Reconfigurable Intelligent Surface-Assisted Key Generation for Millimeter Wave Communications

Tianyu Lu*, Liquan Chen*†, Junqing Zhang‡, Chen Chen‡, Trung Q. Duong§
*School of Cyber Science and Engineering, Southeast University, Nanjing, 210096, China
†Purple Mountain Laboratories, Nanjing, 210096, China
‡Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom
§Institute of Electronics Communications & Information Technology, Queen's University Belfast, Belfast, BT7 1NN, United Kingdom
Corresponding author: Liquan Chen, Email: lqchen@seu.edu.cn

***Abstract*—Physical layer key generation (PLKG) exploits the distributed entropy source of wireless channels to generate secret keys for legitimate users. When the millimeter wave (mmWave) channel is blocked, reconfigurable intelligent surfaces (RISs) have emerged as a prospective approach to constructing reflected channels and improving the secret key rate (SKR). This paper investigates the key generation scheme for the RIS-aided mmWave system. We study the beam domain channel model and exploit the sparsity of mmWave bands to reduce the pilot overhead. We propose a channel probing method to acquire the reciprocal angular information and channel gains. To analyze the SKR, we investigate the channel covariance matrix of beam domain channels. We find that the channel gains of beams are uncorrelated which increases the randomness of secret keys. Considering an eavesdropper, we derive the analytical expressions of SKR when the eavesdropping channel has overlapping clusters with the legitimate channel. Simulations validate that the proposed PLKG scheme outperforms existing schemes.**

***Index Terms*—Reconfigurable intelligent surface, physical layer key generation, and millimeter wave communications.**

I. Introduction

Physical layer key generation (PLKG) is a promising technique for 5G and beyond to address security vulnerabilities in traditional key exchange solutions [1], e.g. Diffie-Hellman key exchange algorithm is threatened by quantum computing. PLKG exploits the properties of channel randomness, channel reciprocity, and spatial decorrelation to generate secure keys [2]. However, PLKG suffers from poor channel conditions. When the channel variation is slow, PLGK can not produce enough secret keys, such as in static environments. Also, the secret key rate (SKR), a metric to quantify the number of secret keys, declines with the decrease in the signal-to-noise ratio (SNR) if the channel is blocked by obstacles.

Recently, the reconfigurable intelligent surface (RIS) has emerged as a prospective approach to address the aforementioned challenges [3]–[6]. A RIS consisting of many discrete elements can timely configure its reflection coefficients to control the channel [7]. In single-antenna systems, the RIS can randomly tune reflection coefficients and change the wireless channel to mimic the fast-fading effects. Ji *et al.* utilize random phase shift vectors to improve the SKR in quasi-static environments [3]. Lu *et al.* derive the analytical expressions of the lower and upper bounds of the SKR in key generation systems with the random configuration of RIS [4]. Low SKR problem is solved by optimizing the phase shift vector to increase the SNR of legitimate users in [5]. Later, Li *et al.* extend the design of phase shift vectors in key generation systems in multi-user scenarios [6]. However, the above works concentrate on sub-6GHz systems and apply the rich-scattering condition to combat eavesdroppers, i.e., the channel of an eavesdropper half-wavelength away from legitimate users is uncorrelated. The condition may not be guaranteed in millimeter waves (mmWaves) communications with inherent sparsity.

The spectral band has been nearly occupied in current cellular networks and mmWave communication systems utilize the bandwidth from 30 GHz to 300 GHz to increase communication capacity. Jiao *et al.* use the angular information of the mmWave channel to create secret keys [8]. However, mmWave bands are prone to blockage effects which have a bad effect on PLKG [8]. When the direct channel is blocked, a RIS can construct a reflected channel to solve the blockage-prone problem in key generation. Our previous works in [9] investigated the RIS-assisted key generation in sub-6GHz environments. We proposed to exploit the randomness from the subchannels associated with each reflecting element. However, the pilot overhead increases with the number of antennas at transceivers and reflecting elements at RIS in the antenna domain. The wireless channels in mmWave bands exhibit sparsity, which gives the insight to construct the beam-domain channel model to reduce pilot overhead [10]. By exploring the sparsity of beam domain channels in RIS-aided systems, Zhou *et al.* propose compressed sensing (CS)-based channel estimation method with low overhead [10]. The channels in the antenna domain are highly spatial correlated, while the subchannels of the beam-domain channel are nearly uncorrelated, which makes secret keys get great randomness. Finally, different from the Gaussian channel assumption in rich-scattering environments in sub-6GHz bands, PLKG needs security analysis on the beam domain channel model.

Motivated by the above challenges, this paper investigates the RIS-assisted key generation for mmWave communications. Our main contributions are summarized as follows:

- We study a PLKG framework for RIS-assisted mmWave communications. A channel probing method based on orthogonal matching pursuit (OMP) algorithms is proposed to acquire the reciprocal spatial angles in the beam domain channel model.
- We demonstrate that the angular information of the beam domain channel changes slowly while the channel gain of each beam provides a rich randomness source for key generation. Compared to channel coefficients in the antenna domain, the channel gains of beams are sparse and uncorrelated, which greatly reduces the pilot overhead and redundancy between measurements.
- To analyze the information leakage from eavesdroppers, we investigate the channel covariance matrices of legitimate users and eavesdroppers. We find that the SKR is determined by overlapping and non-overlapping beams. The analytical expressions of SKR are derived and validated by Monte Carlo simulations.

Notations: Italic letters, boldface lower-case letters, boldface upper-case letters and calligraphic letters denote scalars, vectors, matrices and sets, respectively. diag$(\cdot)$ forms a diagonal matrix out of its vector argument. vec$(\cdot)$ is the vectorization of a matrix argument. $(\cdot)^T$, $(\cdot)^H$, $(\cdot)^{-1}$ and $(\cdot)^*$ denote the transpose, conjugate transpose, inverse, and conjugate, respectively. $\mathbb{C}^{m\times n}$ is the complex space of a $m\times n$ matrix. $\mathbb{Z}$ indicates the set of all integers. $\mathbf{I}_N$ denotes the $N\times N$ identity matrix. $\mathcal{CN}(\mu,\sigma^2)$ denotes the circularly symmetric complex Gaussian distribution with mean μ and variance σ^2. $\mathbb{E}\{\cdot\}$ denotes the statistical expectation, and $\otimes$ is the Kronecker product. $\diamond$ is the transposed Khatri-Rao product. $\mathrm{mod}\,(\cdot)$ is the modulus operator and $\lfloor\cdot\rfloor$ is the floor function.

