \quad (7d)$$

where $\hat{n}_a^p \sim \mathcal{CN}(0, \hat{\sigma}_a^2 = \sigma_a^2/(P_b T_s))$, $\hat{n}_b^p \sim \mathcal{CN}(0, \hat{\sigma}_b^2 = \sigma_b^2/(P_a T_s))$, $\hat{n}_{ae}^p \sim \mathcal{CN}(0, \hat{\sigma}_{ae}^2 = \sigma_e^2/(P_a T_s))$ and $\hat{n}_{be}^p \sim \mathcal{CN}(0, \hat{\sigma}_{be}^2 = \sigma_e^2/(P_b T_s))$ are the estimation error at Alice, Bob and Eve. To extract secret keys from reflecting channels, Alice and Bob subtract their measurements from step 1 from the estimated channels in step 2 to mitigate the influence of the direct channel and Eve also follows the same steps. Accordingly, the samples according to which the secret keys are generated are

$$h_a^p = \hat{h}_a^p - \hat{h}_{ba} = \mathbf{h}_{ra}^H \mathbf{\Phi}^p \mathbf{h}_{br} + \underbrace{\hat{n}_a^p - \hat{n}_{a,2}}_{\hat{z}_a^p}, \quad (8a)$$

$$h_b^p = \hat{h}_b^p - \hat{h}_{ab} = \mathbf{h}_{rb}^H \mathbf{\Phi}^p \mathbf{h}_{ar} + \underbrace{\hat{n}_b^p - \hat{n}_{b,1}}_{\hat{z}_b^p}, \quad (8b)$$

$$h_{ae}^p = \hat{h}_{ae}^p - \hat{h}_{ae} = \mathbf{h}_{re}^H \mathbf{\Phi}^p \mathbf{h}_{ar} + \underbrace{\hat{n}_{ae}^p - \hat{n}_{e,1}}_{\hat{z}_{ae}^p}, \quad (8c)$$

$$h_{be}^p = \hat{h}_{be}^p - \hat{h}_{be} = \mathbf{h}_{re}^H \mathbf{\Phi}^p \mathbf{h}_{br} + \underbrace{\hat{n}_{be}^p - \hat{n}_{e,2}}_{\hat{z}_{be}^p}. \quad (8d)$$

We note that the subtracted noise terms in (8a) through (8d) are independent random variables (RVs). Accordingly, $\hat{z}_a^p \sim \mathcal{CN}(0, \hat{\sigma}_{z_a}^2 = \sigma_a^2/(P_b T_d) + \sigma_a^2/(P_b T_s))$, $\hat{z}_b^p \sim \mathcal{CN}(0, \hat{\sigma}_{z_b}^2 = \sigma_b^2/(P_a T_d) + \sigma_b^2/(P_a T_s))$, $\hat{z}_{ae}^p \sim \mathcal{CN}(0, \hat{\sigma}_{z_{ae}}^2 = \sigma_e^2/(P_a T_d) + \sigma_e^2/(P_a T_s))$ and $\hat{z}_{be}^p \sim \mathcal{CN}(0, \hat{\sigma}_{z_{be}}^2 = \sigma_e^2/(P_b T_d) + \sigma_e^2/(P_b T_s))$.

We further note that we take into account correlated Rayleigh fading channel. Mathematically, the channels are described as

$$h_{ij} \sim \mathcal{CN}(0, \sigma_{ij}^2) \quad \mathbf{h}_{ir} \sim (\mathbf{0}, \mathbf{R}_{ir}) \quad i, j = \{a, b, e\}, \quad (9)$$

.

In (9), σ_{ij}^2 is the path-loss between i and j and $\mathbf{R}_{ir}$ is the correlation matrix of the RIS elements. Here we adopt the RIS channel correlation model proposed in [37]. Accordingly, $\mathbf{R}_{ir}$ is given by

$$\mathbf{R}_{ir} = \underbrace{\sigma_{ir}^2 d_H d_V}_{\kappa_{ir}} \mathbf{R}, \quad (10)$$

in which

$$[\mathbf{R}]_{i,j} = \text{sinc}(2||\mathbf{u}_i - \mathbf{u}_j||/\lambda) \qquad i, j = 1, ..., N. \quad (11)$$

In (10) and (11), d_H and d_V are the vertical height and horizontal width of each RIS element, λ is the wavelength of the plane wave and $\mathbf{u}_\alpha = [0, \mathrm{mod}(\alpha-1, N_H)d_H, \lfloor(\alpha-1)/N_H\rfloor d_V]^T$, $\alpha \in \{i, j\}$, where N_H and N_V denote the elements per row and per column of the two-dimensional rectangular RIS.

Given the channel estimates in (3), (4) and (8), the maximum achievable KGR is given by [45] and [46] as

$$R_s = \frac{1}{2T_d} I(\hat{h}_{ab}; \hat{h}_{ba} | \hat{h}_{ae}, \hat{h}_{be}) + \frac{1}{2PT_s} \sum_{p=1}^{P} I\left(h_a^p; h_b^p | h_{ae}^p, h_{be}^p\right). \quad (12)$$

Remark 1: It may seem desirable to exploit the randomness in the reflecting channels of the RIS as we did so with the direct channel. In fact, this approach is considered in some studies, e.g., [25]. However, here based on the following, we do not recommend incorporating the reflective paths separately in the SKG process:

- Due to the presence of the inherent correlation between the reflective channels, using them in the SKG process will boost the correlation in the finally generated key sequence.
- To exploit the randomness of the reflective paths, Alice and bob should send pilots to the RIS to estimate the reflective channels. Accordingly, the third party controlling the RIS knows the corresponding reflective paths besides the random phase shifts. If the third party is not necessarily trusted, the SKG process will be seriously jeoperdized.
- One may argue that the indirect channel estimation will be necessary for the data transmission phase and accordingly we can exploit its randomness in the SKG phase. However, estimating the reflective paths is not always favorable as it requires relatively complicated signal processing and substantial training overhead [44]. In fact, there are numerous applications in which the phase shifts of the RIS elements are randomly altered to boost communication quality [40]–[44]. In such applications, estimating the indirect channels merely to exploit their randomness in the SKG process is not an efficient approach.

Unlike [24], [31], [32], we are not able to incorporate CLT to calculate the second mutual information term in (12) as we take into account the correlated channel coefficients. To elaborate, we assume two common scenarios namely EPS and RPS. In the following, we will calculate the correlation coefficient between two different probings in the second step $\rho^{(p_1,p_2)}$ and evaluate SKG based on (12) for the formerly mentioned scenarios.

III. Correlation Between Subsequent Probings

The rationale behind using the RIS in our system model is to introduce randomness to a quasi-static wireless channel. Accordingly, it is vital to quantify the correlation between the two probings at Alice and Bob. In this section, we will evaluate this correlation for EPS and RPS schemes. Moreover, here we consider the case in which the two legitimate parties generate secret keys without mitigating the influence of the direct channel. Accordingly, our analysis in this section will include the four cases of EPS and RPS with and without a direct path in channel samples.

A. Correlation in the presence of the direct path

When the direct path is present, the correlation is given by the following theorem.

Theorem 1. *The correlation coefficient between two channel samples is given by*

$$\rho^{(p_1,p_2)} = \frac{\sigma_{ij}^2 + \mathrm{tr}\left\{\mathbf{R}_{ir}\mathbb{E}\left[\mathbf{\Phi}^{p_2 H}\right]\mathbf{R}_{jr}\mathbb{E}\left[\mathbf{\Phi}^{p_1}\right]\right\}}{\sigma_{ij}^2 + \mathrm{tr}\left\{\mathbb{E}\left[\mathbf{R}_{ir}\mathbf{\Phi}^{p_l H}\mathbf{R}_{jr}\mathbf{\Phi}^{p_l}\right]\right\} + \hat{\sigma}_j^2}, \quad (13)$$

where $l \in \{1,2\}$, $i,j \in \{a,b\}$ and $\mathrm{tr}\{.\}$ and $\mathbb{E}[.]$ denote the trace and expectation operators ,respectively.

Proof: Please see Appendix A.

Lemma 1. *The correlation coefficient between two probings when RPS is applied in RIS elements is given by*

$$\rho_{rps_j}^{(p_1,p_2)} = \frac{\sigma_{ij}^2}{\sigma_{ij}^2 + \mathrm{tr}\left\{\mathbf{R}_{jr} \circ \mathbf{R}_{ir}\right\} + \hat{\sigma}_j^2}, \quad (14)$$

where $\circ$ denotes the Hadamard product.

Proof: We denote the random phase shift matrix of RIS as $\mathbf{\Phi}^{p_l} = \mathrm{diag}[e^{j\phi_1^{p_l}}, ..., e^{j\phi_N^{p_l}}]$, where $\phi_i^{p_l} \sim \mathcal{U}(-\pi, \pi)$, $i \in \{1, ..., N\}$ and $l \in \{1,2\}$. Accordingly, $\mathbb{E}\left[\mathbf{\Phi}^{p_1}\right] = \mathbb{E}\left[\mathbf{\Phi}^{p_2 H}\right] = \mathbf{0}$. Furthermore,

$$\mathrm{tr}\left\{\mathbb{E}\left[\mathbf{R}_{ir}\mathbf{\Phi}^{p_l H}\mathbf{R}_{jr}\mathbf{\Phi}^{p_l}\right]\right\} = \sum_{n=1}^{N}\sum_{m=1}^{N} r_{ir}^{nm} r_{jr}^{nm} \mathbb{E}\left\{e^{j(\phi_n^{p_l} - \phi_m^{p_l})}\right\} \overset{(a)}{=} \sum_{n=1}^{N} r_{ir}^{nn} r_{jr}^{nn} = \mathrm{tr}\left\{\mathbf{R}_{jr} \circ \mathbf{R}_{ir}\right\}, \quad (15)$$

where (a) holds because $\mathbb{E}\left\{e^{j(\phi_n^{p_l} - \phi_m^{p_l})}\right\} = 1$, if $n = m$. Otherwise, $\mathbb{E}\left\{e^{j(\phi_n^{p_l} - \phi_m^{p_l})}\right\} = 0$. Substituting in (13) we obtain (14).

