Reconfigurable Intelligent Surface-Assisted Key Generation for Millimetre-Wave Multi-User Systems

Tianyu Lu, *Graduate Student Member, IEEE,* Liquan Chen, *Senior Member, IEEE,*
Junqing Zhang, *Member, IEEE,* Chen Chen, *Member, IEEE* and Trung Q. Duong, *Fellow, IEEE*

***Abstract*—Physical layer key generation (PLKG) leverages wireless channels to produce secret keys for legitimate users. However, in millimetre-wave (mmWave) frequency bands, the presence of blockage significantly reduces the key rate (KR) of a PLKG system. To address this issue, we introduce reconfigurable intelligent surfaces (RISs) as a potential solution for constructing RIS-reflected channels, thereby enhancing the KR. Our study focuses on the beam-domain channel model and exploits the sparsity of mmWave bands to enhance the randomness of secret keys. To relieve pilot overhead in multi-user systems, we employ a compressed sensing (CS) algorithm to estimate angular information and propose a channel probing protocol with the full-array configuration for acquiring the beam-domain channel. We derive the analytical expressions for the KR in the case of full-array configuration. To optimize the KR, we design the phase shift and precoding vectors based on the obtained angular information. Furthermore, we employ a water-filling algorithm that relies on the Karush-Kuhn-Tucker (KKT) conditions to optimize power allocation for estimating the beam-domain channel with the same channel variance. When channel variances of the beam-domain channel differ, we design a deep-learning-based power allocation method for a more complex problem. What is more, we design a sub-array configuration scheme that exploits the difference in spatial angles between users to reduce pilot overhead and derive the analytical expression for the KR. Through extensive simulations, we demonstrate that our proposed PLKG schemes outperform existing methods.**

***Index Terms*—Reconfigurable intelligent surface, key generation, millimetre-wave communications and compressed sensing.**

I. Introduction

Part of this paper has been accepted by IEEE WCNC Workshop 2023. This research is supported by the National Natural Science Foundation of China (No. U22B2026) and the National Key Research and Development Program of China (No. 2020YFE0200600). The work of J. Zhang and C. Chen was also supported by the UK EPSRC under grant ID EP/V027697/1. The work of T. Q. Duong was supported in part by the Canada Excellence Research Chair (CERC) Program CERC-2022-00109. (*Corresponding author: L. Chen*)

T. Lu and L. Chen are with the School of Cyber Science and Engineering, Southeast University, Nanjing, 210096, China (e-mail: effronlu@seu.edu.cn; lqchen@seu.edu.cn). L. Chen is also with the Purple Mountain Laboratories for Network and Communication Security, Nanjing, 211111, China.

J. Zhang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, U. K. (e-mail: junqing.zhang@liverpool.ac.uk)

C. Chen is with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, Sweden (e-mail: chch2@kth.se).

T. Q. Duong is with the Faculty of Engineering and Applied Science, Memorial University, St. John's, NL A1C 5S7, Canada, and is also with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast, U.K. (e-mail: tduong@mun.ca).

THE millimetre-wave (mmWave) communications utilize the bandwidth from 30 GHz to 300 GHz to increase communication capacity [1], which provides large bandwidth available for 5G and beyond. However, due to the open nature of the wireless channels, the mmWave signals received by legitimate users will be intercepted by eavesdroppers. The ongoing task of addressing vulnerabilities in mmWave technology remains crucial to ensuring the security of 5G and beyond [2]. Physical layer security (PLS) can be classified into keyless secure transmission and key generation [3]. In mmWave environments, keyless secure transmission [3], a branch of PLS, is investigated to protect the confidential message transmitted between legitimate users. For example, Ragheb *et al.* [4] designed the signal and artificial noise powers, the beamforming design at the base station (BS), and the phase shifts at the reconfigurable intelligent surface (RIS) to optimize the secrecy rate.

However, keyless secure transmission usually requires the signal-to-interference-plus-noise ratio (SINR) at the user to be better than that at the Eve so that the secrecy rate is non-negative. Also, the channel state information (CSI) of Eve is required to design the optimization algorithm of preceding vectors at the BS or the phase shifts at the RIS. In contrast, physical layer key generation (PLKG) exploits the properties of channel randomness, reciprocity, and spatial decorrelation to achieve information-theoretical security. PLKG is a potential technique to establish symmetric keys between legitimate users [3].

However, PLKG suffers from poor channel conditions such as static channels, obstacle blockages, long distances, and sparsity. Firstly, when the variation of wireless channels is slow, PLKG cannot produce keys efficiently, such as in static environments. Secondly, the key rate (KR), denoting the number of secret keys per channel use, declines with the decrease in the signal-to-noise ratio (SNR) when the channel is blocked by obstacles or the distance between users gets far. Finally, the self-correlation between measurements obtained from antennas in a multiple-input-multiple-output (MIMO) system can have a significant impact on the randomness of secret keys.

Recently, the RIS has emerged as a prospective approach to address the aforementioned challenges [5]–[8]. A RIS consisting of many discrete elements can configure its reflection coefficients to control the channel [9]. In single-antenna systems, the RIS can randomly tune reflection coefficients and change the wireless channel with time to mimic the fast-fading effects. Ji *et al.* [5] utilized the random phase shift vector to improve the KR in quasi-static environments. Lu *et al.* derived

the analytical expressions of the lower and upper bounds of the KR with the random configuration of RIS. Low-SNR problem is solved by optimizing the phase shift vector to improve the channel quality of legitimate users in [7]. Hu *et al.* [8] extended the design of phase shift vectors in key generation systems in multi-antenna scenarios.

However, the above works focus on sub-6GHz systems. In mmWave systems, electromagnetic waves experience significant path loss and limited scattering, leading to a high rate of signal blockage [1]. When the direct channel is blocked, an RIS can construct a reflected channel to solve the blockage-prone problem in key generation. The previous works [10] and [8] have proposed to design the phase shift vector at the RIS and the precoding vector at the BS to increase the KR. However, these works are based on a channel covariance matrix (CCM) that is derived from the full-scattering environments. In mmWave systems, the scatterers are limited and the received signals at transceivers experience paths with different angles of arrival (AoAs) and angles of departure (AoDs). There is an urgent need to design phase shift and precoding vectors based on angular information, in addition to CCMs.

Despite the challenges, the mmWave frequency band presents potential benefits for PLKG. Since the multi-paths from different clusters exhibit independent scattering phenomena [11], the secret keys extracted from the beam-domain channel are random. Furthermore, the sparsity property of the mmWave channel sheds some insights on reducing pilot overhead in key generation. Firstly, the previous works [7], [8], [10] focused on sub-6GHz and required the prior information of CCM to jointly design precoding and phase shift vectors, resulting in an increased pilot overhead to estimate the CCM. In the antenna domain, the pilot overhead to estimate the CCM of the cascaded channels in RIS-assisted systems increases with the increasing number of antennas at transceivers and reflecting elements at RIS. By exploring the sparsity of beam-domain channels in RIS-aided systems, Zhou *et al.* [12] and Wei *et al.* [13] proposed compressed sensing (CS)-based channel estimation method with low overhead. Secondly, the pilot overhead of the orthogonal pilots is linear to the number of users in multi-user systems. Li *et al.* [14] utilized the orthogonal property of spatial angles between users. They designed precoding vectors to align with these orthogonal spatial angles, enabling multiple users to share the same pilot, which effectively reduces pilot overhead. Since the reflecting elements of RIS are massive, the orthogonal property also can be used to relieve the pilot overhead in multi-user systems.

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

- We study a PLKG framework for RIS-assisted mmWave systems, where full-array configuration is configured to allow all reflecting elements to serve a UE. Compared to channel coefficients in the antenna domain, the beam-domain channel is sparse and uncorrelated, which greatly reduces the pilot overhead and redundancy between measurements. We first use the orthogonal matching pursuit (OMP) algorithm to estimate the angular information that changes slowly. Based on the angular information, we propose a channel probing protocol with the least square (LS) estimator to acquire the beam-domain channel.
- We derive the analytical expressions of the KR extracted from the beam-domain channel in the full-array configuration. Based on the estimated angular information, we design the phase shift vector at RIS and the precoding vector at the BS. Furthermore, we find the optimal power allocation using the water-filling algorithm based on the Karush-Kuhn-Tucker (KKT) conditions when channel variances of beams are equal.
- When the channel variances of beams are different, the water-filling algorithm is not applicable to finding the optimal power allocation. We further design an unsupervised deep neural network (DNN), named as KGPA-Net, to output the optimal power allocation based on the channel variances of beams and the power information.
- To further reduce the pilot overhead, we propose to apply a sub-array configuration in which a sub-array serves a user. Since the spatial angles from users to the RIS are different, the users share the same pilot in the downlink channel probing, which reduce the pilot overhead.
- We performed Monte Carlo simulations to validate the analytical expressions of KR for both full-array and sub-array configurations. During these simulations, we evaluated the KR against varying transmit power levels and explored the influence of the number of reflecting elements and antennas on the KR performance. Our results demonstrate that the proposed scheme outperforms existing methods across these different parameters.