II. System Model

A. Overview

As shown in Fig. 1, we consider a RIS mmWave system that consists of a base station (BS), a user equipment (UE), an eavesdropper (Eve), and a RIS. The direct channel between BS and UE is blocked by obstacles, where the RIS constructs a reflected link to assist the key generation process. There are several scatters around the BS and RIS, which causes the reflected link to pass different paths of clusters. Eve is located near UE to eavesdrop on the key generation process.

B. Device Configuration

A Cartesian coordinate system is considered, where a RIS is deployed in parallel to the $y-z$ plane, as shown in Fig. 1. The RIS is modelled as a uniform planar array that has $M = M_y \times M_z$ reflecting elements with M_y elements per row and M_z elements per column.

When a wave impinges on the RIS from the azimuth angle, θ, and the elevation angle, φ, the array response vector of the RIS is given by $\mathbf{a}(\theta,\varphi) = \mathbf{a}_z(\varphi)\otimes\mathbf{a}_y(\theta,\varphi)$, where $\mathbf{a}_z(\varphi) = \frac{1}{\sqrt{M_z}}[1,\ldots,e^{j2\pi(M_z-1)\frac{d}{\lambda}\sin\varphi}]^T$, $\mathbf{a}_y(\theta,\varphi) = \frac{1}{\sqrt{M_y}}[1,\ldots,e^{j2\pi(M_y-1)\frac{d}{\lambda}\cos\varphi\sin\theta}]^T$, λ is the wavelength and d is the side length of a reflecting element. The reflection

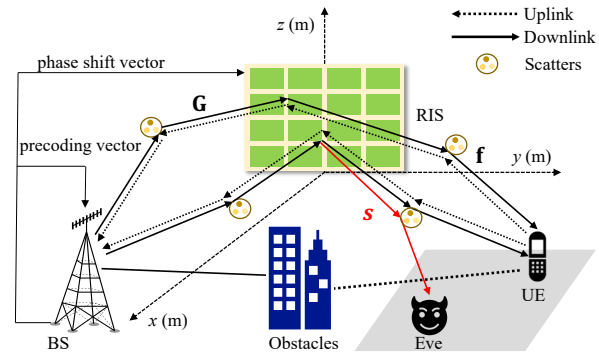

Fig. 1. System model.

coefficients of M reflecting elements are denoted as $\mathbf{v} = [\phi_1,\ldots,\phi_M]^T$, where $\phi_m = e^{j\omega_m}$ is the reflection coefficient of the m-th element and ω_m is its phase shift.

The BS is equipped with a uniform linear array consisting of N antennas and located on the x-axis with d_a antenna spacing. When a wave impinges on the BS from an azimuth angle, ψ, the array response vector is $\mathbf{b}(\psi) = \frac{1}{\sqrt{N}}[1,\ldots,e^{j2\pi(N-1)\frac{d_a}{\lambda}\sin\psi}]^T$. The BS applies a precoding vector, $\mathbf{w}\in\mathbb{C}^{N\times 1}$, or precoding matrix, $\mathbf{P}\in\mathbb{C}^{N\times P}$, for transmission or reception.

C. Channel Model

1) Individual Channel: In full-scattering sub-6GHz environments, the channels can be modelled as complex Gaussian matrices. For example, the BS-RIS channel that experiences the paths from different spatial angles is $\mathbf{G} = \mathbf{R}_r^{H/2}\mathbf{G}_w\mathbf{R}_a^{H/2}$, where $\mathbf{G}_w \sim \mathcal{CN}(0,\mathbf{I})$, and $\mathbf{R}_r$ and $\mathbf{R}_a$ are the channel covariance matrix at RIS and BS, respectively. However, the scattering paths in mmWave channels are not enough to model the channel as a complex matrix. Instead, the geometric channel model is widely used for mmWave channels.

There are four individual channels, including BS-RIS, UE-RIS, UE-BS, and Eve-RIS channels. The small-scale fading for all channels is assumed to be Rayleigh fading.

The BS-RIS channel is modeled as a function of spatial angles and channel gains of paths of clusters, given by

$$\mathbf{G} = \sqrt{\frac{MN}{\beta_g K_g}}\sum_{l_g=1}^{L_g}\sum_{k=1}^{K_{l_g}} g_{l_g,k}\mathbf{a}(\theta_{l_g}^g,\varphi_{l_g}^g)\mathbf{b}^H(\psi_{l_g,k}^g), \quad (1)$$

where $\mathbf{G}\in\mathbb{C}^{M\times N}$, β_g is the path-loss effect, $K_g = \sum_{l_g} K_{l_g}$ is the number of paths of L_g clusters, $g_{l_g,k}$ denotes the corresponding complex gain associated with the l_g-th cluster and the k-th path, $\psi_{l_g,k}^g$ denotes the angle of departure (AoD), and $\theta_{l_g}^g$ and $\varphi_{l_g}^g$ denote the azimuth and elevation angle of arrival (AoA), respectively. The complex gain, $g_{l_g,k}$, is identically and independently distributed (i.i.d.) $\mathcal{CN}(0,\sigma_g^2)$.

The UE-RIS channel is modelled as

$$\mathbf{f} = \sqrt{\frac{M}{\beta_f K_f}}\sum_{l_f=1}^{L_f}\sum_{k=1}^{K_{l_f}} f_{l_f,k}\mathbf{a}(\theta_{l_f,k}^f,\varphi_{l_f,k}^f), \quad (2)$$

where $\mathbf{f} \in \mathbb{C}^{M\times 1}$, β_f is the path-loss effect, $K_f = \sum_{l_f} K_{l_f}$ is the number of paths of L_f clusters, $f_{l_f,k}$ denotes the complex gain associated with the l_f-th cluster and k-th path, and $\theta^f_{l_f,k}$ and $\varphi^f_{l_f,k}$ denote the azimuth and elevation AoA, respectively. The complex gain, $f_{l_f,k}$, is i.i.d. $\mathcal{CN}(0,\sigma_f^2)$.

The Eve-RIS channel is similarly modelled as $\mathbf{s} = \sqrt{\frac{M}{\beta_s K_s}} \sum_{l_s=1}^{L_s} \sum_{k=1}^{K_{l_s}} s_{l_s,k}\mathbf{a}(\theta^s_{l_s,k}, \varphi^s_{l_s,k})$, where $\mathbf{f} \in \mathbb{C}^{M\times 1}$, β_s is the path-loss effect, $K_s = \sum_{l_s} K_{l_s}$ is the number of paths of L_s clusters, $s_{l_s,k}$ denotes the complex gain associated with the l_s-th cluster and k-th path, $\theta^s_{l_s,k}$ and $\varphi^s_{l_s,k}$ denote the azimuth and elevation AoA of the l_s-th path, respectively. The complex gain, $s_{l_s,k}$, is i.i.d. $\mathcal{CN}(0,\sigma_s^2)$.