Lemma 2. *The correlation coefficient between two probings when EPS is applied in RIS elements is given by*

$$\rho_{eps_j}^{(p_1,p_2)} = \frac{\sigma_{ij}^2}{\sigma_{ij}^2 + \mathrm{tr}\left\{\mathbf{R}_{jr}\mathbf{R}_{ir}\right\} + \hat{\sigma}_j^2}, \quad (16)$$

Proof: We denote the equal phase shift in each probing as $\mathbf{\Phi}^{p_l} = e^{j\phi^{p_l}}\mathbf{I}$ where $\phi^{p_l} \sim \mathcal{U}(-\pi, \pi)$, $l \in \{1,2\}$. Accordingly, $\mathbb{E}\left[\mathbf{\Phi}^{p_1}\right] = \mathbb{E}\left[\mathbf{\Phi}^{p_2 H}\right] = \mathbf{0}$. Additionally,

$$\mathrm{tr}\left\{\mathbb{E}\left[\mathbf{R}_{ir}\mathbf{\Phi}^{p_l H}\mathbf{R}_{jr}\mathbf{\Phi}^{p_l}\right]\right\} = \mathrm{tr}\left\{\mathbb{E}\left[\mathbf{R}_{ir}e^{-j\phi_{p_l}}\mathbf{R}_{jr}e^{j\phi_{p_l}}\right]\right\}, = \mathrm{tr}\left\{\mathbf{R}_{jr}\mathbf{R}_{ir}\right\} \quad (17)$$

Substituting in (13), we obtain (16).

B. Correlation without the direct channel

When the direct channel influence is mitigated, $\rho^{(p_1,p_2)}$ is given by the subsequent theorem.

Theorem 2. *The correlation coefficient between two channel samples is calculated as*

$$\rho^{(p_1,p_2)} = \frac{\mathrm{tr}\left\{\mathbf{R}_{ir}\mathbb{E}\left[{\mathbf{\Phi}^{p_2}}^H\right]\mathbf{R}_{jr}\mathbb{E}\left[\mathbf{\Phi}^{p_1}\right]\right\} + \hat{\sigma}^2_{j,k}}{\mathrm{tr}\left\{\mathbb{E}\left[\mathbf{R}_{ir}{\mathbf{\Phi}^{p_l}}^H\mathbf{R}_{jr}\mathbf{\Phi}^{p_l}\right]\right\} + \hat{\sigma}^2_{z_j}}, \quad (18)$$

where $k = 1$ if $j = b$ and $k = 2$ if $j = a$.

Proof: Please see Appendix B.

Lemma 3. *The correlation coefficient between two probings when RPS is applied in RIS elements is given by*

$$\rho^{(p_1,p_2)}_{rps_j} = \frac{\hat{\sigma}^2_{j,k}}{\mathrm{tr}\left\{\mathbf{R}_{jr}\circ\mathbf{R}_{ir}\right\} + \hat{\sigma}^2_{z_j}}, \quad (19)$$

and for EPS is

$$\rho^{(p_1,p_2)}_{eps_j} = \frac{\hat{\sigma}^2_{j,k}}{\mathrm{tr}\left\{\mathbf{R}_{jr}\mathbf{R}_{ir}\right\} + \hat{\sigma}^2_{z_j}}. \quad (20)$$

Proof: Using the same steps in proofs of Lemmas 1 and 2, it is straightforward to obtain the expressions in (19) and (20).

Remark 2: We argue that the spatial correlation considered in our scenario does not have any contribution to boosting $\rho^{(p_1,p_2)}$. As stated before, since we do not use the individual reflective correlated paths in the SKG process, the existing spatial correlation does not have a negative impact on the randomness of the final secret key sequence. Accordingly, $\rho^{(p_1,p_2)}$ is only dealing with the temporal correlation of the channel samples which is suppressed by the random phase shifts in the RIS elements.

IV. Spatially Correlated RIS Secret Key Capacity Upper Bound

In this section, we intend to calculate the mutual information terms in (12). Since CLT is not applicable in our system model due to the spatial correlation between RIS elements, we devise a new approach which exploits eigenvalue decomposition (EVD) to obtain KGR. The following Theorems are prerequisites for our EVD approach.

Theorem 3. *Let Θ and X be two independent RVs with distributions $\Theta \sim \mathcal{U}(-\pi,\pi)$ and $X \sim \mathcal{CN}(0,\sigma^2)$, respectively. The RV, $Y = Xe^{j\Theta}$ is complex Gaussian with distribution $Y \sim \mathcal{CN}(0,\sigma^2)$.*

Proof: We denote the amplitude and phase of X as R and Ψ where they are independent with distributions $R \sim$ *Rayleigh*$(\sigma^2/2)$ and $\Psi \sim \mathcal{U}(-\pi,\pi)$. Moreover, we can write $Y = Re^{j(\Psi+\Theta)} = Re^{j\Phi}$. As Φ is the sum of two independent uniform Rvs distributed in the interval $(-\pi,\pi)$, it has the distribution $\Phi \sim \mathcal{U}(-\pi,\pi)$. Accordingly, $Y = Re^{j\Phi}$ has a complex Gaussian distribution with mean and variance the same as X.

Theorem 4. *Let $\mathbf{\Theta}$ be an $N \times N$ random matrix defined as $\mathbf{\Theta} = \mathrm{diag}[e^{j\theta_1},...,e^{j\theta_N}]$ where $\theta_i \sim \mathcal{U}(-\pi,\pi)$, $i \in 1,...,N$. Additionally, $\mathbf{g}$ is an $N \times 1$ random vector with distribution $\mathbf{g} \sim \mathcal{CN}(\mathbf{0},\mathbf{C})$ where $\mathbf{C}^{N\times N}$ denotes the correlation matrix between the entries of $\mathbf{g}$. The random vector $\mathbf{h} = \mathbf{\Theta}\mathbf{g}$ has the distribution $\mathbf{h} \sim \mathcal{CN}\left(0,\mathrm{diag}[c_1,...,c_N]\right)$ where, $c_i, i \in 1,...,N$ are the diagonal elements of $\mathbf{C}$.*

Proof: For each entry of $\mathbf{h}$ we can write $h_i = g_i e^{j\theta_i}$, where g_i is an entry of $\mathbf{g}$. According to Theorem 3, h_i has a complex Gaussian distribution with zero mean and variance c_i. For the correlation between two entries of $\mathbf{h}$, namely h_i and h_j, $i \neq j$ we can write

$$\mathbb{E}\left\{h_i h_j^*\right\} = \mathbb{E}\left\{g_i g_j^*\right\}\mathbb{E}\left\{e^{j\theta_i}\right\}\mathbb{E}\left\{e^{-j\theta_j}\right\} = 0 \quad (21)$$

Accordingly, the entries of $\mathbf{h}$ are uncorrelated complex Gaussian RVs which implies they are independent with distribution $\mathbf{h} \sim \mathcal{CN}\left(0,\mathrm{diag}[c_1,...,c_N]\right)$.

To calculate KGR the challenging part is to deal with the correlated terms within $\mathbf{h}_{ri}^H\mathbf{\Phi}^p\mathbf{h}_{jr}$, $i,j \in \{a,b,e\}$, in (8). Without the loss of generality, we can express the channel gain vectors $\mathbf{h}_{ri}$ and $\mathbf{h}_{jr}$ in terms of their correlation matrices as $\mathbf{h}_{ri} = \mathbf{R}_{ri}^{\frac{1}{2}}\mathbf{g}_{ri}$ and $\mathbf{h}_{jr} = \mathbf{R}_{jr}^{\frac{1}{2}}\mathbf{g}_{jr}$, where $\mathbf{g}_{ri},\mathbf{g}_{jr} \sim \mathcal{CN}(\mathbf{0},\mathbf{I})$. Now we have the prerequisites to calculate the KGR for our system model.