Our previous work [15] considered exploiting randomness from the beam-domain channel in a single-user mmWave system. In this paper, we considerably extend the work to a more general scenario with multiple users. The phase shift and precoding vectors are designed to maximize the KR when the channel variances of beams are equal. Furthermore, a deep-learning network is proposed to optimize the KR when the channel variances of beams are different. To further relieve the pilot overhead, we design a sub-array configuration to reduce the pilot length in downlink channel probing.

Our previous work in [16] proposed to extract secret keys from massive subchannels associated with each reflecting element in sub-6GHz. We jointly designed the precoding and phase shift vectors to improve KR. While the BS should acquire the prior information of CCM in sub-6GHz, the sparsity property makes the KR be optimized based on the angular information in the mmWave band, which makes the design of precoding and phase shift vectors completely different.

The rest of this paper is organized as follows. Section II illustrates the system model. Section III describes the channel model of the full-array configuration. In Section IV, we propose a channel probing protocol for a multi-user mmWave system, and the expression of KR is derived. Section V formulates an optimization problem. Then we propose a water-filling algorithm-based power allocation method. Furthermore, A deep-learning-based method is extended to solve the general case. In Section VI, we proposed a sub-array configuration to relieve the pilot overhead. Section VII discusses the key generation protocol. Section VIII shows the security analysis.

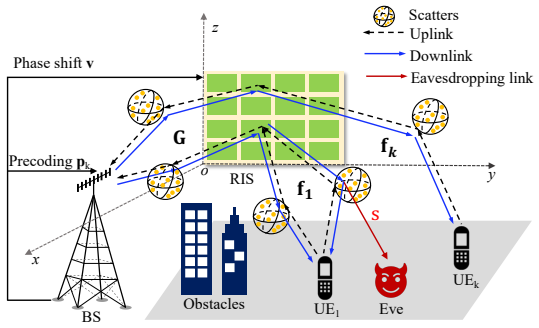

Fig. 1. System model.

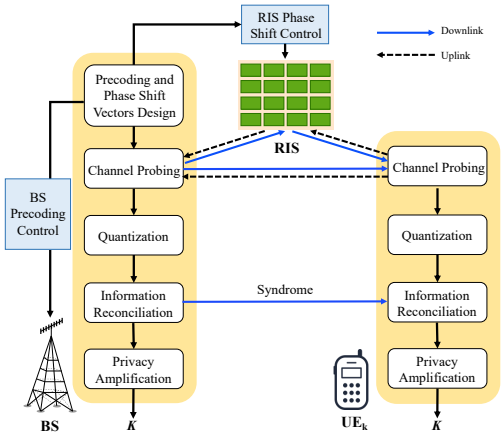

Fig. 2. Key generation protocol.

The simulation results are presented in Section IX. Section X provides the discussion. Section XI concludes this paper.

Notations: Italic letters, boldface lower-case letters, boldface upper-case letters, and calligraphic letters denote scalars, vectors, matrices, and sets, respectively. $\text{diag}(\cdot)$ forms a diagonal matrix out of its vector argument. $\text{vec}(\cdot)$ 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. $[\mathbf{A}]_{m,n}$ denotes the (m,n)-th element of matrix $\mathbf{A}$. $[\mathbf{a}]_m$ denotes the m-th element of vector $\mathbf{a}$. $\mathcal{CN}(\mu, \sigma^2)$ 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. $I(.;.)$ denotes the mutual information. $\diamond$ is the transposed Khatri-Rao product. $\text{mod}\ (\cdot)$ 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-assisted mmWave system that consists of a BS, K pieces of user equipment (UE), and a RIS. The direct channels between BS and UEs are blocked by obstacles, and the RIS constructs reflected channels to assist the key generation process. There are several scatters around the BS and RIS, causing the RIS-reflected channels to pass different paths of clusters.

The PLKG protocol is a four-stage process, including channel probing, quantization, information reconciliation, and privacy amplification, as shown in Fig. 2. Channel probing is conducted in the time division duplex (TDD) mode by UEs and BS; BS and K UEs send pilots to each other to measure the RIS-reflected channels. In the quantization stage, the analogue channel measurements are mapped into a set of binary values. Information reconciliation eliminates discrepancies in binary sequences. Subsequently, privacy amplification algorithms are used to mitigate potential information leakage in the previous stages. BS and the k-th UE agree on the same $\mathbf{K}$ at the end of the key generation, where the $\mathbf{K}$ is unique from other UEs. This paper focuses on channel probing and optimizes phase shift and precoding vectors.

Eavesdropper attempts to intercept the secret key $\mathbf{K}$ by utilizing its own channel measurements. As a fundamental assumption in PLKG, we consider that Eve is located at least half the wavelength away from the UEs and the BS, ensuring that it remains outside the protected area. The pilots received by UEs and BS and the pilots received by the eavesdropper undergo independent channel fading [14]. Due to the extremely small half-wavelength of mmWave, which is 0.5 mm, and the significantly larger size of devices, it is infeasible for Eve to be positioned within the protected area [1], [11], [17]. The proximity of the half wavelength makes it highly likely that Eve would be detected within a distance shorter than the aforementioned threshold.

B. Device Configuration

We consider a Cartesian coordinate system, where a BS is located parallel to the x-axis, as shown in Fig. 1. The BS is modeled as a uniform linear array with N antennas, uniformly spaced with a distance of d_a m. When a wave impinges on the BS from an azimuth angle, ψ, the array response vector (ARV) 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 an angle precoding vector, $\mathbf{w} \in \mathbb{C}^{N\times 1}$, to estimate spatial angles, or a probing precoding vector, $\mathbf{p}_k \in \mathbb{C}^{N\times 1}$, for conducting channel probing with the k-th UE.

A RIS is deployed parallel to the $y-z$ plane. The RIS is modeled as a uniform planar array that has $M = M_y \times M_z$ reflecting elements with M_y reflecting elements per row and M_z elements per column. When a wave reaches the RIS from the azimuth angle, θ, and the elevation angle, φ, the ARV 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.

Each reflecting element of the RIS can control the wave impinging on it. We denote the reflection coefficients of M reflecting elements as $\mathbf{v} = [\phi_1, \ldots, \phi_M]^T$, where ϕ_m is the reflection coefficient of the m-th element. Specifically, $\phi_m = e^{j\omega_m}$, where ω_m is its phase shift which is generated from uniform quantization of $[0, 2\pi)$.

To serve multiple UEs, the RIS is deployed as full-array (FA) or sub-array (SA) configurations. In the FA configuration, all elements of a RIS, $\mathbf{v}$, configure reflection coefficients to a dedicated UE, which will be elaborated in Sections III, IV

and V. Detailed in Section VI, in the SA configuration, a sub-array consisting of a group of M/K elements from $\mathbf{v}$ configures reflection coefficients to a dedicated UE; K sub-arrays simultaneously serve K UEs.

III. FA-Based Channel Model

A. Individual Channel

In full-scattering sub-6GHz environments, the CCM-based model is applied, where channels are the multiplication of two CCMs and a complex gain matrix [9], [18]. The BS-RIS channel experiences the paths from different spatial angles is $\mathbf{G} = \mathbf{R}_r^{H/2}\mathbf{G}_w\mathbf{R}_a^{H/2}$, where the entries of $\mathbf{G}_w$ follow independent and identically distributed (i.i.d.) $\mathcal{CN}(0,1)$, and $\mathbf{R}_r$ and $\mathbf{R}_a$ are the CCMs at RIS and BS, respectively. In mmWave channels, the scattering paths are not enough to model the wireless channel as the CCM-based model. Instead, the geometric channel model is widely used for mmWave channels [12], [13]. There are individual channels, including the BS-RIS channel and the channel from RIS to the k-th UE channels. The complex gains for all channels are assumed to follow complex Gaussian distribution [19].