2) Sparse Cascaded Channel: We define the RIS-controlled channel as the cascaded channel, which is given by

$$\mathbf{h}_c(\mathbf{v}) = \mathbf{G}^H \mathrm{diag}(\mathbf{v})\mathbf{f} = \mathbf{G}^H \mathrm{diag}(\mathbf{f})\mathbf{v} = \mathbf{H}\mathbf{v}, \tag{3}$$

where $\mathbf{h}_c(\mathbf{v}) \in \mathbb{C}^{N\times 1}$, and $\mathbf{H} = [\mathbf{h}_1 \ldots, \mathbf{h}_M]$ is the channel associated with M reflecting elements. The BS and UE can directly measure the cascaded channel and convert their measurements to secret keys, which is commonly adopted by previous works [5], [6]. However, the cascaded channel is coarse-grained. The dimension of the cascaded channel in the antenna domain is N, which fundamentally limits the SKR. Furthermore, our previous work in [9] proposed to extract secret keys from massive subchannels associated with each reflecting element, $\mathbf{h}_m$, $m = 1,\ldots,M$, which extends the dimension of channels for key generation from N to NM. However, to estimate $\mathbf{h}_m$, Alice and Bob should transmit multiple rounds of the pilot to each other with the pilot overhead of at least M, which is challenging to key generation.

We note that the mmWave channels with extremely high carrier frequency exhibit angular sparsity. There are only a few multipath components with different AoDs and AoAs between the BS and UE, which is helpful for reducing pilot overhead. Therefore, we consider the virtual beam-domain representation of the discrete physical model (geometric channel model) to elaborate on the sparsity of the RIS mmWave channels.

The BS-RIS channel (1) can be rewritten as $\mathbf{G} = \mathbf{A}_g\mathbf{\Lambda}_g\mathbf{A}_N^H$, where $\mathbf{A}_g = [\mathbf{a}(\theta^g_1,\varphi^g_1),\ldots,\ldots,\mathbf{a}(\theta^g_{L_g},\varphi^g_{L_g})]$, $\mathbf{A}_g \in \mathbb{C}^{M\times L_g}$, $\mathbf{A}_N = [\mathbf{b}(\psi^g_{1,1}),\ldots,\mathbf{b}(\psi^g_{L_g,K_{L_g}})]$ and $\mathbf{A}_N \in \mathbb{C}^{N\times K_g}$. The matrix $\mathbf{A}_g$ and $\mathbf{A}_N$ represent the AoAs and AoDs, respectively. $\mathbf{\Lambda}_g \in \mathbb{C}^{L_g\times K_g}$, is the beam-domain channel with L_gK_g non-zero entries along the diagonal line.

The UE-RIS channel (2) is rewritten as $\mathbf{f} = \mathbf{A}_f\mathbf{c}_f$, where $\mathbf{A}_f = [\mathbf{a}(\theta^f_{1,1},\varphi^f_{1,1}),\ldots,\mathbf{a}(\theta^f_{L_f,K_{L_f}},\varphi^f_{L_f,K_{L_f}})]$, $\mathbf{A}_f \in \mathbb{C}^{M\times K_f}$, $\mathbf{c}_f = [f_{1,1},\ldots,f_{L_f,K_{L_f}}]$ and $\mathbf{c}_f \in \mathbb{C}^{K_f\times 1}$.

Based on (3), the cascaded channel $\mathbf{H}$ is simplified as

$$\begin{aligned}\mathbf{H}^H &= (\mathbf{A}_f^*\mathbf{c}_f^*)\diamond(\mathbf{A}_g\mathbf{\Lambda}_g\mathbf{A}_N^H) \overset{(a)}{=} \mathbf{A}_f^*\diamond\mathbf{A}_g(\mathbf{c}_f^*\otimes(\mathbf{\Lambda}_g\mathbf{A}_N^H)) \\ &\overset{(b)}{=} \mathbf{A}_f^*\diamond\mathbf{A}_g(\mathbf{c}_f^*\otimes\mathbf{\Lambda}_g)(1\otimes\mathbf{A}_N^H) = \mathbf{A}_M\mathbf{\Lambda}\mathbf{A}_N^H,\end{aligned} \tag{4}$$

where $\mathbf{H} \in \mathbb{C}^{N\times M}$, $\mathbf{A}_M = \mathbf{A}_f^*\diamond\mathbf{A}_g$, $\mathbf{A}_M \in \mathbb{C}^{M\times L_gK_f}$, $\mathbf{\Lambda} = \mathbf{c}_f^*\otimes\mathbf{\Lambda}_g$, and $\mathbf{\Lambda} \in \mathbb{C}^{L_gK_f\times K_g}$. (a) holds due to the property of transposed Khatri-Rao product, i.e., $(\mathbf{AC})\diamond(\mathbf{BD}) = (\mathbf{A}\diamond\mathbf{B})(\mathbf{C}\otimes\mathbf{D})$. (b) holds due to the property of Kronecker product, i.e., $(\mathbf{AC})\otimes(\mathbf{BD}) = (\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D})$. Therefore, $\mathbf{H} = \mathbf{A}_N(\mathbf{c}_f^T\otimes\mathbf{\Lambda}_g^H)\mathbf{A}_M^H$.

The geometric channel model (4) exhibits the sparsity of the mmWave channels. The CS-based channel estimation methods can be used to measure sparse channels [10]. Therefore, we transform the channel (4) into the virtual beam-domain channel, i.e., $\mathbf{H} = \mathbf{U}\widetilde{\mathbf{H}}\mathbf{V}^H$, where $\mathbf{U} \in \mathbb{C}^{N\times N}$ and $\mathbf{V} \in \mathbb{C}^{M\times M}$ are the unitary matrices at the BS and the RIS, respectively.

The unitary matrices $\mathbf{U}$ and $\mathbf{V}$ consist of some samples of spatial angles. We set $\mathbf{U} = [\mathbf{b}(\psi_1),\ldots,\mathbf{b}(\psi_N)]$, where ψ_n, $n = 1,\ldots,N$, is the predefined spatial angle at the BS. Define $\bar{\psi}_n = \frac{d}{\lambda}\sin\psi_n = \frac{1}{N}(n - \frac{N+1}{2})$ as the virtual spatial angle at the BS. Also, we set $\mathbf{V} = \mathbf{V}_z\otimes\mathbf{V}_y$, where $\mathbf{V}_z = [\mathbf{a}_z(\varphi_1),\ldots,\mathbf{a}_z(\varphi_{M_z})]$, $\mathbf{V}_z \in \mathbb{C}^{M_z\times M_z}$, $\mathbf{V}_y = [\mathbf{a}_y(\theta_1,\varphi_1),\ldots,\mathbf{a}_y(\theta_{M_y},\varphi_{M_y})]$ and $\mathbf{V}_y \in \mathbb{C}^{M_y\times M_y}$. Define $\bar{\varphi}_{n_z} = \frac{d}{\lambda}\sin\varphi_{n_z} = \frac{1}{M_z}(n_z - \frac{M_z+1}{2})$, $n_z = 1,\ldots,M_z$, as the virtual elevation angle, where φ_{n_z} are the predefined elevation angle. Define $\bar{\theta}_{n_y} = \frac{d}{\lambda}\cos\varphi_{n_y}\sin\theta_{n_y} = \frac{1}{M_y}(n_y - \frac{M_y+1}{2})$ as the virtual azimuth angle, $n_y = 1,\ldots,M_y$, where θ_{n_y} are the predefined azimuth angle.