A. KGR for RPS scheme

To obtain KGR we firstly write the term $\mathbf{h}_{ri}^H\mathbf{\Phi}^p\mathbf{h}_{jr}$ as

$$\mathbf{h}_{ri}^H\mathbf{\Phi}^p\mathbf{h}_{jr} = \mathbf{g}_{ri}^H\mathbf{R}_{ri}^{\frac{1}{2}}\mathbf{u}_{jr}^p, \quad (22)$$

where $\mathbf{u}_{jr}^p = \mathbf{\Phi}^p\mathbf{h}_{jr}$. According to Theorem 4 and equations (10) and (11), the entries of $\mathbf{u}_{jr}^p$ are i.i.d. complex Gaussian RVs with distribution $\mathbf{u}_{jr}^p \sim \mathcal{CN}(\mathbf{o},\kappa_{jr}\mathbf{I})$. We perform the EVD on $\mathbf{R}_{ri}^{\frac{1}{2}}$ as $\mathbf{R}_{ri}^{\frac{1}{2}} = \mathbf{Q}_{ri}\mathbf{\Sigma}_{ri}\mathbf{Q}_{ri}^H$ where $\mathbf{Q}_{ri}$ is an $N \times N$ complex unitary matrix and $\mathbf{\Sigma}_{ri}$ is an $N \times N$ diagonal matrix, i.e., $\mathbf{\Sigma}_{ri} = \mathrm{diag}[\lambda_{ri}^1,...,\lambda_{ri}^N]$. Accordingly, we can rewrite (22) as

$$\mathbf{h}_{ri}^H\mathbf{\Phi}^p\mathbf{h}_{jr} = \underbrace{\mathbf{g}_{ri}^H\mathbf{Q}_{ri}}_{\mathbf{w}_{ri}^H}\mathbf{\Sigma}_{ri}\underbrace{\mathbf{Q}_{ri}^H\mathbf{u}_{jr}^p}_{\mathbf{w}_{jr}}. \quad (23)$$

Since $\mathbf{Q}_{ri}$ is a unitary matrix, the new channel vectors are $\mathbf{w}_{ri} \sim \mathcal{CN}(\mathbf{0},\mathbf{I})$, $\mathbf{w}_{jr} \sim \mathcal{CN}(\mathbf{0},\kappa_{jr}\mathbf{I})$. Now that we are dealing with the sum of independent RVs in (23), we can assert that for $N \gg 1$, $\mathbf{h}_{ri}^H\mathbf{\Phi}^p\mathbf{h}_{jr}$ is complex Gaussian with $\mathcal{CN}(0,\kappa_{jr}\sum_{n=1}^N {\lambda_{ri}^n}^2)$. Accordingly, we could transform correlated channel vector entries to i.i.d. entries through applying Theorem 4 and performing EVD.

B. KGR for EPS scheme

In the EPS case for the phase shift matrix of RIS we have $\mathbf{\Phi}^p = e^{j\phi^p}\mathbf{I}$, $\phi^p \sim \mathcal{U}(-\pi,\pi)$. Accordingly, we can write

$$\mathbf{h}_{ri}^H\mathbf{\Phi}^p\mathbf{h}_{jr} = e^{j\phi^p}\mathbf{g}_{ri}^H\underbrace{\mathbf{R}_{ri}^{\frac{1}{2}}\mathbf{R}_{jr}^{\frac{1}{2}}}_{\mathbf{\Psi}_{ij}}\mathbf{g}_{jr}. \quad (24)$$

Performing EVD on $\mathbf{\Psi}_{ij}$, we can write $\mathbf{\Psi}_{ij} = \mathbf{P}_{ij}\mathbf{\Xi}_{ij}\mathbf{P}_{ij}^H$, where $\mathbf{P}_{ij}$ is an $N \times N$ complex unitary matrix and $\mathbf{\Xi}_{ij}$

is an $N \times N$ diagonal matrix, i.e., $\mathbf{\Xi}_{ij} = \text{diag}[\rho_{ij}^1, ..., \rho_{ij}^N]$. Accordingly,

$$\mathbf{h}_{ri}^H \mathbf{\Phi}^p \mathbf{h}_{jr} = e^{j\phi^p} \underbrace{\mathbf{g}_{ri}^H \mathbf{P}_{ij}}_{\mathbf{v}_{ri}^H} \mathbf{\Xi}_{ij} \underbrace{\mathbf{P}_{ij}^H \mathbf{g}_{jr}}_{\mathbf{v}_{jr}}. \tag{25}$$

Since $\mathbf{P}_{ij}$ is a unitary matrix, the new channel vectors are $\mathbf{v}_{ri} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$, $\mathbf{v}_{jr} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ and for $N \gg 1$ we can apply CLT on $x_{ij} = \mathbf{v}_{ri}^H \mathbf{\Xi}_{ij} \mathbf{v}_{jr}$ as x_{ij} is the sum of independent RVs. This leads to $x_{ij} \sim \mathcal{CN}(0, \sum_{n=1}^N {\rho_{ij}^n}^2)$. Finally,

$$\mathbf{h}_{ri}^H \mathbf{\Phi}^p \mathbf{h}_{jr} = e^{j\phi^p} x_{ij} = y_{ij}, \tag{26}$$

in which according to Theorem 3, y_{ij} is a complex Gaussian RV with the same mean and variance as x_{ij}, $y_{ij} \sim \mathcal{CN}(0, \sum_{n=1}^N {\rho_{ij}^n}^2)$.

We remark that the variance of $\mathbf{h}_{ri}^H \mathbf{\Phi}^p \mathbf{h}_{jr}$ obtained in this section is equal to the expression calculated in Section III. In other words, we have

$$\kappa_{jr} \sum_{n=1}^N {\lambda_{ri}^n}^2 = \text{tr}\left\{\mathbf{R}_{jr} \circ \mathbf{R}_{ir}\right\}, \tag{27}$$

$$\sum_{n=1}^N {\rho_{ij}^n}^2 = \text{tr}\left\{\mathbf{R}_{jr} \mathbf{R}_{ir}\right\}. \tag{28}$$

Verifying the above equations is straightforward using the well-known properties of eigenvalues. Now that we have the statistical properties of our channel samples, we can evaluate the KGR.

Theorem 5. *The maximum achievable KGR in RIS-assisted wireless network with spatial correlation between RIS elements is*

$$R_s = \frac{1}{2T_d} \log_2 \Lambda(\mathbf{\Omega}) + \frac{1}{2T_s} \log_2 \Lambda(\mathbf{\Delta}) \tag{29}$$

where by defining $\mathbf{v} = (x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4)$, $\Lambda(\mathbf{v})$ *is defined at the top of the next page and* $\mathbf{\Omega} = (\Omega_1, \Omega_2, \Omega_3, \Omega_4, \omega_1, \omega_2, \omega_3, \omega_4)$, $\mathbf{\Delta} = (\Delta_1, \Delta_2, \Delta_3, \Delta_4, \delta_1, \delta_2, \delta_3, \delta_4)$. *Moreover we have*

$$\Omega_1 = \upsilon_{aa} = \sigma_{ab}^2 + \hat{\sigma}_{a,2}^2, \tag{31}$$

$$\Omega_2 = \upsilon_{bb} = \sigma_{ab}^2 + \hat{\sigma}_{b,1}^2, \tag{32}$$

$$\Omega_3 = \upsilon_{aeae} = \sigma_{ae}^2 + \hat{\sigma}_{e,1}^2, \tag{33}$$

$$\Omega_4 = \upsilon_{bebe} = \sigma_{be}^2 + \hat{\sigma}_{e,2}^2, \tag{34}$$

$$\omega_1 = \upsilon_{ab} = \upsilon_{ba} = \sigma_{ab}^2, \tag{35}$$

$$\omega_2 = \upsilon_{aebe} = \upsilon_{beae} = \rho_{ab}\sigma_{ae}\sigma_{be}, \tag{36}$$

$$\omega_3 = \upsilon_{aae} = \upsilon_{aea} = \upsilon_{bae} = \upsilon_{aeb} = \rho_{be}\sigma_{ae}\sigma_{ab}, \tag{37}$$

$$\omega_4 = \upsilon_{abe} = \upsilon_{bbe} = \upsilon_{bea} = \upsilon_{beb} = \rho_{ae}\sigma_{ab}\sigma_{be}, \tag{38}$$

$$\Delta_1 = \eta_{aa} = \text{tr}\left\{\mathbf{R}_{ar} \odot \mathbf{R}_{br}\right\} + \hat{\sigma}_{z_a}^2, \tag{39}$$

$$\Delta_2 = \eta_{bb} = \text{tr}\left\{\mathbf{R}_{ar} \odot \mathbf{R}_{br}\right\} + \hat{\sigma}_{z_b}^2, \tag{40}$$

$$\Delta_3 = \eta_{aeae} = \text{tr}\left\{\mathbf{R}_{ar} \odot \mathbf{R}_{er}\right\} + \hat{\sigma}_{z_{ae}}^2, \tag{41}$$

$$\Delta_4 = \eta_{bebe} = \text{tr}\left\{\mathbf{R}_{br} \odot \mathbf{R}_{er}\right\} + \hat{\sigma}_{z_{be}}^2, \tag{42}$$

$$\delta_1 = \eta_{ab} = \eta_{ba} = \text{tr}\left\{\mathbf{R}_{ar} \odot \mathbf{R}_{br}\right\}, \tag{43}$$

$$\delta_2 = \eta_{aebe} = \eta_{beae} = \rho_{ab}\sqrt{\kappa_{ar}}\sqrt{\kappa_{br}}\kappa_{re} \times \text{tr}\left\{\mathbf{R} \odot \mathbf{R}\right\}, \tag{44}$$

$$\delta_3 = \eta_{aae} = \eta_{aea} = \eta_{bae} = \eta_{aeb} = \rho_{be}\sqrt{\kappa_{er}} \times \sqrt{\kappa_{br}}\kappa_{ra}\text{tr}\left\{\mathbf{R} \odot \mathbf{R}\right\}, \tag{45}$$

$$\delta_4 = \eta_{abe} = \eta_{bbe} = \eta_{bea} = \eta_{beb} = \rho_{ae}\sqrt{\kappa_{er}} \times \sqrt{\kappa_{ar}}\kappa_{rb}\text{tr}\left\{\mathbf{R} \odot \mathbf{R}\right\}, \tag{46}$$

where we have accounted for the reciprocal channels between the nodes $\sigma_{ij}^2 = \sigma_{ji}^2, i, j \in \{a, b, e\}$. *Additionally,* $\rho_{ij} = J_0(2\pi d_{ij}/\lambda)$ *denotes the spatial correlation coefficient between the channels of nodes* i *and* j*, where* $J_0(.)$ *is the zeroth-order Bessel function of the first kind,* λ *is the wavelength and* d_{ij} *is the distance between the two nodes. Finally,* $\odot$ *denotes the matrix multiplication when EPS is deployed in RIS while it denotes Hadamard product in RPS mode.*

Proof: Please see Appendix C.