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

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

where $\mathbf{G} \in \mathbb{C}^{M\times N}$, β_g is the path-loss effect, $J_g = \sum_{l_g=1}^{L_g} J_{l_g}$ is the number of paths for L_g clusters, the l_g-th cluster has J_{l_g} paths, $g_{l_g,j}$ denotes the corresponding complex gain associated with the j-th path of the l_g-th cluster, $\psi_{l_g,j}^g$ denotes the AoD, and $\theta_{l_g}^g$ and $\varphi_{l_g}^g$ denote the azimuth and elevation AoA, respectively. The complex gain, $g_{l_g,j} \sim \mathcal{CN}(0,\sigma_g^2)$, is identically and independently distributed (i.i.d.).

The channel from the k-th UE to RIS is modeled as

$$\mathbf{f}_k = \sqrt{\frac{M}{\beta_{f,k} J_{f,k}}} \sum_{l_f=1}^{L_{f,k}} \sum_{j=1}^{J_{l_f,k}} f_{l_f,j,k}\mathbf{a}(\theta_{l_f,j,k}^f, \varphi_{l_f,j,k}^f), \quad (2)$$

where $\mathbf{f}_k \in \mathbb{C}^{M\times 1}$, $\beta_{f,k}$ is the path-loss effect, $J_{f,k} = \sum_{l_f=1}^{L_{f,k}} J_{l_f,k}$ is the number of paths for $L_{f,k}$ clusters, the l_f-th cluster has $J_{f,k}$ paths, $f_{l_f,j,k}$ denotes the complex gain associated with the j-th path of the l_f-th cluster, and $\theta_{l_f,j,k}^f$ and $\varphi_{l_f,j,k}^f$ denote the azimuth and elevation AoA, respectively. The $J_{f,k}$ paths are sorted based on the (l_f, j)-th path for $j = 1,\ldots,J_{l_f,k}$ and $l_f = 1,\ldots,L_{f,k}$. The complex gain of the l-th path, $f_{l_f,j,k} \sim \mathcal{CN}(0,\sigma_{f,k,l}^2)$, is i.i.d.

B. Cascaded Channel

We define the cascaded channel controlled by RIS as

$$\mathbf{h}_k(\mathbf{v}) = \mathbf{G}^H \text{diag}(\mathbf{v})\mathbf{f}_k = \mathbf{G}^H \text{diag}(\mathbf{f}_k)\mathbf{v} = \mathbf{H}_k\mathbf{v}, \quad (3)$$

where $\mathbf{h}_k(\mathbf{v}) \in \mathbb{C}^{N\times 1}$, and $\mathbf{H}_k = [\mathbf{h}_{k,1}\ldots,\mathbf{h}_{k,M}] \in \mathbb{C}^{N\times M}$ is the channel associated with M reflecting elements. The BS and the k-th UE can directly measure the cascaded channel and convert their measurements to secret keys, which is commonly adopted by previous works [7], [8]. However, the cascaded channel is coarse-grained. The dimension of the cascaded channel in the antenna domain is N, which fundamentally limits the SKR. Our previous work in [16] proposed to extract secret keys from massive subchannels associated with each reflecting element, $\mathbf{h}_{k,m} = \mathbf{g}_m f_{k,m}$, $m = 1,\ldots,M$, where $\mathbf{g}_m$ is the m-th column of $\mathbf{G}^H$ and $f_{k,m}$ is the m-th entry of $\mathbf{f}_k$. The subchannels of the cascaded channel extend the dimension of channels for key generation from N to NM.

To estimate $\mathbf{h}_{k,m}$, Alice and Bob transmit multiple rounds of pilots to each other with a pilot overhead of at least M, which is challenging to key generation. We note that mmWave channels with extremely high carrier frequencies exhibit the well-known angular sparsity [12], [13]. There are only a few multipath components with different AoDs and AoAs between the BS and UE, which is helpful for reducing pilot overhead.

C. Sparse Cascaded Channel

We consider the virtual beam-domain representation of the geometric channel models to elaborate on the sparsity of the RIS mmWave channels. Before that, we transfer the scalar form of channels (1), (2) into the matrix form.

The BS-RIS channel in (1) is rewritten in matrix form as $\mathbf{G} = \mathbf{A}_g\mathbf{\Lambda}_g\mathbf{A}_N^H$, where $\mathbf{A}_g \in \mathbb{C}^{M\times L_g}$, $\mathbf{A}_g = [\mathbf{a}(\theta_1^g,\varphi_1^g),\ldots,,\ldots,\mathbf{a}(\theta_{L_g}^g,\varphi_{L_g}^g)]$, $\mathbf{A}_N \in \mathbb{C}^{N\times J_g}$, and $\mathbf{A}_N = [\mathbf{b}(\psi_{1,1}^g),\ldots,\mathbf{b}(\psi_{L_g,J_{L_g}}^g)]$. The matrices $\mathbf{A}_g$ and $\mathbf{A}_N$ represent the AoAs and AoDs, respectively. $\mathbf{\Lambda}_g \in \mathbb{C}^{L_g\times J_g}$, is the beam-domain channel with J_g non-zero entries, as follows

$$\mathbf{\Lambda}_g = \begin{bmatrix} g_{1,1},\ldots,g_{1,J_1} & & 0 \\ & \cdots & \\ 0 & & g_{L_g,1},\ldots,g_{L_g,J_{L_g}} \end{bmatrix}. \quad (4)$$

The k-th UE-RIS channel in (2) is rewritten in matrix form as $\mathbf{f}_k = \mathbf{A}_{f,k}\mathbf{c}_{f,k}$, where $\mathbf{A}_{f,k} \in \mathbb{C}^{M\times J_{f,k}}$, $\mathbf{A}_{f,k} = [\mathbf{a}(\theta_{1,1,k}^f,\varphi_{1,1,k}^f),\ldots,\mathbf{a}(\theta_{L_{f,k},J_{L_{f,k}},k}^f,\varphi_{L_{f,k},J_{L_{f,k}},k}^f)]$, $\mathbf{c}_{f,k} \in \mathbb{C}^{J_{f,k}\times 1}$, and $\mathbf{c}_{f,k} = [f_{1,1,k},\ldots,f_{L_{f,k},J_{L_{f,k}},k}]$.

Based on (3), the cascaded channel of the k-th UE, $\mathbf{H}_k$, is represented as a geometric channel model, which is given by

$$\begin{aligned}\mathbf{H}_k^H &= (\mathbf{A}_{f,k}^*\mathbf{c}_{f,k}^*) \diamond (\mathbf{A}_g\mathbf{\Lambda}_g\mathbf{A}_N^H) \\ &\overset{(a)}{=} \mathbf{A}_{f,k}^* \diamond \mathbf{A}_g\left(\mathbf{c}_{f,k}^* \otimes (\mathbf{\Lambda}_g\mathbf{A}_N^H)\right) \\ &\overset{(b)}{=} \mathbf{A}_{f,k}^* \diamond \mathbf{A}_g(\mathbf{c}_{f,k}^* \otimes \mathbf{\Lambda}_g)(1 \otimes \mathbf{A}_N^H) = \mathbf{A}_{M,k}\mathbf{\Lambda}_k\mathbf{A}_N^H, \quad (5)\end{aligned}$$

where $\mathbf{H}_k \in \mathbb{C}^{N\times M}$, $\mathbf{A}_{M,k} = \mathbf{A}_{f,k}^* \diamond \mathbf{A}_g$, $\mathbf{A}_{M,k} \in \mathbb{C}^{M\times L_g J_{f,k}}$, $\mathbf{\Lambda}_k = \mathbf{c}_{f,k}^* \otimes \mathbf{\Lambda}_g$, and $\mathbf{\Lambda}_k \in \mathbb{C}^{L_g J_{f,k}\times J_g}$. (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, $\mathbf{H}_k = \mathbf{A}_N(\mathbf{c}_{f,k}^T \otimes \mathbf{\Lambda}_g^H)\mathbf{A}_{M,k}^H$.