Based on (2) and (1), the virtual channel representation of the beam-domain channel $\widetilde{\mathbf{H}} = \mathbf{U}^H\mathbf{H}\mathbf{V}$ is given by

$$\begin{aligned}\widetilde{\mathbf{H}} &= \sum_{l_g=1}^{L_g}\sum_{k_g=1}^{K_{l_g}}\sum_{l_f=1}^{L_f}\sum_{k_f=1}^{K_{l_f}} g^*_{l_g,k_g} f_{l_f,k_f}\mathbf{U}^H\mathbf{b}(\psi^g_{l_g,k_g}) \\ &\times \mathbf{a}^H(-\theta^f_{l_f,k_f}+\theta^g_{l_g}, -\varphi^f_{l_f,k_f}+\varphi^g_{l_g})\mathbf{V} \\ &\overset{(c)}{\approx} \sum_{l_g=1}^{L_g}\sum_{k_g=1}^{K_{l_g}}\sum_{l_f=1}^{L_f}\sum_{k_f=1}^{K_{l_f}} g^*_{l_g,k_g} f_{l_f,k_f}\delta(\bar{\psi}-\bar{\psi}^g_{l_g,k_g}) \\ &\times \delta(\bar{\theta}+\bar{\theta}^f_{l_f,k_f}-\bar{\theta}^g_{l_g})\delta(\bar{\varphi}+\bar{\varphi}^f_{l_f,k_f}-\bar{\varphi}^g_{l_g}),\end{aligned} \tag{5}$$

where (c) holds on if $M\to\infty$ and $N\to\infty$. The proof will be given in our journal version. Similarly, we can get the virtual channel representation of Eve's beam-domain channel.

III. RIS-ASSISTED BEAM-DOMAIN CHANNEL PROBING

Compared to rapidly-varying channel gains, the physical positions of BS and RIS vary much more gradually. Thus, it is plausible to suppose that over several channel coherence blocks, the AoAs and AoDs at the BS and the RIS remain constant. The proposed channel probing protocol consists of two parts. The first part is to estimate the spatial angles at the BS and RIS in the first coherence time slot. With the angular sparsity, BS and UE apply the OMP algorithm to measure the angular information. The second part is to measure the rapidly-varying channel gains of the beam-domain channel in subsequent coherence time slots. Given the estimated spatial angles, the simple least square (LS) estimator is applied to measure the rapidly-varying channel gains, which greatly reduces the computational complexity and the pilot overhead.

A. Estimating the Virtual Spatial Angles

As shown in Fig. 2, the first part of the channel probing protocol consists of uplink and downlink phases. In the uplink

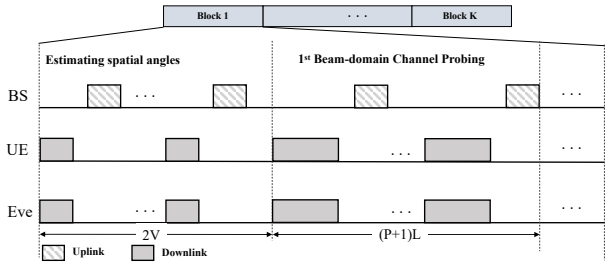

Fig. 2. Channel probing protocol.

(downlink) phase, the UE (BS) transmits several packets to BS (UE). Eve receives the packets in the downlink phase to intercept the virtual spatial angles. To estimate the sparse spatial angles, the BS controls the phase shift vector for each packet in the uplink or downlink phases.

1) Uplink Channel Estimation: When the BS configures the phase shift vector $\mathbf{v}(t)$, the UE transmits the t-th uplink packet to the BS. The received signal at the BS is $\mathbf{y}_a(t) = \mathbf{h}_c(\mathbf{v}(t))s(t) + \mathbf{n}_a(t)$, where $\mathbf{y}_a(t) \in \mathbb{C}^{N\times 1}$, $\mathbf{n}_a(t) \in \mathbb{C}^{N\times 1}$ is the complex noise, and $\mathbf{n}_a(t) \sim \mathcal{CN}(0, \sigma_a^2\mathbf{I})$. Then, the BS uses the precoding vector $\mathbf{w}^H(t)$ to transform $\mathbf{y}_a(t)$ as

$$\begin{aligned}\widehat{y}_a(t) &= \mathbf{w}^H(t)\mathbf{H}\mathbf{v}(t) + \mathbf{w}^H(t)\mathbf{n}_a(t)s^*(t)(s(t)s^*(t))^{-1} \\ &\overset{(d)}{=} (\mathbf{v}^T(t)\otimes \mathbf{w}^H(t))\mathbf{F}\mathbf{x} + \widehat{n}_a(t),\end{aligned} \tag{6}$$

where (d) holds due to $\text{vec}(\mathbf{ABC}) = (\mathbf{C}^T \otimes \mathbf{A})\text{vec}(\mathbf{B})$, $\widehat{y}_a(t) \in \mathbb{C}$, $\mathbf{F} = \mathbf{V}^* \otimes \mathbf{U}$, $\mathbf{F} \in \mathbb{C}^{MN\times MN}$, $\mathbf{x} = \text{vec}(\widetilde{\mathbf{H}})$, $\mathbf{x} \in \mathbb{C}^{MN\times 1}$, and P_b is the transmit power of UE.

To recover the virtual spatial angles, BS receives overall V packets in (6) and stacks them into a vector, i.e., $\widehat{\mathbf{y}}_a = [\widehat{y}_a(1), \ldots, \widehat{y}_a(V)]^T = \mathbf{PFx} + \boldsymbol{\eta}_a$, where $\widehat{\mathbf{y}}_a \in \mathbb{C}^{V\times 1}$. Specially, $\mathbf{P}$ is the configuration of phase shift and precoding vectors over V packets in the uplink phase, i.e., $\mathbf{P} = [\mathbf{v}^T(1)\otimes \mathbf{w}^H(1); \ldots; \mathbf{v}^T(V)\otimes \mathbf{w}^H(V)]$. $\boldsymbol{\eta}_a = [\widehat{n}_a(t); \ldots; \widehat{n}_a(t)]$ is the uplink estimation noise, where $\boldsymbol{\eta}_a \sim \mathcal{CN}(0, \sigma_a^2/P_b\mathbf{I}_V)$. We define $\boldsymbol{\Phi} = \mathbf{PF}$, $\boldsymbol{\Phi} \in \mathbb{C}^{V\times MN}$, as the uplink sensing matrix.