V. Optimization of Sampling Period and Probing Time

In this section, we intend to develop an optimization framework to determine the optimum sampling period and probing time for direct and aggregate randomly configured sub-reflective channel. In fact, the idea of implementing random shifts in RIS to enhance KGR has its own limitations. Specifically, one may assume that by reducing the sampling period T_s we can obtain more channel samples and increase the KGR. However, reducing T_s will lead to a reduction in the number of bits extracted from each sample [29]. This is because reducing T_s will enhance the channel estimation noise power and accordingly limit the KGR. Moreover, choosing a large T_s will hinder the maximum utilization of RIS in generating secret keys. Therefore, the optimum selection of T_s is vital to achieve the maximum KGR. We further note that it is important to optimally allocate the overall probing time between the direct and reflective paths as this can affect both the correlation between the samples and the maximum

$$\mathbf{\Lambda}(\mathbf{v}) = \frac{\left[x_1(x_3x_4 - y_2^2) + 2y_2y_3y_4 - y_4^2x_3 - y_3^2x_4\right]\left[x_2(x_3x_4 - y_2^2) + 2y_2y_3y_4 - y_4^2x_3 - y_3^2x_4\right]}{(x_3x_4 - y_2^2)\left[(x_1 + x_2 - 2y_1)(2y_2y_3y_4 - y_4^2x_3 - y_3^2x_4) - (x_3x_4 - y_2^2)(y_1^2 - x_1x_2)\right]} \tag{30}$$

achievable KGR. Accordingly, we formulate our optimization problem as

$$\max_{T_d,T_r,T_s} \; R_s, \tag{47a}$$
$$\text{s.t.} : 2T_d + T_r = T_p, \tag{47b}$$
$$T_s \leq \frac{T_r}{2}, \tag{47c}$$
$$\max\{\rho_{s_a}^{(p_1,p_2)}, \rho_{s_b}^{(p_1,p_2)}\} \leq \rho^t, \tag{47d}$$

where $s \in \{rps, eps\}$ and ρ^t and T_p denote the maximum permissible correlation between the channel samples and the dedicated time to probing within a coherence time of the channel, respectively. Substituting (47b) into (47c), we can reformulate the optimization problem as

$$\max_{T_d,T_s} \; R_s, \tag{48a}$$
$$\text{s.t.} : T_s + T_d \leq \frac{T_p}{2}, \tag{48b}$$
$$\rho_{s_a}^{(p_1,p_2)} \leq \rho^t, \tag{48c}$$
$$\rho_{s_b}^{(p_1,p_2)} \leq \rho^t. \tag{48d}$$

To provide more insights into the objective function, we have plotted the KGR versus T_d and T_s in Fig. 3 for different levels of transmit power in Alice and Bob. In both Fig. 3.a and Fig. 3.b, we can observe that there is an optimum value for T_d and T_s, respectively which maximizes the KGR given in (48a). This observation is our motivation in raising the optimization problem in (48).

Remark 3: To enhance the randomness in generated secret keys, we subtracted the direct channel coefficient from the aggregate sub-reflective channel. Accordingly, the channel estimation error (CEE) in the second term of (29) is the aggregate of CEE in both direct and indirect probings. However, maximizing T_d to minimize the estimation error is not an optimum strategy. This is because of the contribution of the direct channel in KGR, reflected in the first term of (29). Accordingly, reckless maximizing of T_d can degrade the KGR generated by the direct path. This trade off shows the existence of an optimum value for T_d reflected in curves of Fig. 3.a.

Remark 4: As stated before, reducing T_s can hinder the SKG process by enhancing the CEE in the indirect probing phase. According to Fig. 3.b in the higher levels of transmit power, the optimal value for T_s gets smaller. This means that in a given T_r, the RIS can change the phase of its arrays more rapidly in high transmit powers and accordingly, enhance the KGR. We will further discuss the details in the next section.

Here, we intend to develop an optimization algorithm based on SCP, to derive the optimum T_s and T_d, namely $T_s{}^\star$ and $T_d{}^\star$, for (48). We remark that the objective function (48a) is non-concave. Additionally, the inequality conditions (48c) and (48d) are also non-concave due to the presence of T_dT_s term in them. To deal with the non-concavity problem, we apply

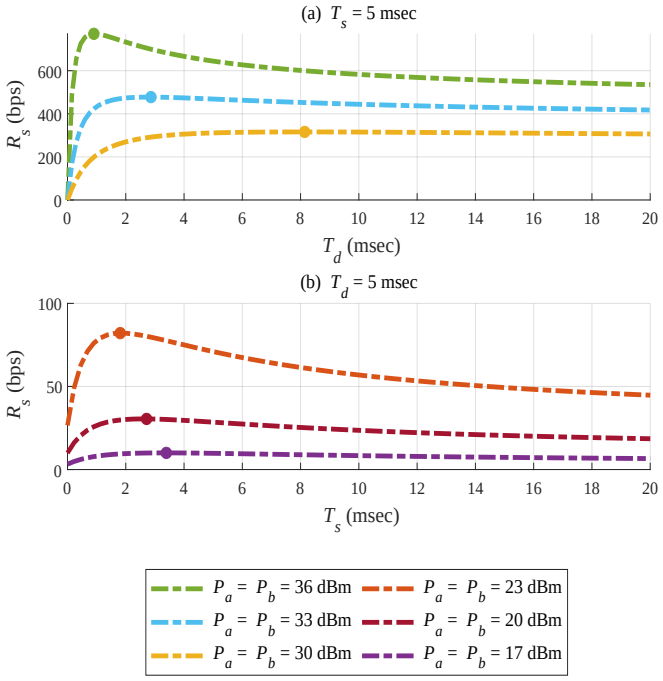

Fig. 3: KGR versus allocated time for direct probing and aggregate randomly configured sub-reflective channel probing for different levels of transmit power in the nodes.

the second order Taylor expansion of the objective function and (48c) and (48d) constraints as

$$\hat{f}^{(m+1)}(\mathbf{T}) = f\left(\mathbf{T}^{(m)}\right) + \nabla f\left(\mathbf{T}^{(m)}\right)^T\left(\mathbf{T} - \mathbf{T}^{(m)}\right) + \frac{1}{2}\left(\mathbf{T} - \mathbf{T}^{(m)}\right)^T\left(\nabla^2 f\left(\mathbf{T}^{(m)}\right)\right)_+\left(\mathbf{T} - \mathbf{T}^{(m)}\right), \tag{49}$$

where $\mathbf{T} = [T_d \quad T_s]^T$, $f \in \{R_s, \rho_{s_a}^{(p_1,p_2)}, \rho_{s_b}^{(p_1,p_2)}\}$, $\mathbf{T}_m$ is the point at which we approximate the f in step m of the algorithm and $(.)_+$ denotes the positive semi-definite (PSD) part of the Hessian matrix. Therefore, we have successfully transferred the non-concave problem in (48) into a concave problem. Algorithm 1 details the proposed SCP based algorithm, where M is the maximum number of iterations.

In Algorithm 1, due to the approximation of the two inequality constraints by the second order Taylor expansion, it is possible that the obtained $\mathbf{T}^{(m)}$ at each step does not satisfy the exact correlation constraints. Accordingly, we check this possibility in the following conditional expression to exclude the $\mathbf{T}^{(m)}$'s which do not satisfy the correlation constraints from the final step. Accordingly, it is not necessary to set feasible initial values for T_d and T_s. Throughout this paper, we use the recommended initial values in all of the presented results. We further remark that computing the PSD part of the Hessian matrices in each iteration is not computationally demanding as the Hessians are 2×2 matrices. We further note that the proposed algorithm converges fast and as we will

Algorithm 1 Proposed SCP Based Iterative Optimization

Input: $\mathbf{R}_{ar}, \mathbf{R}_{br}, \sigma_{ab}^2, P_a, P_b, \rho_{ab}, \rho_{ae}, \rho_{be}, \rho^t, T_p, M$
Output: T_d, T_s

Initialization: for $m = 0$
- $T_d^{(0)} = 0.4T_p$
- $T_s^{(0)} = 0.16T_p$

repeat (SCP Algorithm for T_d and T_s)
  Update $m = m + 1$.
  Solve the concave program to obtain $T_d^{(m)}$ and $T_s^{(m)}$:

$$\max_{T_d, T_s} \quad \hat{R}_s^{(m)}(\mathbf{T})$$
$$\text{s.t}: T_d + T_s \leq \frac{T_p}{2},$$
$$\hat{\rho}_{s_a}^{(p_1,p_2)^{(m)}}(\mathbf{T}) \leq \rho^t,$$
$$\hat{\rho}_{s_b}^{(p_1,p_2)^{(m)}}(\mathbf{T}) \leq \rho^t,$$

  if $\rho_{s_a}^{(p_1,p_2)^{(m)}}\left(\mathbf{T}^{(m)}\right) \geq \rho^t$ **or**
    $\rho_{s_b}^{(p_1,p_2)^{(m)}}\left(\mathbf{T}^{(m)}\right) \geq \rho^t$ **then**
      $R_s^{(m)}\left(\mathbf{T}^{(m)}\right) = 0$
  end if
until $m = M$.
calculate $T_d^\star, T_s^\star$ as:

$$T_d^\star, T_s^\star = \arg\max_{\mathbf{T}^{(m)}} \quad R_s^{(m)}\left(\mathbf{T}^{(m)}\right)$$

show in the following section, it only requires a few iterations to converge to an optimum point.