The geometric channel model (5) exhibits the sparsity of the RIS mmWave channels. Therefore, CS-based channel estimation methods can be utilized to measure the sparse channel [12]. To employ CS-based channel estimation methods, we transform the channel (5) into the virtual beam-domain channel, $\widetilde{\mathbf{H}}_k$, which is given by

$$\mathbf{H}_k = \mathbf{U}_N\widetilde{\mathbf{H}}_k\mathbf{U}_M^H, \quad (6)$$

where $\mathbf{U}_N \in \mathbb{C}^{N\times N}$ and $\mathbf{U}_M \in \mathbb{C}^{M\times M}$ are the codebooks at the BS and the RIS, respectively. From the mathematical aspects, $\mathbf{U}_N$ and $\mathbf{U}_M$ are unitary matrices consisting of samples of virtual angles.

We set $\mathbf{U}_N = [\mathbf{b}(\psi_1), \ldots, \mathbf{b}(\psi_N)]$, 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 $\mathbf{U}_M = \mathbf{U}_z \otimes \mathbf{U}_y$, where $\mathbf{U}_z = [\mathbf{a}_z(\varphi_1), \ldots, \mathbf{a}_z(\varphi_{M_z})]$, $\mathbf{U}_z \in \mathbb{C}^{M_z\times M_z}$, $\mathbf{U}_y = [\mathbf{a}_y(\theta_1, \varphi_1), \ldots, \mathbf{a}_y(\theta_{M_y}, \varphi_{M_y})]$ and $\mathbf{U}_y \in \mathbb{C}^{M_y\times M_y}$. 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 spatial elevation angle, where φ_{n_z} is the predefined elevation angle. Define $\bar{\theta}_{n_y} = \frac{d}{\lambda}\cos\varphi_{n_z}\sin\theta_{n_y} = \frac{1}{M_y}(n_y - \frac{M_y+1}{2})$ as the virtual spatial azimuth angle, $n_y = 1, \ldots, M_y$, where θ_{n_y} is the predefined azimuth angle. Thus, $\mathbf{U}_M = [\mathbf{u}(1), \mathbf{u}(2), \ldots, \mathbf{u}(J)]$ is the full-array codebook, where $J = M$ is the number of predefined directions, and $\mathbf{u}(j) = \mathbf{a}_z(\varphi_{n_z}) \otimes \mathbf{a}_y(\theta_{n_y}, \varphi_{n_z})$ with $n_z = \lfloor (j-1)/M_y \rfloor$ and $n_y = \mod(j-1, M_y)$ is the codeword of the j-th direction.

According to (6), the virtual channel representation of the beam-domain channel $\widetilde{\mathbf{H}}_k = \mathbf{U}_N^H \mathbf{H}_k \mathbf{U}_M$ is shown at the top of the next page. In (7), the equation (c) holds on if $M \to \infty$ and $N \to \infty$. The proof is shown in Appendix A.

IV. FA-Based Beam-Domain Channel Probing

The beam-domain channel is a matrix characterized by a combination of non-zero channel gains and zero values. The row and column coordinates of non-zero channel gains within the channel matrix align with the indices in the codebooks at the BS and RIS, respectively, indicating the corresponding virtual AoAs and AoDs. Compared to channel gains that change rapidly, the physical positions of BS and RIS vary much more slowly [12], [20]. Thus, it is plausible to suppose that the virtual spatial angles, i.e., AoDs from the RIS and AoAs to the BS, remain constant over several channel coherence blocks. The proposed channel probing protocol consists of two phases. In the first phase, the angular information is estimated, since the angular information changes slowly with physical positions. Benefitting from the angular sparsity, BS applies the OMP algorithm to measure the angular information. In the second phase, given the virtual AoAs and AoDs, a simple LS estimator is applied to measure the varying beam-domain channel in subsequent coherence time slots, which greatly reduces the computational complexity and pilot overhead.

A. Estimating the Virtual Spatial Angles

BS estimates the spatial angles from the uplink channel in the first phase. In the uplink channel, UEs transmit multiple packets to BS. The BS adjusts the phase shift vector for each packet to configure the sensing matrix for the OMP algorithm.

When the BS configures the phase shift vector $\mathbf{v}(t)$ for the t-th uplink packet, the k-th UE transmits the public uplink packet, $\mathbf{s}_k \in \mathbb{C}^{K\times 1}$, to the BS. The packets of K UEs are orthogonal, i.e. $\mathbf{s}_{k_1}^H \mathbf{s}_{k_2} = KP_b$ for $k_1 = k_2$ and $\mathbf{s}_{k_1}^H \mathbf{s}_{k_2} = 0$ for $k_1 \neq k_2$, where P_b is the transmit power of UEs. According to (3), the received signal at the BS is

$$\mathbf{Y}_a(t) = \sum\nolimits_{k=1}^{K} \mathbf{H}_k \mathbf{v}(t) \mathbf{s}_k^H + \mathbf{N}_a(t), \tag{8}$$

where $\mathbf{Y}_a(t) \in \mathbb{C}^{N\times K}$, $\mathbf{N}_a(t) \in \mathbb{C}^{N\times K}$ is the complex Gaussian noise, the entry of $\mathbf{N}_a(t)$ is i. i. d. n_a, and $n_a \sim \mathcal{CN}(0, \sigma_a^2)$. Then, the BS applies the angle precoding vector $\mathbf{w}^H(t)$ to transform $\mathbf{Y}_a(t)\mathbf{s}_k(\mathbf{s}_k^H\mathbf{s}_k)^{-1}$ as

$$\begin{aligned}\widehat{y}_{a,k}(t) &= \mathbf{w}^H(t)\mathbf{H}_k\mathbf{v}(t) + \mathbf{w}^H(t)\mathbf{N}_a(t)\mathbf{s}_k(\mathbf{s}_k^H\mathbf{s}_k)^{-1} \\ &= \mathbf{w}^H(t)(\mathbf{v}^T(t)\otimes\mathbf{I})\mathrm{vec}(\mathbf{H}_k) + \widehat{n}_{a,k}(t) \\ &= (\mathbf{v}^T(t)\otimes\mathbf{w}^H(t))\mathbf{F}\mathbf{x}_k + \widehat{n}_{a,k}(t),\end{aligned} \tag{9}$$

where $\widehat{y}_{a,k}(t) \in \mathbb{C}$, $\mathbf{F} = \mathbf{U}_M^* \otimes \mathbf{U}_N$, $\mathbf{F} \in \mathbb{C}^{MN\times MN}$, $\mathbf{x}_k = \mathrm{vec}(\widetilde{\mathbf{H}}_k)$, $\mathbf{x}_k \in \mathbb{C}^{MN\times 1}$, and $\widehat{n}_{a,k}(t) \in \mathcal{CN}(0, P_a\sigma_a^2/(KP_b))$. With unit power input signal, the numerical results of $\|\mathbf{w}\|_F^2$ equals the transmit power of BS, i.e., $P_a = \|\mathbf{w}\|_F^2$.

To recover the virtual spatial angles, BS receives overall V packets in (9) and stacks them into a vector, given by

$$\widehat{\mathbf{y}}_{a,k} = [\widehat{y}_{a,k}(1), \ldots, \widehat{y}_{a,k}(V)]^T = \mathbf{P}\mathbf{F}\mathbf{x}_k + \mathbf{n}_{a,k}, \tag{10}$$

where $\widehat{\mathbf{y}}_{a,k} \in \mathbb{C}^{V\times 1}$. Specially, $\mathbf{P}$ is the configuration of phase shift and precoding vectors over V packets, i.e., $\mathbf{P} = [\mathbf{v}^T(1)\otimes\mathbf{w}^H(1); \ldots; \mathbf{v}^T(V)\otimes\mathbf{w}^H(V)]$. Here, $\mathbf{n}_{a,k} = [\widehat{n}_{a,k}(t); \ldots; \widehat{n}_{a,k}(t)]$ is the uplink estimation noise. We define $\mathbf{\Phi} = \mathbf{P}\mathbf{F}$, $\mathbf{\Phi} \in \mathbb{C}^{V\times MN}$, as the sensing matrix.