Since $\mathbf{x}$ is sparse, BS applies the OMP algorithm based on the sensing matrix, $\boldsymbol{\Phi}$, to measure the virtual beam-domain channel [10]. In each iteration, the BS update the residue $\mathbf{r}_k = \widehat{\mathbf{y}}_a - [\boldsymbol{\Phi}]_{:,\mathcal{I}_k}\widehat{\mathbf{x}}_{s,k}$, where $\mathcal{I}_k$ is the spatial support index set and $\widehat{\mathbf{x}}_{s,k} = ([\boldsymbol{\Phi}]_{:,\mathcal{I}_k})^H\widehat{\mathbf{y}}_a$ is the estimated channel. Until the residue is smaller than the threshold ϵ, the estimated beam-domain channel is $[\widehat{\mathbf{x}}_a]_{\mathcal{I}_k} = \widehat{\mathbf{x}}_{s,k}$. BS gets the $\widehat{\mathbf{x}}_a$ and rearranges it into the matrix, $\widehat{\mathbf{H}}_a$, which is the estimation of $\widetilde{\mathbf{H}}_a$. The row index of non-zero values in $\widehat{\mathbf{H}}_a$ denotes the estimation of the index of virtual spatial angle in $\mathbf{U}$. The corresponding column vector in $\mathbf{U}$ represents the estimated spatial angle at BS, i.e., $\widehat{\mathbf{A}}_{N,a}$. The column index of non-zero values in $\widehat{\mathbf{H}}_a$ denotes the estimation of the index of virtual spatial angle in $\mathbf{V}$. The corresponding column vector in $\mathbf{V}$ represents the estimated spatial angle at RIS, i.e., $\widehat{\mathbf{A}}_{M,a}$.

2) Downlink Channel Estimation: With phase shift vector $\mathbf{v}^H(t)$, BS utilizes $\mathbf{w}(t)$ to transmit a downlink packet to the UE, and UE receives the signal as $y_b(t) = \mathbf{h}_c^H(\mathbf{v}(t))\mathbf{w}(t)s(t) + n_b(t)$, where $y_b(t) \in \mathbb{C}$, $n_b(t) \in \mathbb{C}$ is the complex Gaussian noise, and $n_b(t) \sim \mathcal{CN}(0, \sigma_b^2)$. Based on (3) and (4), the received signal is converted to

$$\begin{aligned}\widehat{y}_b(t) &= \mathbf{v}^H(t)\mathbf{H}^H\mathbf{w}(t) + n_b(t)s^*(t)(s(t)s^*(t))^{-1} \\ &= (\mathbf{v}^H(t)\otimes \mathbf{w}^T(t))\mathbf{F}_d\mathbf{x}^* + \widehat{n}_b(t),\end{aligned} \tag{7}$$

where $\mathbf{F}_d = \mathbf{V}\otimes\mathbf{U}^*$, $\widehat{n}_b(t)$ is the estimation noise of UE, $\widehat{n}_b(t) \sim \mathcal{CN}(0, \sigma_b^2/P_a)$, and P_a is the transmit power of BS.

The UE receives V downlink packets and stacks them into a vector, i.e., $\widehat{\mathbf{y}}_b = [\widehat{y}_b(1), \ldots, \widehat{y}_b(V)]^T = \mathbf{P}_d\mathbf{F}_d\mathbf{x} + \boldsymbol{\eta}_b$, where $\widehat{\mathbf{y}}_b \in \mathbb{C}^{V\times 1}$ and $\boldsymbol{\eta}_b = [\widehat{n}_b(1), \ldots, \widehat{n}_b(V)]^T$ with $\mathbb{E}\{\boldsymbol{\eta}_b\boldsymbol{\eta}_b^H\} = \sigma_b^2\mathbf{I}_V$. $\mathbf{P}_d$ is the configuration of phase shift and precoding vectors over V packets in the downlink phase, which is given by $\mathbf{P}_d = [\mathbf{v}^H(1)\otimes\mathbf{w}^T(1); \ldots; \mathbf{v}^H(V)\otimes\mathbf{w}^T(V)]$. We define $\boldsymbol{\Phi}_d = \mathbf{P}_d\mathbf{F}_d$ as the downlink sensing matrix.

Similarly, Eve gets the measurements as $\widehat{\mathbf{y}}_e = \mathbf{P}_d\mathbf{F}_d\mathbf{x}_e + \boldsymbol{\eta}_e = \boldsymbol{\Phi}_d\mathbf{x}_e + \boldsymbol{\eta}_e$, where $\mathbf{x}_e = \text{vec}(\widetilde{\mathbf{H}}_e)$, $\mathbf{y}_e \in \mathbb{C}^{V\times 1}$ and $\mathbb{E}\{\boldsymbol{\eta}_e\boldsymbol{\eta}_e^H\} = \sigma_e^2\mathbf{I}_V$. Based on their measurements and sensing matrix, UE and Eve apply the OMP algorithm to measure the angular information, i.e., $\widehat{\mathbf{A}}_{N,b}$, $\widehat{\mathbf{A}}_{M,b}$, $\widehat{\mathbf{A}}_{N,e}$, and $\widehat{\mathbf{A}}_{N,e}$.

B. Channel Probing for Beam-domain Channels

Given the estimated angular information, the BS and UE only need to measure the channel gains of the beam-domain channel in the remaining coherence slots. They apply the LS estimator that has $(Kg+1)L_gK_f$ pilots overhead.

1) Uplink Channel Probing: The BS applies the precoding matrix $\mathbf{P}^H$, $\mathbf{P} \in \mathbb{C}^{N\times P}$, to the t-th received packet and gets

$$\widehat{\mathbf{z}}_a(t) = \mathbf{P}^H\mathbf{H}\mathbf{v}(t) + \mathbf{P}^H\mathbf{n}_a(t)s^*(t)(s(t)s^*(t))^{-1}, \tag{8}$$

where $\widehat{\mathbf{z}}_a(t) \in \mathbb{C}^{P\times 1}$, $\widehat{\mathbf{n}}_a(t) = 1/\sqrt{P_b}\mathbf{P}^H\mathbf{n}_a(t)$ is the estimation noise, and $\mathbb{E}\{\widehat{\mathbf{n}}_a(t)\widehat{\mathbf{n}}_a^H(t)\} = \sigma_b^2/P_b\mathbf{I}$.