VI. Numerical Results and Discussions

In this section, we intend to discuss the vital parameters affecting the KGR in the presence of a spatially correlated RIS and present our numerical results. In all the following results, unless otherwise stated, we assume an square RIS with $N_H = N_v = 30$ and the element sizes of $d_H = d_V = 0.15m$. The channel variances are given by $\sigma_{ij}^2 = G_i + G_j + 10\zeta_{ij}\log_{10}(d_{ij}/d_0) + \sigma_0^2$, where $i, j \in \{a, b, r, e\}$, $\sigma_0^2 = -30$ dB is the path loss at $d_0 = 1$ m and $G_i = G_j = 4$ dBi denote the antenna gains at Alice, Bob and Eve and 0 dBi for Rose. Additionally, the distance between the nodes are considered as $d_{ab} = 70$ m, $d_{ae} = 0.15$ m, $d_{ar} = 4$ m, $d_{be} = d_{ab} - d_{ae}$, $d_{re} = d_{ar}$ and $d_{rb} = \sqrt{d_{ab}^2 + d_{ar}^2 - d_{ab}d_{ae}}$, where without the loss of generality, we have assumed that the all nodes are located in a two-dimensional plane and Eve is closer to Alice so that its observed channel can be correlated with the legitimate ones. The path loss exponents are assumed as $\zeta_{ab} = \zeta_{be} = 4.8$, $\zeta_{ae} = \zeta_{ar} = \zeta_{er} = 2.1$ and $\zeta_{br} = 2.2$. Moreover, we assume the carrier frequency is $f_c = 1$ GHz, the system bandwidth is BW = 10 MHz and the noise figure at Alice, Bob and Eve to be NF = 5 dB. We further set $T_c = 1sec$, $T_p = T_c/10$, $T_{los} = T_p/10$, $T_r = T_p - T_{los}$ and $P = 5$.

Ensuring randomness in the generated secret key sequence is a vital prerequisite in PLKG. Fig. 4, demonstrates the correlation between the two channel samples used in the PLKG process. We can observe that mitigating the impact of

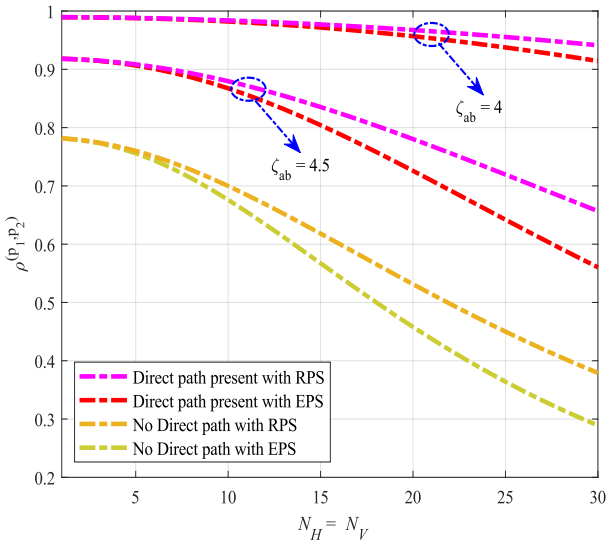

Fig. 4: Correlation coefficient for EPS and RPS schemes in the presence and absence of direct path in the SKG process ($P_a = P_b = 24$ dBm).

the direct channel can lead to considerably lower correlation and thus improved randomness of the generated key sequence. Despite assuming path loss exponents twice larger than the indirect paths in the direct channel, the correlation is still high even for the large number of N. In fact, in the case of the direct channel being present with RPS, meeting the condition $N \gg \sigma_{ab}^2/(d_H^2 d_V^2 \sigma_{ra}^2 \sigma_{br}^2)$ requires way more RIS elements than the $N \gg \sigma_{ab}^2/(\sigma_{ra}^2\sigma_{br}^2)$ stated in [24]. This shows that when taking a practical RIS model into account with isotropic scattering elements, mitigating the impact of the direct channel should be considered to avoid a strong correlation in the final generated bit sequence. Moreover, the figure shows that the EPS scheme leads to a lower correlation than the RPS either when the impact of the direct path is mitigated or not. This shows that by employing EPS we can exploit the correlation between the reflected paths to enhance the randomness in the final secret key sequence.

Fig. 5, explores the impact of various parameters on the correlation when the impact of the direct channel is mitigated. It shows how the increase of the transmit power can enhance the randomness in the final key sequence. This is because the transmit power enhancement will lead to an accurate estimation of the direct channel. Accordingly, the two sides can effectively remove the impact of the direct channel which is the main contributor to a strong correlation. Moreover, increasing the channel probation time in direct probing has the same impact. However, this should be considered precisely as reckless increasing of T_d can hinder the benefit of the random phase shifting in RIS to boost the KGR. Accordingly, we have considered the correlation term in our optimization problem in (48) to account for this trade-off. Finally, we can observe that the EPS scheme exploits the intrinsic correlation between the RIS elements to further mitigate the correlation. Accordingly, switching to the lower frequencies which leads to a stronger correlation between the indirect paths leads to a lower $\rho^{(p_1,p_2)}$

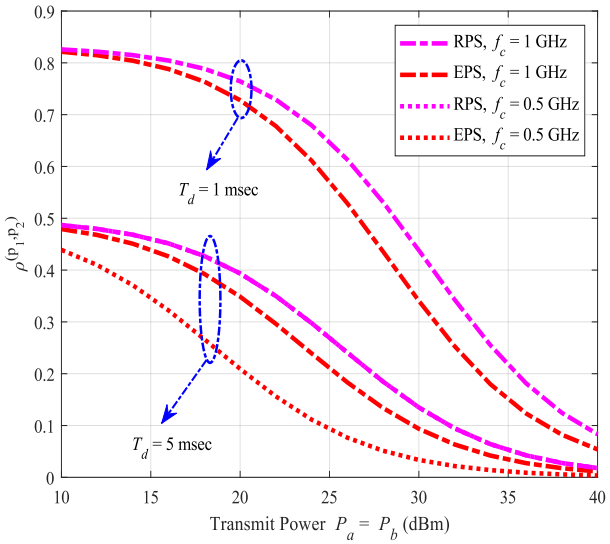

Fig. 5: Correlation coefficient versus transmit power when the impact of the direct channel is mitigated.

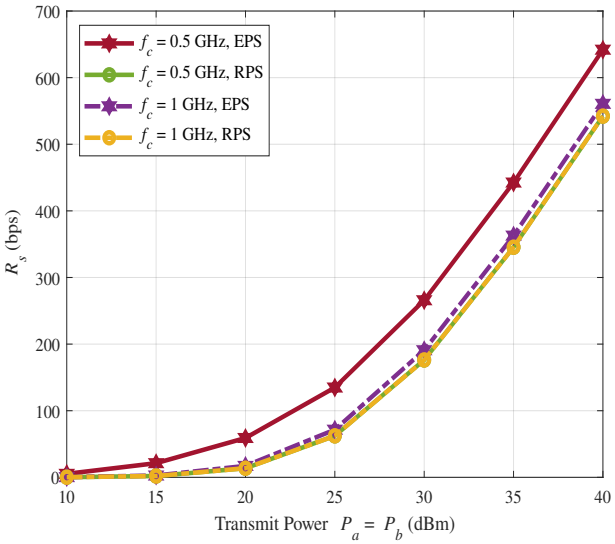

Fig. 6: KGR with EPS and RPS schemes when the channel of eavesdropper is independent of the channel of legitimate nodes.

in EPS. However, this has no impact when RPS is deployed.

Fig. 6, demonstrates the KGR in (29) for the EPS and RPS schemes when the eavesdropper channel is independent of the legitimate channels. We can observe that the EPS scheme outperforms the RPS for the whole range of transmit power. In fact, the spatial correlation between the RIS elements is the cause of this difference. To be specific, in the RPS case, the random phase shifts of the RIS elements can lead to either constructive or destructive addition of the reflected signals from RIS. However, in a spatially correlated RIS, the equal phase between the RIS elements will not alter the phase of the transmitted signal dramatically. Accordingly, there is a high probability that the reflected signals from the RIS add up constructively in the destination. This can also be inferred from (27) and (28). According to (27), deploying RPS in a spatially correlated RIS is equivalent to deploying a hypothetical uncorrelated RIS and the correlation enhancement within $\mathbf{R}$, will not affect the KGR of the system. This is reflected in Fig. 6 as we can observe that lowering the carrier frequency does not have any impact on KGR in the RPS scheme. However, it has enhanced the KGR by increasing $\mathrm{tr}\{\mathbf{R}_{jr}\mathbf{R}_{ir}\}$ in the EPS case. This observation reveals that deploying EPS in a spatially correlated RIS is the optimum strategy and it can lead to a higher KGR if the spatial correlation between the RIS elements is enhanced.