Based on (10), the BS applies the OMP algorithm to measure the virtual AoAs and AoDs of the beam-domain channel [12], [13]. BS gets the $\widehat{\mathbf{x}}_k$ and rearranges the vector form into the matrix form, $\widehat{\mathbf{H}}_k$, which is the estimation of $\widetilde{\mathbf{H}}_k$. The row coordinate of a non-zero value in $\widehat{\mathbf{H}}_k$ indicates the estimation of the index of a virtual spatial angle in $\mathbf{U}_N$. Thus, the column vectors of $\mathbf{U}_N$ corresponding to row coordinates of non-zero values in $\widetilde{\mathbf{H}}_k$ represent the estimated virtual AoAs to BS, i.e., $\widehat{\mathbf{A}}_{N,k}$. The column coordinate of a non-zero value in $\widehat{\mathbf{H}}_k$ indicates the estimation of the index of a virtual spatial angle in $\mathbf{U}_M$. Thus, the column vectors of $\mathbf{U}_M$ corresponding to column coordinates of non-zero values in $\widetilde{\mathbf{H}}_k$ represent the estimated virtual AoDs from RIS, i.e., $\widehat{\mathbf{A}}_{M,k}$.

B. Channel Sampling for Beam-Domain Channels

Given the estimated virtual spatial angles, the BS and UEs only need to measure the channel gains of the beam-domain channel in the remaining coherence slots. We apply the LS estimator that has $2KL = 2K\sum_{k=1}^{K} J_{f,k}$ pilot overhead, where $J_{f,k}$ slots are consumed for estimating the beams of the k-th UE in the uplink or downlink channel sampling.

1) Uplink Channel Sampling: K UEs simultaneously transmit the t-th uplink packet to the BS. The received signal at the BS is $\mathbf{Y}_a(t)$. Applying the LS estimator, the BS gets the cascaded channel of the k-th UE as

$$\widehat{\mathbf{z}}_{a,k}(t) = \mathbf{H}_k\mathbf{v}(t) + \widehat{\mathbf{n}}_{a,k}(t), \tag{11}$$

where $\widehat{\mathbf{z}}_{a,k}(t) \in \mathbb{C}^{N\times 1}$, $\widehat{\mathbf{n}}_{a,k}(t) = \mathbf{N}_a(t)\mathbf{s}_k(\mathbf{s}_k^H\mathbf{s}_k)^{-1} \in \mathbb{C}^{N\times 1}$ is the LS estimation noise, $\widehat{\mathbf{n}}_{a,k} \sim \mathcal{CN}(0, \widehat{\sigma}_a^2\mathbf{I})$, and $\widehat{\sigma}_a^2 = \sigma_a^2/(KP_b)$ is the mean square error (MSE) of the BS.

The BS is equipped with a hybrid precoder that consists of a radio frequency (RF) precoder, $\mathbf{F}_{RF} \in \mathbb{C}^{N\times N_{RF}}$, and K digital baseband (BB) precoders, $\mathbf{f}_{BB,k} \in \mathbb{C}^{N_{RF}\times 1}$, $k = 1, \ldots, K$. Specifically, $\mathbf{F}_{RF} \in \mathbb{C}^{N\times N_{RF}}$ is the radio frequency precoder, where N_{RF} is the number of radio frequency chains

$$\widetilde{\mathbf{H}}_k = \sum_{l_g=1}^{L_g}\sum_{j_g=1}^{J_{l_g}}\sum_{l_f=1}^{L_f}\sum_{j_f=1}^{J_{l_f}} g^*_{l_g,j_g} f_{l_f,j_f,k}\mathbf{U}_N^H\mathbf{b}(\psi^g_{l_g,j_g})\times \mathbf{a}^H(-\theta^f_{l_f,j_f,k}+\theta^g_{l_g}, -\varphi^f_{l_f,j_f,k}+\varphi^g_{l_g})\mathbf{U}_M$$
$$\overset{(c)}{\approx} \sum_{l_g=1}^{L_g}\sum_{j_g=1}^{J_{l_g}}\sum_{l_f=1}^{L_f}\sum_{j_f=1}^{J_{l_f}} g^*_{l_g,k_g} f_{l_f,j_f,k}\delta(\bar{\psi}-\bar{\psi}^g_{l_g,j_g})\times\delta(\bar{\theta}+\bar{\theta}^f_{l_f,j_f,k}-\bar{\theta}^g_{l_g})\times\delta(\bar{\varphi}+\bar{\varphi}^f_{l_f,j_f,k}-\bar{\varphi}^g_{l_g}). \quad (7)$$

and $N > N_{RF}$ [21]. The BS applies the probing precoding vector, $\mathbf{p}_k = \mathbf{F}_{RF}\mathbf{f}_{BB,k}$, $\mathbf{p}_k \in \mathbb{C}^{N\times 1}$, to the k-th UE and gets

$$\widehat{z}_{a,k}(t) = \mathbf{p}_k^H\widehat{\mathbf{z}}_{a,k}(t) = \mathbf{p}_k^H\mathbf{H}_k\mathbf{v}(t) + \widehat{n}_{a,k}(t), \quad (12)$$

where $\widehat{n}_{a,k}(t) = \mathbf{p}_k^H\widehat{\mathbf{n}}_a(t)$ is the estimation noise after precoding and $\widehat{n}_{a,k}(t) \sim \mathcal{CN}(0, P_{a,k}\widehat{\sigma}_a^2)$. With the unit power of the input signal, the numerical value of $\|\mathbf{p}_k\|_F^2$ equals the transmit power of k-th UE, i.e., $\|\mathbf{p}_k\|_F^2 = P_{a,k}$.

After the k-th UE transmit L_k packets, the BS obtains L_k measurements in (12) and stacks them into a vector given by $\mathbf{z}_{a,k} = [\widehat{z}_{a,k}(1),\ldots,\widehat{z}_{a,k}(L_k)] = \mathbf{p}_k^H\mathbf{A}_N\mathbf{\Lambda}^H\mathbf{A}_{M,k}^H\mathbf{V}_k + \bar{\boldsymbol{\eta}}_{a,k}$, where $\mathbf{z}_{a,k} \in \mathbb{C}^{1\times L_k}$ and $\bar{\boldsymbol{\eta}}_{a,k} = [\widehat{n}_{a,k}(1),\ldots,\widehat{n}_{a,k}(L_k)]$.

We replace the $\mathbf{z}_{a,k}$ with its conjugate transpose, i.e.,

$$\mathbf{z}_{a,k} = \mathbf{V}_k^H\mathbf{A}_{M,k}\mathbf{\Lambda}\mathbf{A}_N^H\mathbf{p}_k + \boldsymbol{\eta}_{a,k}, \quad (13)$$

where $\mathbf{z}_{a,k} \in \mathbb{C}^{L_k\times 1}$, $\boldsymbol{\eta}_{a,k} \in \mathbb{C}^{L_k\times 1}$ is the estimation noise after precoding, and $\boldsymbol{\eta}_{a,k} \sim \mathcal{CN}(0, P_{a,k}\widehat{\sigma}_a^2\mathbf{I}_{L_k})$.

We define $\mathbf{V}_k = [\mathbf{v}(1),\ldots,\mathbf{v}(L_k)] \in \mathbb{C}^{M\times L_k}$ as the phase shift matrix to model the configuration of the phase shift vectors over L_k packets. L_k equals the number of paths from the k-th UE to RIS, i.e., $L_k = J_{f,k}$. Notably, L_k can be get from the number of non-zero values of $\widehat{\mathbf{H}}_k$ in the first phase. Thus, the total number of packets for the uplink channel sampling is $L = \sum_{k=1}^K L_k = \sum_{k=1}^K J_{f,k}$. With K packet length, the uplink pilot overhead is KL.

2) Downlink Channel Sampling: The digital BB precoding matrix is $\mathbf{F}_{BB} = [\mathbf{f}_{BB,1},\ldots,\mathbf{f}_{BB,K}]$, $\mathbf{f}_{BB} \in \mathbb{C}^{N_{RF}\times K}$. The precoded signal at the BS is expressed as $\mathbf{S} = \mathbf{F}_{RF}\mathbf{F}_{BB}\mathbf{X}$, where $\mathbf{S} \in \mathbb{C}^{N\times T_d}$, $\mathbf{X} = [\mathbf{x}_1^T,\ldots,\mathbf{x}_K^T]^T$, $\mathbf{X} \in \mathbb{C}^{K\times T_d}$, $\mathbf{x}_k \in \mathbb{C}^{1\times T_d}$ and T_d is the length of a downlink packet. $\mathbf{x}_k$ is the data symbol vector of a downlink packet with $\mathbb{E}\{\mathbf{x}_k^H\mathbf{x}_k\} = \mathbf{I}_{T_d}$. With orthogonal downlink packet to distinguish UEs, we set $T_d = K$ to distinguish K UEs.