We define $\mathbf{W} = [\mathbf{v}(1), \ldots, \mathbf{v}(L)] \in \mathbb{C}^{M\times L}$ as the phase shift matrix to model the configuration of the phase shift vector over L packets. The BS receives L packets in (8) and stacks them into a vector, which is given by $\mathbf{Z}_a = [\widehat{\mathbf{z}}_a(1), \ldots, \widehat{\mathbf{z}}_a(L)] = \mathbf{P}^H\mathbf{A}_N\boldsymbol{\Lambda}^H\mathbf{A}_M^H\mathbf{W} + \mathbf{N}_a$, where $\mathbf{Z}_a \in \mathbb{C}^{P\times L}$ and $\mathbf{N}_a = [\widehat{\mathbf{n}}_a(1), \ldots, \widehat{\mathbf{n}}_a(L)]^T$. Based on the estimated spatial angles, BS uses the LS estimation method to measure the $\boldsymbol{\Lambda}$, which is given by

$$\begin{aligned}\widehat{\boldsymbol{\Lambda}}_a^H &= (\widehat{\mathbf{A}}_{N,a}^H\mathbf{P}\mathbf{P}^H\widehat{\mathbf{A}}_{N,a})^{-1}\widehat{\mathbf{A}}_{N,a}^H\mathbf{P}\mathbf{Z}_a \\ &\times \mathbf{W}^H\widehat{\mathbf{A}}_{M,a}(\widehat{\mathbf{A}}_{M,a}^H\mathbf{W}\mathbf{W}^H\widehat{\mathbf{A}}_{M,a})^{-1} \approx \boldsymbol{\Lambda}^H + \widehat{\mathbf{N}}_a,\end{aligned} \tag{9}$$

where $\widehat{\mathbf{N}}_a$ has the noise power $\widehat{\sigma}_a^2$, $\mathbf{P}^H\widehat{\mathbf{A}}_{N,a} \in \mathbb{C}^{P\times K_g}$ and $\widehat{\mathbf{A}}_{M,a}^H\mathbf{W} \in \mathbb{C}^{L_gK_f\times L}$. Notably, $P \geq K_g$ and $L \geq L_gK_f$ should be satisfied to make $\mathbf{P}^H\widehat{\mathbf{A}}_{N,a} \in \mathbb{C}^{P\times K_g}$ have full row rank and $\widehat{\mathbf{A}}_{M,a}^H\mathbf{W} \in \mathbb{C}^{L_gK_f\times L}$ have full column rank.

2) Downlink Channel Probing: The BS uses $\mathbf{P}$ to transmit the t-th downlink packet, $\mathbf{P}\mathbf{S}_d^H$, to the UE. We assume equal power allocation, i.e., $\mathbf{S}_d^H\mathbf{S}_d = P_a\mathbf{I}_P$. The RIS controls $\mathbf{v}(t)$ to reflect it and then the UE receives the signal as $\mathbf{y}_b(t) = \mathbf{v}^H(t)\mathbf{H}^H\mathbf{P}\mathbf{S}_d^H + \mathbf{n}_b(t)$, where $\mathbf{y}_b(t) \in \mathbb{C}^{1\times P}$ and $\mathbf{n}_b(t) \in \mathbb{C}^{1\times P}$ is the noise vector. By the LS estimation, the UE measures the cascaded channel as $\widehat{\mathbf{z}}_b(t) = \mathbf{y}_b(t)\mathbf{S}_d(\mathbf{S}_d^H\mathbf{S}_d)^{-1} = \mathbf{v}^H(t)\mathbf{H}^H\mathbf{P} + \widehat{\mathbf{n}}_b(t)$, where $\widehat{\mathbf{z}}_b(t) \in \mathbb{C}^{1\times P}$.

The UE collects L measurements stacks them as $\mathbf{Z}_b = [\widehat{\mathbf{z}}_b(1);\ldots;\widehat{\mathbf{z}}_b(L)] = \mathbf{W}^H\mathbf{A}_M\mathbf{\Lambda}\mathbf{A}_N^H\mathbf{P} + \mathbf{N}_b$, where $\mathbf{Z}_b \in \mathbb{C}^{L\times P}$ and $\mathbf{N}_b = [\widehat{\mathbf{n}}_b(1);\ldots;\widehat{\mathbf{n}}_b(L)]$. Based on the angular information, UE uses the LS estimation method to measure the $\mathbf{\Lambda}$, which is given by

$$\widehat{\mathbf{\Lambda}}_b = (\widehat{\mathbf{A}}_{M,b}^H\mathbf{W}\mathbf{W}^H\widehat{\mathbf{A}}_{M,b})^{-1}\widehat{\mathbf{A}}_{M,b}^H\mathbf{W}\mathbf{Z}_b \\ \mathbf{P}^H\widehat{\mathbf{A}}_{N,b}(\widehat{\mathbf{A}}_{N,b}^H\mathbf{P}\mathbf{P}^H\widehat{\mathbf{A}}_{N,b})^{-1} \approx \mathbf{\Lambda} + \widehat{\mathbf{N}}_b, \quad (10)$$

where the estimation noise power is $\widehat{\sigma}_b^2$. Similarly, Eve gets the estimated beam-domain channel as $\widehat{\mathbf{\Lambda}}_e \approx \mathbf{\Lambda}_e + \widehat{\mathbf{N}}_e$.

IV. Secret Key Rate Analysis

The UE and Eve share the same BS-RIS channel, while they share different UE-RIS channels. Since the physical locations of BS and RIS are static, the BS-RIS channel is quasi-static. To extract secret keys from varying UE-RIS channels, the BS and UE choose the maximal value among each column of $\widehat{\mathbf{\Lambda}}_a$ and $\widehat{\mathbf{\Lambda}}_b$ as $\mathbf{z}_a$ and $\mathbf{z}_b$, respectively. Eve acquires the eavesdropping measurement $\mathbf{z}_e$. We first analyze the channel covariance matrix of $\mathbf{f}$, which is computed as $\mathbf{R} = \frac{\beta_f}{L_f\sigma_f}\mathbb{E}\left\{\mathbf{f}\mathbf{f}^H\right\} = \mathbb{E}\left\{\mathbf{a}(\theta_f,\varphi_f)\mathbf{a}^H(\theta_f,\varphi_f)\right\}$. The virtual beam-domain channel is defined as $\widetilde{\mathbf{f}} = \mathbf{V}^H\mathbf{f}$, $\widetilde{\mathbf{f}} \in \mathbb{C}^{M\times 1}$.