However, if the condition of the uncorrelated eavesdropper is not satisfied, the idea of using the lowest available carrier frequency will not necessarily lead to higher KGR. Fig. 7, clearly shows that exploiting lower carrier frequencies or equivalently higher wavelengths can degrade the KGR in the EPS case. The figure shows there is an optimal frequency in which the KGR is maximized and further decreasing the frequency can degrade the KGR of the EPS scheme. Additionally, we can observe increasing the wavelength has merely a negative impact in the RPS case. The maximum point is the

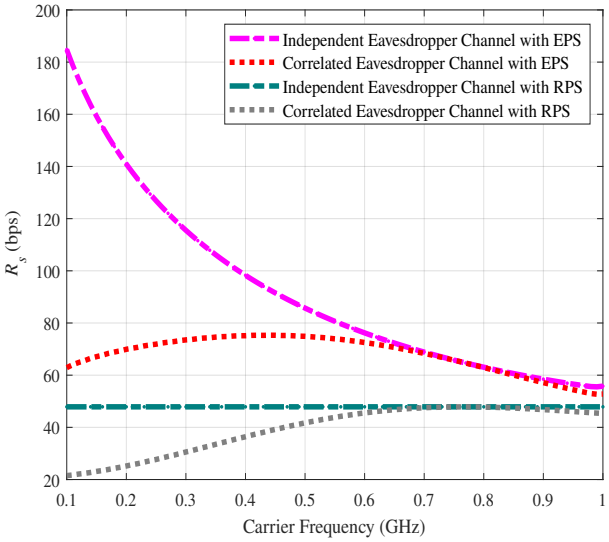

Fig. 7: KGR of EPS and RPS schemes versus frequency for $P_a = P_b = 24$ dBm

result of fluctuations in the $J_0(.)$ and as in a real practical scenario it is not easy to locate the exact position of a passive attacker, it can not be exploited during the SKG process. Accordingly, we can state that in the RPS scheme switching to lower frequencies in the SKG stage can generally lead to the degradation of the resulting rate while in the EPS case, it should take place carefully for the correlated eavesdropper channel.

Fig. 8, contrasts the performance of our SCP based optimization algorithm with the results obtained by the exhaustive search (ES). We define $N_{T_d} = 1/\zeta_{T_d}$ and $N_{T_s} = 1/\zeta_{T_s}$, where ζ_{T_d} and ζ_{T_s} denote the search step size for T_d and T_s in our ES algorithm. Here, we have set $\zeta_{T_d} = \zeta_{T_s} = 10^{-2}$. Furthermore, we assumed the maximum permissible correla-

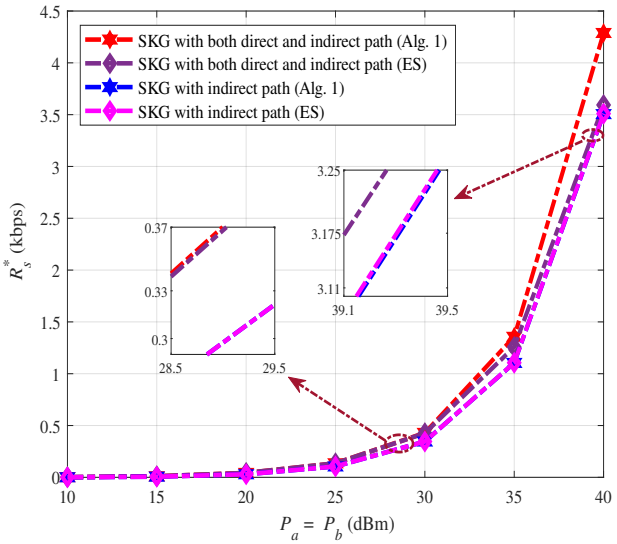

Fig. 8: Contrasting the performance of Algorithm 1 with the ES results for $M = 20$.

tion between the channel samples $\rho^t = 0.1$ which is shown to be sufficient in the SKG applications [47]. We have also accounted for the EPS scheme. It can be observed that our algorithm outperforms the ES when direct and indirect probing samples are jointly considered in the SKG process. The gap between the two approaches becomes significant in high SNRs. Moreover, when we utilize only the indirect probing samples, the two algorithms lead nearly to the same rate. However, our algorithm is considerably time efficient compared to the ES.

VII. Conclusion

In this contribution, for the first time, we took into account the impact of spatial correlation between the RIS elements to study its impact on the SKG in a quasi-static environment. We showed that in comparison to the widely considered random independent phase shifts between the elements, EPS can lead to a higher KGR in most cases. We further proposed to exploit the randomness of direct and randomly configured sub-reflective channels separately to avoid a strong correlation between the symbols of generated random key sequence. Moreover, we showed that it is vital to optimally allocate the direct and indirect time for probing the channel in each coherence time as the limited power can lead to significant CEE. Accordingly, we proposed an SCP based algorithm which is shown to be accurate and time efficient.

Appendix A

Based on (7), we consider two channel samples, namely s^{p_1} and s^{p_2} as

$$s^{p_1} = h_{ij} + \mathbf{h}_{rj}^H \mathbf{\Phi}^{p_1} \mathbf{h}_{ir} + \hat{n}_j^{p_1}, \tag{51}$$
$$s^{p_2} = h_{ij} + \mathbf{h}_{rj}^H \mathbf{\Phi}^{p_2} \mathbf{h}_{ir} + \hat{n}_j^{p_2}. \tag{52}$$

We seek to calculate the cross correlation $\mathbb{E}[s^{p_1} {s^{p_2}}^*]$ and the variance $\mathbb{E}\left[|s^{p_l}|^2\right]$, $l \in \{1, 2\}$. Accordingly, for the cross correlation we can write

$$\begin{aligned}\mathbb{E}\left[s^{p_1} {s^{p_2}}^*\right] &= \mathbb{E}\left[|h_{ij}|^2\right] + \mathbb{E}\left[\mathbf{h}_{rj}^H \mathbf{\Phi}^{p_1} \mathbf{h}_{ir} {\mathbf{h}_{ir}}^H {\mathbf{\Phi}^{p_2}}^H \mathbf{h}_{rj}\right] \\ &= \sigma_{ij}^2 + \mathbb{E}\left[\mathrm{tr}\left\{\mathbf{h}_{ir} {\mathbf{h}_{ir}}^H {\mathbf{\Phi}^{p_2}}^H \mathbf{h}_{rj} \mathbf{h}_{rj}^H \mathbf{\Phi}^{p_1}\right\}\right] \\ &= \sigma_{ij}^2 + \mathrm{tr}\left\{\mathbf{R}_{ir} \mathbb{E}\left[{\mathbf{\Phi}^{p_2}}^H\right] \mathbf{R}_{jr} \mathbb{E}\left[\mathbf{\Phi}^{p_1}\right]\right\}. \end{aligned} \tag{53}$$

Additionally, for the variance we have

$$\begin{aligned}\mathbb{E}\left[|s^{p_l}|^2\right] &= \mathbb{E}\left[|h_{ij}|^2\right] + \mathbb{E}\left[\mathbf{h}_{rj}^H \mathbf{\Phi}^{p_l} \mathbf{h}_{ir} {\mathbf{h}_{ir}}^H {\mathbf{\Phi}^{p_l}}^H \mathbf{h}_{rj}\right] + \hat{\sigma}_j^2 \\ &= \sigma_{ij}^2 + \mathbb{E}\left[\mathrm{tr}\left\{\mathbf{h}_{rj}^H \mathbf{\Phi}^{p_l} \mathbf{h}_{ir} {\mathbf{h}_{ir}}^H {\mathbf{\Phi}^{p_l}}^H \mathbf{h}_{rj}\right\}\right] + \hat{\sigma}_j^2 \\ &= \sigma_{ij}^2 + \mathbb{E}\left[\mathrm{tr}\left\{\mathbf{h}_{ir} {\mathbf{h}_{ir}}^H {\mathbf{\Phi}^{p_l}}^H \mathbf{h}_{rj} \mathbf{h}_{rj}^H \mathbf{\Phi}^{p_l}\right\}\right] + \hat{\sigma}_j^2 \\ &= \sigma_{ij}^2 + \mathrm{tr}\left\{\mathbb{E}\left[\mathbf{h}_{ir} {\mathbf{h}_{ir}}^H\right] \mathbb{E}\left[{\mathbf{\Phi}^{p_l}}^H \mathbf{h}_{rj} \mathbf{h}_{rj}^H \mathbf{\Phi}^{p_l}\right]\right\} + \hat{\sigma}_j^2 \\ &= \sigma_{ij}^2 + \mathbb{E}\left[\mathrm{tr}\left\{\mathbf{h}_{rj} \mathbf{h}_{rj}^H \mathbf{\Phi}^{p_l} \mathbf{R}_{ir} {\mathbf{\Phi}^{p_l}}^H\right\}\right] + \hat{\sigma}_j^2 \\ &= \sigma_{ij}^2 + \mathrm{tr}\left\{\mathbb{E}\left[\mathbf{h}_{rj} \mathbf{h}_{rj}^H\right] \mathbb{E}\left[\mathbf{\Phi}^{p_l} \mathbf{R}_{ir} {\mathbf{\Phi}^{p_l}}^H\right]\right\} + \hat{\sigma}_j^2 \\ &= \sigma_{ij}^2 + \mathrm{tr}\left\{\mathbb{E}\left[\mathbf{R}_{ir} {\mathbf{\Phi}^{p_l}}^H \mathbf{R}_{jr} \mathbf{\Phi}^{p_l}\right]\right\} + \hat{\sigma}_j^2. \end{aligned} \tag{54}$$

Substituting into $\rho^{(p_1,p_2)} = \frac{\mathbb{E}[s^{p_1} {s^{p_2}}^*]}{\mathbb{E}[|s^{p_l}|^2]}$, we obtain the expression in (13).