In the t-th slot, the BS transmits the preceded signal to the UEs. The RIS controls $\mathbf{v}(t)$ to reflect it and then the k-th UE receives the signal as

$$\mathbf{y}_{b,k}(t) = \mathbf{v}^H(t)\mathbf{H}_k^H\mathbf{S} + \mathbf{n}_{b,k}(t)$$
$$= \mathbf{v}^H(t)\mathbf{H}_k^H\sum\nolimits_{k'=1}^K \mathbf{F}_{RF}\mathbf{f}_{BB,k'}\mathbf{x}_{k'} + \mathbf{n}_{b,k}(t), \quad (14)$$

where $\mathbf{y}_{b,k}(t) \in \mathbb{C}^{1\times K}$, $\mathbf{n}_{b,k}(t) \in \mathbb{C}^{1\times K}$ is the Gaussian noise vector and the noise power is σ_b^2. By the LS estimation, the k-th UE measures the cascaded channel as $\widehat{z}_{b,k}(t) = \mathbf{v}^H(t)\mathbf{H}_k^H\mathbf{p}_k + \widehat{n}_{b,k}(t)$, where $\widehat{n}_{b,k}(t) = \mathbf{n}_{b,k}(t)\mathbf{x}_k^H(\mathbf{x}_k\mathbf{x}_k^H)^{-1}$ and $\widehat{n}_{b,k}(t) \sim \mathcal{CN}(0, \widehat{\sigma}_b^2)$. The MSE of UE is $\widehat{\sigma}_b^2 = \sigma_b^2/K$.

The k-th UE collects L_k measurements as $\mathbf{z}_{b,k} = [\widehat{z}_{b,k}(1);\ldots;\widehat{z}_{b,k}(L_k)] = \mathbf{V}_k^H\mathbf{A}_{M,k}\mathbf{\Lambda}_k\mathbf{A}_N^H\mathbf{p}_k + \boldsymbol{\eta}_{b,k}$, where $\mathbf{z}_{b,k} \in \mathbb{C}^{L_k\times 1}$, $\boldsymbol{\eta}_{b,k} = [\widehat{n}_{b,k}(1);\ldots;\widehat{n}_{b,k}(L_k)]$ and $\boldsymbol{\eta}_{b,k} \sim \mathcal{CN}(0, \widehat{\sigma}_b\mathbf{I}_{L_k})$. The downlink pilot overhead is KL.

C. Channel Covariance Matrix of Antenna-Domain Channels

When the paths originate from all possible angles in front of the RIS in sub-6GHz, the CCM at the RIS can be approximated as a real matrix, as depicted in equation (11) of [9]. Especially, the spatial correlation matrix is the CCM normalized by the channel variance. In contrast, the CCM in mmWave environments does not yield a simplified version. Different from the CCM in sub-6GHz, the CCM at the RIS in mmWave environments is given by

$$\mathbf{R}_{RIS} = \mathbb{E}\left\{(\mathbf{A}_R\mathbf{g}_R)(\mathbf{A}_R\mathbf{g}_R)^H\right\} \overset{(a)}{\approx} \mathbf{A}_R\mathbb{E}\left\{\mathbf{g}_R\mathbf{g}_R^H\right\}\mathbf{A}_R^H$$
$$= \mathbf{A}_R\mathbf{\Lambda}_R\mathbf{A}_R^H, \quad (15)$$

where $\mathbf{A}_R = [\mathbf{a}(\theta_1,\varphi_1),\ldots,\ldots,\mathbf{a}(\theta_{L_R},\varphi_{L_R})] \in \mathbb{C}^{M\times L_R}$ is the matrix containing the array response vectors of L_R paths, $\mathbf{g}_R = [c_1,\ldots,c_{L_B}]^T \in \mathbb{C}^{L_B\times 1}$ is the corresponding complex gains, and $\mathbf{\Lambda}_B \in \mathbb{C}^{L_B\times L_B}$ is a diagonal matrix whose diagonal entries are channel eigenvalues. The equation (a) holds since the range of spatial angles is approximately zero in mmWave scenarios [22]. Since the BS-RIS channel is quasi-static, the spatial angles and channel gains do not change over a long time. Therefore, the CCM at the BS is not analyzed here.

To calculate the KR in mmWave environments, we initiate the construction of the CCM for subchannels of the cascaded channel, i.e., $\mathbf{h}_{s,k} = \mathrm{vec}(\mathbf{H}_k^H) \in \mathbb{C}^{NM\times 1}$. We define $\mathbf{R}_{s,k} = \mathbb{E}\{\mathbf{h}_{s,k}\mathbf{h}_{s,k}^H\}$, which is given by

$$\mathbf{R}_{s,k} = \mathbb{E}\{\mathbf{h}_{s,k}\mathbf{h}_{s,k}^H\} = \mathbb{E}\left\{\mathrm{vec}(\mathbf{H}_k^H)(\mathrm{vec}(\mathbf{H}_k^H))^H\right\}$$
$$\overset{(b)}{=} \mathbb{E}\left\{(\mathbf{A}_N^*\otimes\mathbf{A}_{M,k})\mathrm{vec}(\mathbf{\Lambda}_k)\mathrm{vec}^H(\mathbf{\Lambda}_k)(\mathbf{A}_N^T\otimes\mathbf{A}_{M,k}^H)\right\}$$
$$\approx \mathbf{U}_{s,k}\mathbf{\Lambda}_{s,k}\mathbf{U}_{s,k}^H, \quad (16)$$

where (b) holds due to $\mathrm{vec}(\mathbf{ABC}) = (\mathbf{C}^T\otimes\mathbf{A})\mathrm{vec}(\mathbf{B})$, $\mathbf{U}_{s,k} = \mathbf{A}_N^*\otimes\mathbf{A}_{M,k} \in \mathbb{C}^{NM\times J_gL_gJ_{f,k}}$ is the tall matrix describing the spatial correlation between antennas and elements, $\mathbf{\Lambda}_{s,k} = \mathbb{E}\{\mathrm{vec}(\mathbf{\Lambda}_k)\mathrm{vec}^H(\mathbf{\Lambda}_k)\} \in \mathbb{C}^{J_gL_gJ_{f,k}\times J_gL_gJ_{f,k}}$ is a matrix whose diagonal entries are channel variances of sub-channels, $\mathbf{\Lambda}_{s,k}$ describes the correlation between channel gains of sub-channels.

D. Key Rate

In practice, statistical information about Eve is hard to acquire [10]. In such a case, the KR between the BS and the k-th UE is the mutual information of their measurements, i.e., $I(\mathbf{z}_{a,k};\mathbf{z}_{b,k})$ [23]. Based on (16), we construct the covariance matrices of BS's and UE's measurements. Define $\mathbf{R}_{a,k} = \mathbb{E}\{\mathbf{z}_{a,k}\mathbf{z}_{a,k}^H\}$ and $\mathbf{R}_{b,k} = \mathbb{E}\{\mathbf{z}_{b,k}\mathbf{z}_{b,k}^H\}$ as the covariance matrices of $\mathbf{z}_{a,k}$ and $\mathbf{z}_{b,k}$, respectively. Define

$\mathbf{R}_{ab,k} = \mathbb{E}\{\mathbf{z}_{a,k}\mathbf{z}_{b,k}^H\}$ as the cross-covariance matrix of $\mathbf{z}_{a,k}$ and $\mathbf{z}_{b,k}$. Then, we get

$$\mathbf{R}_{a,k} = \mathbf{V}_{p,k}^H \mathbf{R}_{s,k} \mathbf{V}_{p,k} + \frac{P_{a,k}\sigma_a^2}{KP_b}\mathbf{I}_{L_k}, \tag{17}$$

$$\mathbf{R}_{b,k} = \mathbf{V}_{p,k}^H \mathbf{R}_{s,k} \mathbf{V}_{p,k} + \frac{\sigma_b^2}{K}\mathbf{I}_{L_k}, \tag{18}$$

$$\mathbf{R}_{ab,k} = \mathbf{R}_{ba,k} = \mathbf{V}_{p,k}^H \mathbf{R}_{s,k} \mathbf{V}_{p,k}, \tag{19}$$

where $\mathbf{V}_{p,k} = \mathbf{p}_k^* \otimes \mathbf{V}_k \in \mathbb{C}^{NM \times L_k}$ is the equivalent precoding matrix. The full CCM of both measurements is

$$\mathbf{K}_{ab,k} = \mathbb{E}\left\{ \begin{bmatrix} \mathbf{z}_{a,k} \\ \mathbf{z}_{b,k} \end{bmatrix} [\mathbf{z}_{a,k}^H, \mathbf{z}_{b,k}^H] \right\} = \begin{bmatrix} \mathbf{R}_{a,k} & \mathbf{R}_{ab,k} \\ \mathbf{R}_{ba,k} & \mathbf{R}_{b,k} \end{bmatrix}. \tag{20}$$