The normalized channel covariance matrix of $\widetilde{\mathbf{f}}$ is given by

$$\lim_{M_z,M_y\to\infty}[\widetilde{\mathbf{R}}]_{p,q} = [\mathbb{E}\left\{\mathbf{V}^H\mathbf{a}(\theta_f,\varphi_f)\mathbf{a}(\theta_f,\varphi_f)^H\mathbf{V}\right\}]_{p,q} \\ = \int_{\theta_f^{\min}}^{\theta_f^{\max}}\int_{\varphi_f^{\min}}^{\varphi_f^{\max}}\delta(\frac{d}{\lambda}\sin\varphi_f - x)\delta(q_z - p_z) \\ \times\delta(\frac{d}{\lambda}\cos\varphi_f\sin\theta_f - y)\delta(q_y - p_y)f(\varphi_f,\theta_f)d\varphi_f d\theta_f, \quad (11)$$

where $x = \frac{p_z-(M_z+1)/2}{M_z}$, $y = \frac{p_y-(M_y+1)/2}{M_y}$, $p = (M_y-1)p_z + p_y$ and $q = (M_y-1)q_z + q_y$, and $f(\varphi_f,\theta_f)$ is the probability density function. (11) indicates that $\widetilde{\mathbf{R}}$ approaches a diagonal matrix when M_z and M_y are large enough. The diagonal matrix contains a small portion of non-zero entries and a large portion of zero entries. The non-zero entries represent clusters whose elevation angle ranges from $\varphi_f^{\min}$ to $\varphi_f^{\max}$ and azimuth angle ranges from $\theta_f^{\min}$ to $\theta_f^{\max}$, i.e., $\theta_f \in [\theta_f^{\min},\theta_f^{\max}]$ and $\varphi_f \in [\varphi_f^{\min},\varphi_f^{\max}]$. We define $\mathcal{A}$ as the non-zero diagonal indices in the $\widetilde{\mathbf{R}}$, which is computed as $\mathcal{A} = \{p|p = (M_y-1)p_z + p_y, p\in\mathbb{Z}, \lfloor M_z\frac{d}{\lambda}\sin\varphi_f^{\min}\rfloor + \frac{M_z+1}{2} \le p_z \le \lfloor M_z\frac{d}{\lambda}\sin\varphi_f^{\max}\rfloor + \frac{M_z+1}{2}, \lfloor M_y\frac{d}{\lambda}\cos\varphi_{f,i}\sin\theta_f^{\min}\rfloor + \frac{M_y+1}{2} \le p_y \le \lfloor M_y\frac{d}{\lambda}\cos\varphi_f\sin\theta_f^{\max}\rfloor + \frac{M_y+1}{2}\}$.

A. Non-overlapping Case

The beams of Eve and UE are not overlapping. The SKR is the mutual information of the measurements of the beam-domain channel, which is calculated as

$$C_k = I(\mathbf{z}_a;\mathbf{z}_b) = \sum\nolimits_{l=1}^{K_f} I(\widehat{z}_{a,l};\widehat{z}_{b,l}) \\ = \sum\nolimits_{l=1}^{K_f}\log_2\left(1 + \frac{1}{\eta_{a,l}+\eta_{b,l}+\eta_{a,l}\eta_{b,l}}\right), \quad (12)$$

where $\eta_{a,l} = \widehat{\sigma}_a^2/(g_m\sigma_f^2)$ and $\eta_{b,l} = \widehat{\sigma}_b^2/(g_m\sigma_f^2)$ are the mean square error (MSE) of the l-th beam of BS and UE, respectively, and g_m is the maximal value of $g_{l_g,k}$.

B. Overlapping case

In this case, parts of the beams of Eve and UE are overlapping. The correlation between $z_{e,l}$ and $z_{b,l}$ is given by $\rho = \frac{\mathbb{E}\{z_{e,l}z_{b,l}^*\}}{\sqrt{\mathbb{E}\{z_{e,l}z_{e,l}^*\}\mathbb{E}\{z_{b,l}z_{b,l}^*\}}}$. We calculate the SKR as

$$C_{k,o} = I(\mathbf{z}_a;\mathbf{z}_b) - I(\mathbf{z}_e;\mathbf{z}_b) = C_k - \sum\nolimits_{l,l\in\mathcal{L}} I(\widehat{z}_{e,l};\widehat{z}_{b,l}) \\ = C_k - \sum_{l,l\in\mathcal{L}}\log_2\left(1 + \frac{\rho^2}{1-\rho^2+\eta_{b,l}+\eta_{e,l}+\eta_{b,l}\eta_{e,l}}\right), \quad (13)$$

where $\eta_{b,l}$ is the MSE of the l-th beam of Eve, $\mathcal{L}$ is the set of the overlapped beams and l_{leak} is the number of overlapping beams.

V. Simulation Results

In all the figures, solid lines and markers denote numerical results and simulation results, respectively.

A. Parameter Settings

1) Device Configuration: The antenna spacing normalized by wavelength is $d_a = 0.5$. The side length of an element normalized by the wavelength is $d_r = \frac{d_r}{\lambda}$. The transmit powers of the BS and UE are set identically as $P_t = P_a = P_b$ dBm. All noise powers are set as $\sigma^2 = \sigma_a^2 = \sigma_b^2 = -96$ dBm.

2) Channel Configuration: The path-loss effect is modeled as $\beta_{uv} = \beta_0(\frac{d_{uv}}{d_0})^{-\epsilon_{uv}}$, $u,v\in\{a,b,r\}$, where ϵ_{uv} is the path-loss exponent, $\beta_0 = -30$ dB denotes the path-loss effect at $d_0 = 1$ m and d_{uv} is the link distance. The path-loss exponents of the BS-RIS and UE-RIS links are set as $\epsilon_{ar} = 2$ and $\epsilon_{br} = 2$, respectively. $l_g = 2$, $K_{l_g} = 3$, $l_f = 2$, and $K_{l_f} = 2$.

The following benchmark schemes are considered:

1) Random configuration: Both the precoding and phase-shift vectors are randomly configured [3], [4]. LS method is employed to estimate the cascaded channel.
2) Optimal configuration: Both the precoding and phase-shift vectors are optimized [5]. LS method is employed to estimate the cascaded channel.
3) DFT-pattern configuration: The precoding and phase-shift vectors are configured in the DFT pattern. The LS estimator is employed to estimate subchannels.

B. Performance Analysis

Fig. 3 exhibits the SKR that BS and UE can extract in each channel probing with different transmit powers. The increase in the transmit power has a big influence on the SKR since the high power improves the similarity of their measurements. The average gap between the SKR of the proposed scheme and the optimal configuration is great because the beam-domain channel provides more channel dimension for key generation. Compared to the DFT-pattern configuration, the proposed scheme also has a small decrease, since the DFT-pattern configuration consumes more pilot overhead to estimate the subchannels of the cascaded channel. However, there exists serious auto-correlation between the measurements from the DFT-pattern configuration while the measurements from the proposed scheme are nearly uncorrelated, as shown in Fig. 4.