Appendix B

Based on (8), we consider two channel samples, namely s^{p_1} and s^{p_2} as

$$s^{p_1} = \mathbf{h}_{rj}^H \mathbf{\Phi}^{p_1} \mathbf{h}_{ir} + \hat{z}_j^{p_1}, \tag{55}$$
$$s^{p_2} = \mathbf{h}_{rj}^H \mathbf{\Phi}^{p_2} \mathbf{h}_{ir} + \hat{z}_j^{p_2}. \tag{56}$$

We need to calculate the cross correlation between the above samples. Accordingly, we have

$$\begin{aligned}\mathbb{E}\left[s^{p_1} {s^{p_2}}^*\right] &= \mathbb{E}\left[\mathbf{h}_{rj}^H \mathbf{\Phi}^{p_1} \mathbf{h}_{ir} {\mathbf{h}_{ir}}^H {\mathbf{\Phi}^{p_2}}^H \mathbf{h}_{rj}\right] + \mathbb{E}\left[\hat{z}_j^{p_1} {\hat{z}_j^{p_2}}^*\right] \\ &\overset{(53)}{=} \mathrm{tr}\left\{\mathbf{R}_{ir} \mathbb{E}\left[{\mathbf{\Phi}^{p_2}}^H\right] \mathbf{R}_{jr} \mathbb{E}\left[\mathbf{\Phi}^{p_1}\right]\right\} + \mathbb{E}\left[\hat{z}_j^{p_1} {\hat{z}_j^{p_2}}^*\right] \\ &\overset{(a)}{=} \mathrm{tr}\left\{\mathbf{R}_{ir} \mathbb{E}\left[{\mathbf{\Phi}^{p_2}}^H\right] \mathbf{R}_{jr} \mathbb{E}\left[\mathbf{\Phi}^{p_1}\right]\right\} + \hat{\sigma}_{j,k}^2, \end{aligned} \tag{57}$$

where (a) holds because $\mathbb{E}\left[\hat{z}_j^{p_1} {\hat{z}_j^{p_2}}^*\right] = \mathbb{E}\left[\hat{n}_{j,k} \hat{n}_{j,k}^*\right] = \hat{\sigma}_{j,k}^2$. Moreover,

$$\begin{aligned}\mathbb{E}\left[|s^{p_l}|^2\right] &= \mathbb{E}\left[\mathbf{h}_{rj}^H \mathbf{\Phi}^{p_l} \mathbf{h}_{ir} {\mathbf{h}_{ir}}^H {\mathbf{\Phi}^{p_l}}^H \mathbf{h}_{rj}\right] + \mathbb{E}\left[|\hat{z}_j^{p_l}|^2\right] \\ &\overset{(54)}{=} \mathrm{tr}\left\{\mathbb{E}\left[\mathbf{R}_{ir} {\mathbf{\Phi}^{p_l}}^H \mathbf{R}_{jr} \mathbf{\Phi}^{p_l}\right]\right\} + \mathbb{E}\left[|\hat{z}_j^{p_l}|^2\right] \\ &= \mathrm{tr}\left\{\mathbb{E}\left[\mathbf{R}_{ir} {\mathbf{\Phi}^{p_l}}^H \mathbf{R}_{jr} \mathbf{\Phi}^{p_l}\right]\right\} + \hat{\sigma}_{z_j}^2. \end{aligned} \tag{58}$$

. Finally, substituting into $\rho^{(p_1,p_2)} = \frac{\mathbb{E}[s^{p_1} {s^{p_2}}^*]}{\mathbb{E}[|s^{p_l}|^2]}$, we obtain the expression in (18).

Appendix C

We consider the mutual information term associated with the indirect path in (12) as the calculations for the direct path term is similar and straightforward. Since we showed that $\mathbf{h}_{ri}^H \mathbf{\Phi}^p \mathbf{h}_{jr}$, $i, j \in \{a, b, e\}$ terms in (8) have complex normal

distribution for $N \gg 1$, the conditional mutual information can be calculated as

$$I\left(h_a^p; h_b^p | h_{ae}^p, h_{be}^p\right) = H(h_a^p, h_{ae}^p, h_{be}^p) + H(h_b^p, h_{ae}^p, h_{be}^p) - H(h_a^p, h_b^p, h_{ae}^p, h_{be}^p) - H(h_{ae}^p, h_{be}^p) = \log_2 \frac{\det(\mathbf{M}_{aaebe}) \det(\mathbf{M}_{baebe})}{\det(\mathbf{M}_{aebe}) \det(\mathbf{M}_{abaebe})}, \quad (59)$$

where $\det(.)$ is the matrix determinant, and

$$\mathbf{M}_{abaebe} = \mathbb{E}\left[\begin{pmatrix} h_a^p \\ h_b^p \\ h_{ae}^p \\ h_{be}^p \end{pmatrix} \begin{pmatrix} h_a^{p^*} & h_b^{p^*} & h_{ae}^{p^*} & h_{be}^{p^*} \end{pmatrix}\right] = \begin{bmatrix} \eta_{aa} & \eta_{ab} & \eta_{aae} & \eta_{abe} \\ \eta_{ba} & \eta_{bb} & \eta_{bae} & \eta_{bbe} \\ \eta_{aea} & \eta_{aeb} & \eta_{aeae} & \eta_{aebe} \\ \eta_{bea} & \eta_{beb} & \eta_{beae} & \eta_{bebe} \end{bmatrix}, \quad (60)$$

where $\eta_{mn} = \mathbb{E}\left[h_m^p h_n^{p^*}\right]$, $m, n \in \{a, b, ae, be\}$ is the correlation function. Obtaining the expressions for $\eta_{aa}, \eta_{bb}, \eta_{aeae}, \eta_{bebe}, \eta_{ab} = \eta_{ba}$ is straightforward by following the steps in obtaining $\mathbb{E}\left[|s^{p_l}|^2\right]$ in Section III. For the other terms, e.g., η_{aebe}, we have

$$\begin{aligned} \eta_{aebe} &= \mathbb{E}\left[h_{ae}^p h_{be}^{p^*}\right] = \mathbb{E}\left[\mathbf{h}_{re}^H \mathbf{\Phi}^p \mathbf{h}_{ar} \mathbf{h}_{br}^H \mathbf{\Phi}^{p^H} \mathbf{h}_{re}\right] \\ &= \mathrm{tr}\left\{\mathbb{E}\left[\mathbf{\Phi}^p \mathbf{h}_{ar} \mathbf{h}_{br}^H \mathbf{\Phi}^{p^H}\right] \mathbb{E}\left[\mathbf{h}_{re} \mathbf{h}_{re}^H\right]\right\} \\ &= \mathbb{E}\left[\mathrm{tr}\left\{\mathbf{h}_{ar} \mathbf{h}_{br}^H \mathbf{\Phi}^{p^H} \mathbf{R}_{re} \mathbf{\Phi}^p\right\}\right] \\ &= \mathrm{tr}\left\{\mathbb{E}\left[\mathbf{h}_{ar} \mathbf{h}_{br}^H\right] \mathbb{E}\left[\mathbf{\Phi}^{p^H} \mathbf{R}_{re} \mathbf{\Phi}^p\right]\right\} \\ &= \mathrm{tr}\left\{\mathbf{R}_{ar}^{\frac{1}{2}} \mathbb{E}\left[\mathbf{g}_{ar} \mathbf{g}_{br}^H\right] \mathbf{R}_{br}^{\frac{1}{2}^H} \mathbb{E}\left[\mathbf{\Phi}^{p^H} \mathbf{R}_{re} \mathbf{\Phi}^p\right]\right\} \\ &\overset{(a)}{=} \rho_{ab} \mathrm{tr}\left\{\mathbb{E}\left[\mathbf{R}_{ar}^{\frac{1}{2}} \mathbf{R}_{br}^{\frac{1}{2}} \mathbf{\Phi}^{p^H} \mathbf{R}_{re} \mathbf{\Phi}^p\right]\right\} \\ &\overset{(b)}{=} \rho_{ab} \sqrt{\kappa_{ar}} \sqrt{\kappa_{br}} \kappa_{re} \mathrm{tr}\left\{\mathbf{R} \odot \mathbf{R}\right\}, \end{aligned} \quad (61)$$

where (a) holds because, $\mathbf{h}_{ir} = \mathbf{R}_{ir}^{\frac{1}{2}} \mathbf{g}_{ir}$, $i \in \{a, b\}$, $\mathbb{E}\left[\mathbf{g}_{ar} \mathbf{g}_{br}^H\right] = \rho_{ab} \mathbf{I}$ and (b) is deduced based on the proofs of lemmas 1 and 2. Following the same steps, other correlation terms in (60) can be obtained. Similarly, the determinants of the other matrices in (59) are calculated.

REFERENCES

[1] National Institute of Standards and Technology (1979). "FIPS-46: Data Encryption Standard (DES)." Revised as FIPS 46-1:1988, FIPS 46-2:1993, FIPS 46-3:1999

[2] N. F. Pub, "197: Advanced encryption standard (AES)," Federal Inf. Process. Standards, vol. 197, no. 441, p. 0311, 2001.

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 26, no. 1, pp. 9699, Jan. 1983.

[4] A. D. Wyner, "Wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 13551387, Oct. 1975.

[5] A. Kuhestani, A. Mohammadi and P. L. Yeoh, "Security-reliability trade-off in cyber-physical cooperative systems with non-ideal untrusted relaying," *IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, 2018, pp. 552557.

[6] M. Letafati, A. Kuhestani, and H. Behroozi, "Three-hop untrusted relay networks with hardware imperfections and channel estimation errors for Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 28562868, Mar. 2020.