Therefore, the k-th UE's KR can be expressed as

$$\begin{aligned} I(\mathbf{z}_{a,k}; \mathbf{z}_{b,k}) &= \log_2 \left(\frac{|\mathbf{R}_{a,k}||\mathbf{R}_{b,k}|}{|\mathbf{K}_{ab,k}|} \right) \\ &= \log_2 \left(\frac{|\mathbf{R}_{v,k} + P_{a,k}\widehat{\sigma}_a^2 \mathbf{I}_{L_k}||\mathbf{R}_{v,k} + \widehat{\sigma}_b^2 \mathbf{I}_{L_k}|}{|(P_{a,k}\widehat{\sigma}_a^2 + \widehat{\sigma}_b^2)\mathbf{R}_{v,k} + P_{a,k}\widehat{\sigma}_a^2\widehat{\sigma}_b^2 \mathbf{I}_{L_k}|} \right), \end{aligned} \tag{21}$$

where $\mathbf{R}_{v,k} = \mathbf{V}_{p,k}^H \mathbf{R}_{s,k} \mathbf{V}_{p,k}$ is the equivalent CCM. Apparently, the KR in (21) is determined by the $\mathbf{R}_{v,k}$. Previous works on RIS-assisted key generation [10] and [8] designed the precoding and phase shift vectors to modify $\mathbf{R}_{v,k}$ so as to improve the KR. However, the BS should acquire the prior information of the equivalent CCM, which induces a burden for pilot overhead. Benefitting from the sparsity of the mmWave band, the KR in (21) can be simplified and optimized based on the prior information of virtual spatial angles.

Notably, the analytical expression of the KR relies on the Gaussian distribution assumption for the sub-channels of the cascaded channel, denoted as $\mathbf{h}_{s,k}$. Given the stationary physical locations of the BS and RIS, the BS-RIS channel $\mathbf{G}$ is quasi-static, while the channel from the k-th UE to the RIS, $\mathbf{f}_k$, is subject to variations. The assumption is widely used in [24] and [25]. Consequently, the sub-channels of the cascaded channel are modeled to follow a Gaussian distribution.

V. FA-Based Key Rate Optimization

Since the physical locations of BS and RIS are stationary, the BS-RIS channel is quasi-static, while the channel from the k-th UE to the RIS is varying. The design of probing precoding and phase shift vectors contains two steps. Firstly, the BS designs the probing precoding vector to align with the maximal channel gain of the quasi-static BS-RIS channel. Secondly, the phase shift vectors are designed to extract secret keys from varying channels from the k-th UE to RIS. Given the probing precoding and phase shift vectors, we design two algorithms to find the optimal power allocation of multiple UEs when the channel variances of beams are equal and not equal, respectively.

A. Design Probing Precoding Vector

The precoding vector is $\mathbf{p}_k = \sqrt{P_{a,k}}\mathbf{p}_{n,k}$, where $P_{a,k}$ is the power allocated to the k-th UE and $\mathbf{p}_{n,k}$ represents the unit $N \times 1$ precoding weight vector. In order to maximize the received power, $\mathbf{p}_{n,k}$ is set as the eigenvector corresponding to the maximal channel eigenvalue, i.e., the x-th column of $\widehat{\mathbf{A}}_{N,k}$. Given the $\mathbf{p}_k$, $\mathbf{z}_{a,k}$ is simplified as

$$\begin{aligned} \mathbf{z}_{a,k} &= \mathbf{V}_k^H \mathbf{A}_{M,k} \mathbf{\Lambda}_k \mathbf{A}_N^H \mathbf{p}_k + \boldsymbol{\eta}_{a,k} \\ &\approx g_M \sqrt{P_{a,k}} \mathbf{V}_k^H \mathbf{A}_{M,k}(\mathbf{c}_{f,k} \otimes \mathbf{e}) + \boldsymbol{\eta}_{a,k} \\ &= g_M \sqrt{P_{a,k}} (\mathbf{U}_M^H \mathbf{V}_k)^H (\mathbf{U}_M^H \mathbf{f}_{M,k}) + \boldsymbol{\eta}_{a,k}, \end{aligned} \tag{22}$$

where $g_M = \max\{g_{l_g,j}\}$, $\mathbf{f}_{M,k} = \mathbf{A}_{M,k}(\mathbf{c}_{f,k} \otimes \mathbf{e})$, $\mathbf{e} \in \mathbb{C}^{L_g \times 1}$ with the only 1 at the l_{max}-th column and l_{max} is the corresponding row index of $g_{l_g,j}$ in $\mathbf{\Lambda}_k$. Notably,

$$\begin{aligned} \mathbf{f}_{M,k} &= \mathbf{A}_{M,k}(\mathbf{c}_{f,k} \otimes \mathbf{e}) = (\mathbf{A}_{f,k}^* \diamond \mathbf{A}_g)(\mathbf{c}_{f,k} \otimes \mathbf{e}) \\ &\overset{(c)}{=} (\mathbf{A}_{f,k}^* \mathbf{c}_{f,k}) \diamond (\mathbf{A}_g \mathbf{e}) = (\mathbf{A}_{f,k}^* \mathbf{c}_{f,k}) \diamond (\mathbf{a}_g) \\ &\overset{(d)}{=} (\mathbf{A}_{f,k}^* \diamond \mathbf{a}_g)(\mathbf{c}_{f,k} \otimes 1) = (\mathbf{A}_{f,k}^* \diamond \mathbf{a}_g)\mathbf{c}_{f,k}, \end{aligned} \tag{23}$$

where (c) and (d) due to $(\mathbf{AC}) \diamond (\mathbf{BD}) = (\mathbf{A} \diamond \mathbf{B})(\mathbf{C} \otimes \mathbf{D})$ and $\mathbf{a}_g$ is the AoD of g_M in $\mathbf{A}_g$.

Similarly, we get $\mathbf{z}_{b,k} = g_M \sqrt{P_{a,k}} \mathbf{V}_k^H \mathbf{f}_{M,k} + \boldsymbol{\eta}_{b,k}$. According to [21], an indiscriminate power allocation is configured for all RF chains, i.e., $\mathbf{f}_{BB,k} = \frac{\sqrt{P_{a,k}}}{N_{RF}} \mathbf{1}_{N_{RF}}$ and $\mathbf{F}_{RF} = [\mathbf{p}_{n,k}, \ldots, \mathbf{p}_{n,k}]$. Therefore, $\mathbf{p}_k$ can be decomposed as $\mathbf{F}_{RF}\mathbf{f}_{BB,k}$. Specially, $\mathbf{p}_{n,k} = \cdots = \mathbf{p}_{n,K}$ since all UEs share the same BS-RIS channel.

B. Channel Covariance Matrix of Beam-Domain Channels

The CCM of $\mathbf{f}_{M,k}$ is $\mathbf{R}_{f,k} = \mathbb{E}\left\{\mathbf{f}_{M,k}\mathbf{f}_{M,k}^H\right\}$. The virtual beam-domain channel is defined as $\widetilde{\mathbf{f}}_{M,k} = \mathbf{U}_M^H \mathbf{f}_{M,k}$, $\widetilde{\mathbf{f}}_{M,k} \in \mathbb{C}^{M \times 1}$. The CCM of $\widetilde{\mathbf{f}}_{M,k}$ is $\widetilde{\mathbf{R}}_{f,k} = \mathbb{E}\left\{\widetilde{\mathbf{f}}_{M,k}\widetilde{\mathbf{f}}_{M,k}^H\right\}$. Based on [26], the channel variance of $\mathbf{c}_{f,k}$ are equal in isotropic environments. We set $\sigma_{f,k,l}^2 = \sigma_{f,k}^2$ for $l = 1, \ldots, J_{f,k}$. The normalized CCM of $\widetilde{\mathbf{f}}_M$ is $\widetilde{\mathbf{R}}_{n,k} = \mathbb{E}\left\{\widetilde{\mathbf{f}}_{M,k}\widetilde{\mathbf{f}}_{M,k}^H\right\}/\sigma_{f,k}^2$.