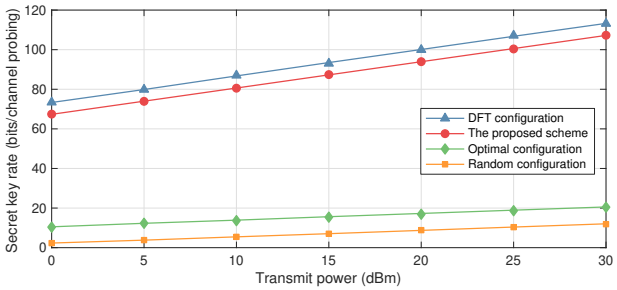

Fig. 3. SKR versus transmit power. $N = 49$, $M = 121$.

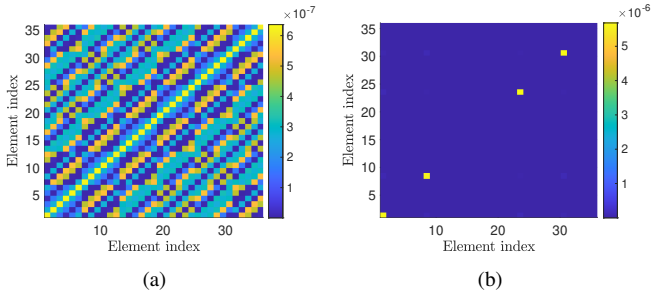

Fig. 4. (a) Correlation of channels in the antenna domain. (b) Correlation of channels in the beam domain. $N = 46$, $M = 36$, $P_t = 10$ dBm.

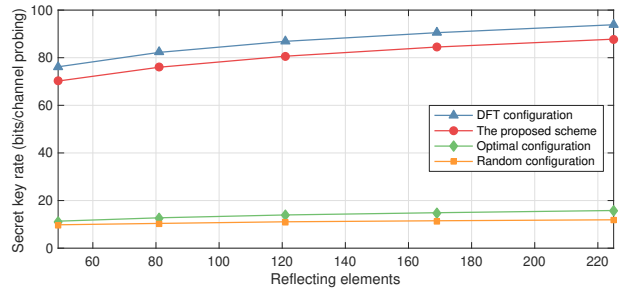

Fig. 5. SKR versus reflecting elements. $N = 49$, $P_t = 10$ dBm.

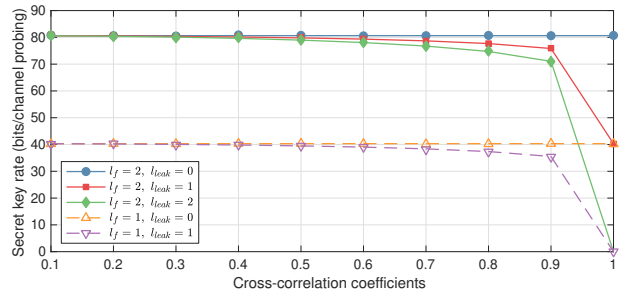

Fig. 6. SKR versus cross-correlation. $N = 49$, $M = 121$, $P_t = 10$ dBm.

Fig. 5 illustrates the SKR per channel probing for a different number of reflecting elements. It is apparent that the SKR improves with the number of reflecting elements since the increase of reflecting elements improve the SNR at the receivers. The SKR of the optimal and random configurations do not increase greatly, because the channel dimension is limited.

Fig. 6 shows the impact of the cross-correlation on the SKR. As the ρ gets larger from 0.1 to 1, the SKR decreases since Eve eavesdrops on more secret keys. Especially, the blue and orange curves show the SKR extracts from environments with two and one non-overlapping beams, respectively, which exhibit the upper bounds. The red and green curves show the SKR extracts from environments with one and two overlapping beams, which means the increase of the overlapping beams reduces the SKR. Also, there is a large performance gain in the two-beams case marked with solid lines compared with the one-beam case marked with dashed lines.

VI. Conclusion

In this paper, the PLKG in RIS-assisted mmWave communication systems was investigated. We proposed a channel probing method based on the OMP algorithm to estimate spatial angles in the first coherence slot and the LS algorithm to estimate the channel gains in the following slots. We analyzed the channel covariance matrix of the beam domain channel and found the channel gains are uncorrelated. We further investigated the problem of information leakage imposed by an eavesdropper. The SKR was derived, which was determined by overlapping and non-overlapping beams. Numerical results validated that the proposed method outperforms existing algorithms in key generation.

Acknowledgment

This research is supported by National key research and development program of China, 2020YFE0200600. The work of J. Zhang and C. Chen was also supported by the UK EPSRC under grant ID EP/V027697/1.

References

[1] M. Ylianttila, R. Kantola, A. Gurtov *et al.*, "6G white paper: Research challenges for trust, security and privacy," 2021. [Online]. Available: https://arxiv.org/pdf/2004.11665.pdf

[2] J. Zhang, G. Li, A. Marshall *et al.*, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138 406–138 446, Aug. 2020.

[3] Z. Ji, P. L. Yeoh, G. Chen *et al.*, "Random shifting intelligent reflecting surface for OTP encrypted data transmission," *IEEE Wireless Commun. Lett.*, vol. 10, no. 1192–1196, pp. 1–5, Jun. 2020.

[4] T. Lu, L. Chen, J. Zhang *et al.*, "Reconfigurable intelligent surface assisted secret key generation in quasi-static environments," *IEEE Commun. Lett.*, vol. 26, no. 2, pp. 244–248, Feb. 2022.

[5] Z. Ji, P. L. Yeoh, D. Zhang *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.

[6] G. Li, C. Sun, W. Xu *et al.*, "On maximizing the sum secret key rate for reconfigurable intelligent surface-assisted multiuser systems," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 211–225, Jan. 2022.

[7] E. Björnson, H. Wymeersch, B. Matthiesen *et al.*, "Reconfigurable intelligent surfaces: A signal processing perspective with wireless applications," *IEEE Signal Processing Mag.*, vol. 39, no. 2, pp. 135–158, Mar. 2022.

[8] L. Jiao, N. Wang, P. Wang *et al.*, "Physical layer key generation in 5G wireless networks," *IEEE Wirel. Commun.*, vol. 26, no. 5, pp. 48–54, Oct. 2019.

[9] T. Lu, L. Chen, J. Zhang *et al.*, "Joint precoding and phase shift design in reconfigurable intelligent surfaces-assisted secret key generation," 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2208.00218

[10] G. Zhou, C. Pan, and H. Ren, "Channel estimation for RIS-aided multiuser millimeter-wave systems," *IEEE Trans. Signal Process.*, vol. 70, pp. 1478–1492, Mar. 2022.