[7] A. Kuhestani, A. Mohammadi, and M. Mohammadi "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol 13, no. 2, pp. 341355, Feb. 2018.

[8] M. Forouzesh, P. Azmi, A. Kuhestani and P. L. Yeoh, "Joint Information-Theoretic Secrecy and Covert Communication in the Presence of an Untrusted User and Warden," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7170-7181, 1 May1, 2021, doi: 10.1109/JIOT.2020.3038682.

[9] M. Forouzesh, F. S. Khodadad, P. Azmi, A. Kuhestani and H. Ahmadi, "Simultaneous Secure and Covert Transmissions Against Two Attacks Under Practical Assumptions," *IEEE Internet Things J.*, doi: 10.1109/JIOT.2023.3237640.

[10] J. Zhang, G. Li, A. Marshall, A. Hu and L. Hanzo, "A New Frontier for IoT Security Emerging From Three Decades of Key Generation Relying on Wireless Channels," *IEEE Access*, vol. 8, pp. 138406-138446, 2020, doi: 10.1109/ACCESS.2020.3012006.

[11] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16-20, June 2015, doi: 10.1109/MCOM.2015.7120011.

[12] M. Letafati, A. Kuhestani, K. -K. Wong and M. J. Piran, "A Lightweight Secure and Resilient Transmission Scheme for the Internet of Things in the Presence of a Hostile Jammer," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4373-4388, 15 March15, 2021, doi: 10.1109/JIOT.2020.3026475.

[13] M. Letafati, A. Kuhestani, H. Behroozi and D. W. K. Ng, "Jamming-Resilient Frequency Hopping-Aided Secure Communication for Internet-of-Things in the Presence of an Untrusted Relay," *IEEE Trans. Wireless Commun.*, vol. 19, no. 10, pp. 6771-6785, Oct. 2020, doi: 10.1109/TWC.2020.3006012.

[14] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the Internet of things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 12941312, 3rd Quart., 2015.

[15] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614626, 2016.

[16] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116-120, Feb. 2017.

[17] J. Wallace, "Secure physical layer key generation schemes: Performance and information theoretic limits," *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 943947.

[18] C. Huth, R. Guillaume, T. Strohm, P. Duplys, I. A. Samuel, and T. Gneysu, "Information reconciliation schemes in physical-layer security: A survey," *Comput. Netw.*, vol. 109, pp. 84104, Nov. 2016.

[19] C. H. Bennett, G. Brassard, C. Crpeau, and U. M. Maurer, "Generalized privacy amplification,"*IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 19151923, Nov. 1995.

[20] A. F. Molisch, Wireless Communications, vol. 34. Hoboken, NJ, USA: Wiley, 2012.

[21] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 26922705, Feb. 2020.

[22] H. Taha and E. Alsusa, Secret key exchange using private random precoding in MIMO FDD and TDD systems, *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 48234833, Jun. 2017.

[23] Y. Chen, K. Huang, Y. Zhou, K. Ma, H. Jin, and X. Xu, Physical layer key generation scheme through scrambling the correlated eavesdropping channel, *IEEE Access*, vol. 8, pp. 4898248990, 2020.

[24] Z. Ji et al., "Random Shifting Intelligent Reflecting Surface for OTP Encrypted Data Transmission," *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1192-1196, June 2021, doi: 10.1109/LWC.2021.3061549.

[25] T. Lu, L. Chen, J. Zhang, K. Cao and A. Hu, "Reconfigurable Intelligent Surface Assisted Secret Key Generation in Quasi-Static Environments," *IEEE Commun. Lett.*, vol. 26, no. 2, pp. 244-248, Feb. 2022, doi: 10.1109/LCOMM.2021.3130635.

[26] Z. Wei, W. Guo and B. Li, "A Multi-Eavesdropper Scheme Against RIS Secured LoS-Dominated Channel," *IEEE Commun. Lett.*, vol. 26, no. 6, pp. 1221-1225, June 2022, doi: 10.1109/LCOMM.2022.3166239.

[27] S. Yang, H. Han, Y. Liu, W. Guo, Z. Pang, and L. Zhang, "Reconfigurable Intelligent Surface-induced Randomness for mmWave Key Generation," *arXiv:2111.00428 [eess]*, Aug. 2022. [Online]. Available: https://arxiv.org/abs/2111.00428

[28] Z. Wei and W. Guo, "Random Matrix based Physical Layer Secret Key Generation in Static Channels," *arXiv:2110.12785 [cs, eess, math]*, Oct. 2021. [Online]. Available: https://arxiv.org/abs/2110.12785

[29] 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 Commun. Lett.*, vol. 10, no. 9, pp. 1867-1870, Sept. 2021, doi: 10.1109/LWC.2021.3084347.

[30] 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," *IEEE 32nd Annu. Int. Symp. on Pers., Indoor and Mobile Radio Commun. (PIMRC)*, 2021, pp. 745-751, doi: 10.1109/PIMRC50174.2021.9569556.

[31] Z. Ji et al., "Secret Key Generation for Intelligent Reflecting Surface Assisted Wireless Communication Networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 1030-1034, Jan. 2021, doi: 10.1109/TVT.2020.3045728.

[32] X. Lu, J. Lei, Y. Shi and W. Li, "Intelligent Reflecting Surface Assisted Secret Key Generation," *IEEE Signal Process. Lett.*, vol. 28, pp. 1036-1040, 2021, doi: 10.1109/LSP.2021.3061301.

[33] G. Li, C. Sun, W. Xu, M. D. Renzo and A. Hu, "On Maximizing the Sum Secret Key Rate for Reconfigurable Intelligent Surface-Assisted Multiuser Systems," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 211-225, 2022, doi: 10.1109/TIFS.2021.3138612.

[34] Y. Chen, G. Li, C. Pan, L. Hu, and A. Hu, "Intelligent Reflecting Surface-Assisted Secret Key Generation In Multi-antenna Network," *arXiv:2105.00511 [cs, math]*, May 2021. [Online]. Available: https://arxiv.org/abs/2105.00511

[35] G. Li et al., "Reconfigurable Intelligent Surface for Physical Layer Key Generation: Constructive or Destructive?," *IEEE Wireless Commun.*, doi: 10.1109/MWC.007.2100545.

[36] L. Hu, G. Li, H. Luo and A. Hu, "On the RIS Manipulating Attack and Its Countermeasures in Physical-layer Key Generation," 2021 *IEEE 94th Veh. Technol. Conf.* (VTC2021-Fall), 2021, pp. 1-5, doi: 10.1109/VTC2021-Fall52928.2021.9625442.

[37] E. Bjrnson and L. Sanguinetti,"Rayleigh Fading Modeling and Channel Hardening for Reconfigurable Intelligent Surfaces," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 830-834, April 2021, doi: 10.1109/LWC.2020.3046107.

[38] A. Papazafeiropoulos, C. Pan, A. Elbir, P. Kourtessis, S. Chatzinotas and J. M. Senior, "Coverage Probability of Distributed IRS Systems Under Spatially Correlated Channels," *IEEE Wireless Commun. Lett.*, vol. 10, no. 8, pp. 1722-1726, Aug. 2021, doi: 10.1109/LWC.2021.3077991.

[39] A. P. Ajayan, S. P. Dash and B. Ramkumar, "Performance Analysis of an IRS-Aided Wireless Communication System With Spatially Correlated Channels," *IEEE Wireless Commun. Lett.,* vol. 11, no. 3, pp. 563-567, March 2022, doi: 10.1109/LWC.2021.3136210.

[40] A. Papazafeiropoulos, P. Kourtessis, S. Chatzinotas and J. M. Senior, "Coverage Probability of Double-IRS Assisted Communication Systems," *IEEE Wireless Commun. Lett.,* vol. 11, no. 1, pp. 96-100, Jan. 2022, doi: 10.1109/LWC.2021.3121209.

[41] T. Van Chien, A. K. Papazafeiropoulos, L. T. Tu, R. Chopra, S. Chatzinotas and B. Ottersten, "Outage Probability Analysis of IRS-Assisted Systems Under Spatially Correlated Channels," *IEEE Wireless Commun. Lett.,* vol. 10, no. 8, pp. 1815-1819, Aug. 2021, doi: 10.1109/LWC.2021.3082409.

[42] A. Papazafeiropoulos, "Ergodic Capacity of IRS-Assisted MIMO Systems With Correlation and Practical Phase-Shift Modeling," *IEEE Wireless Commun. Lett.*, vol. 11, no. 2, pp. 421-425, Feb. 2022, doi: 10.1109/LWC.2021.3131401.

[43] C. Psomas and I. Krikidis, "SWIPT With Intelligent Reflecting Surfaces Under Spatial Correlation," *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 1924-1928, Sept. 2021, doi: 10.1109/LWC.2021.3086430.

[44] Q. Tao, S. Zhang, C. Zhong and R. Zhang, "Intelligent Reflecting Surface Aided Multicasting With Random Passive Beamforming," *IEEE Wireless Commun. Lett.*, vol. 10, no. 1, pp. 92-96, Jan. 2021, doi: 10.1109/LWC.2020.3021473.

[45] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733-742, May 1993, doi: 10.1109/18.256484.

[46] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121-1132, July 1993, doi: 10.1109/18.243431.

[47] J. Zhang, A. Marshall, R. Woods and T. Q. Duong, "Efficient Key Generation by Exploiting Randomness From Channel Responses of Individual OFDM Subcarriers," *IEEE Trans. on Commun.*, vol. 64, no. 6, pp. 2578-2588, June 2016, doi: 10.1109/TCOMM.2016.2552165.