To investigate the normalized CCM of a UE, we ignore the subscript k of $\widetilde{\mathbf{R}}_{n,k}$ for simplicity. According to Appendix A, the normalized CCM is calculated at the top of the next page (24), where $x = \frac{1}{M_z}(p_z - \frac{M_z+1}{2})$, $y = \frac{1}{M_y}(p_y - \frac{M_y+1}{2})$, $p = (M_y - 1)p_z + p_y$ and $q = (M_y - 1)q_z + q_y$, and $f(\varphi_f, \theta_f)$ is the probability density function. The (24) 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 $\widetilde{\mathbf{R}}$, which is computed as $\mathcal{A} = \{p | p = (M_y - 1)p_z + p_y, p \in \mathbb{Z}, \lfloor M_z \frac{d}{\lambda} \sin\varphi_f^{\min} \rfloor + \frac{M_z+1}{2} \leq p_z \leq \lfloor M_z \frac{d}{\lambda} \sin\varphi_f^{\max} \rfloor + \frac{M_z+1}{2}, \lfloor M_y \frac{d}{\lambda} \cos\varphi_{f,i} \sin\theta_f^{\min} \rfloor + \frac{M_y+1}{2} \leq p_y \leq \lfloor M_y \frac{d}{\lambda} \cos\varphi_f \sin\theta_f^{\max} \rfloor + \frac{M_y+1}{2}\}$.

C. Design Phase Shift Matrix

Based on the CCM analysis of $\widetilde{\mathbf{f}}_{M,k}$, we observe that the virtual beam-domain channel can be approximated as a matrix where the channel gains $\mathbf{c}_{f,k}$ are present at specific locations, while the remaining entries are zero. The index of non-zero values in $\widetilde{\mathbf{f}}_{M,k}$ denote the channel gains corresponding to the

$$\lim_{M_z,M_y\to\infty}[\widetilde{\mathbf{R}}_n]_{p,q}=[\mathbb{E}\left\{\mathbf{U}_M^H\mathbf{a}(\theta_f,\varphi_f)\mathbf{a}(\theta_f,\varphi_f)^H\mathbf{U}_M\right\}]_{p,q}$$
$$=\int_{\theta_f^{\min}}^{\theta_f^{\max}}\int_{\varphi_f^{\min}}^{\varphi_f^{\max}}\delta(\frac{d}{\lambda}\sin\varphi_f-x)\delta(q_z-p_z)\delta(\frac{d}{\lambda}\cos\varphi_f\sin\theta_f-y)\delta(q_y-p_y)f(\varphi_f,\theta_f)d\varphi_f d\theta_f, \quad (24)$$

samples of $\mathbf{A}_{M,f,k}$. Based on (23), $\mathbf{A}_{M,f,k}=\mathbf{A}_{f,k}^*\diamond\mathbf{a}_g\in\mathbb{C}^{M\times J_{f,k}}$ is the paths from the k-th UE to the RIS and then to the BS through the path with the best channel gain. To estimate the virtual beam-domain channel $\widetilde{\mathbf{f}}_{M,k}$, the phase shift matrix $\mathbf{V}_k$ is configured as $\sqrt{M}\widehat{\mathbf{A}}_{M,f,k}$. With the estimated channels $\widehat{\mathbf{A}}_{M,k}$, $\widehat{\mathbf{A}}_{M,f,k}$ consisting of $J_{f,k}$ columns is selected from $\widehat{\mathbf{A}}_{M,k}$. Given the $\mathbf{V}_k$, $\mathbf{z}_{a,k}$ in (22) is further simplified as

$$\mathbf{z}_{a,k}\approx g_M\sqrt{MP_{a,k}}\mathbf{c}_{f,k}+\boldsymbol{\eta}_{a,k}. \quad (25)$$

Similarly, we get the measurement of the k-th UE as follows:

$$\mathbf{z}_{b,k}\approx g_M\sqrt{MP_{a,k}}\mathbf{c}_{f,k}+\boldsymbol{\eta}_{b,k}, \quad (26)$$

where $\mathbf{z}_{b,k}$ is the measurement of instantaneous channel gains $\mathbf{c}_{f,k}$. Next, we will derive the analytical expression of the KR in terms of the channel variance of $\mathbf{c}_{f,k}$ and the transmit power $P_{a,k}$. Furthermore, we will optimize the transmit power $P_{a,k}$ to maximize the KR. Notably, there is no loss of phase information in (26). Since the number of elements M is large, the size of the codebook $\mathbf{U}_M\in\mathbb{C}^{M\times M}$ is large. This ensures the array response vector of a path aligns with a specific column of $\mathbf{U}_M$ and is orthogonal to other columns. Therefore, the phase shift matrix that is designed according to $\mathbf{U}_M$ can align with array response vectors of $\mathbf{A}_{M,k}$ and eliminate the impact of the spatial angles from the RIS. Similarly, when the number of antennas N is large, the precoding vector that is designed according to $\mathbf{U}_N\in\mathbb{C}^{N\times N}$ can align with an array response vector of $\mathbf{A}_N$ and eliminate the impact of the spatial angles from the BS. However, if M and N are not large, there is a loss of phase information, presenting a potential area for future research. Nevertheless, our approach establishes an upper bound for such cases.

D. Key Rate Derivation and Optimization Problems

When the $\mathbf{p}_n$ aligns with the spatial angle of the maximal channel gain of the BS-RIS channel and the phase shift vectors align with spatial angles of $\widetilde{\mathbf{f}}_{M,k}$, the source of randomness is converted from the subchannels $\mathbf{h}_{s,k}$ in (21) to the varying channel gains $\mathbf{c}_{f,k}$. We define the CCM of $\mathbf{c}_{f,k}$ as $\mathbf{\Lambda}_{f,k}=\mathbb{E}\{\mathbf{c}_{f,k}\mathbf{c}_{f,k}^H\}=\mathrm{diag}\{[\sigma_{f,1}^2,\ldots,\sigma_{f,J_{f,k}}^2]\}$. Thus, the KR in (21) is approximated as

$$\begin{aligned}C_k&=I(\mathbf{z}_{a,k};\mathbf{z}_{b,k})\\&\approx\log_2\left(\frac{|M\sigma_g^2P_{a,k}\mathbf{\Lambda}_{f,k}+\widehat{\sigma}_a^2P_{a,k}\mathbf{I}||M\sigma_g^2P_{a,k}\mathbf{\Lambda}_{f,k}+\widehat{\sigma}_b^2\mathbf{I}|}{|M\sigma_g^2P_{a,k}(\widehat{\sigma}_a^2P_{a,k}+\widehat{\sigma}_b^2)\mathbf{\Lambda}_{f,k}+\widehat{\sigma}_b^2\widehat{\sigma}_a^2P_{a,k}\mathbf{I}|}\right)\\&=\sum_{l=1}^{J_{f,k}}\log_2\left(1+\frac{M\sigma_g^2\sigma_{f,k,l}^2P_{a,k}}{\widehat{\sigma}_a^2P_{a,k}+\widehat{\sigma}_b^2+\widehat{\sigma}_a^2\widehat{\sigma}_b^2/(M\sigma_g^2\sigma_{f,k,l}^2)}\right)\\&=\sum_{l=1}^{J_{f,k}}\log_2\left(1+\frac{1}{\eta_{a,k,l}+\eta_{b,k,l}+\eta_{a,k,l}\eta_{b,k,l}}\right),\end{aligned} \quad (27)$$

where $\eta_{a,k,l}=\frac{\widehat{\sigma}_a^2}{M\sigma_g^2\sigma_{f,k,l}^2}$ and $\eta_{b,k,l}=\frac{\widehat{\sigma}_b^2}{M\sigma_g^2\sigma_{f,k,l}^2P_{a,k}}$ are the MSE of the l-th beam of BS and k-th UE, respectively, and σ_g^2 is the variance of g_M.

Based on (27), we formulate the optimization problem of the multi-user case as follows.

$$(P1):\ \max_{P_{a,k}}\ \sum_{k=1}^{K}\sum_{l=1}^{J_{f,k}}\log_2\left(1+\frac{M\sigma_g^2\sigma_{f,k,l}^2P_{a,k}}{\widehat{\sigma}_a^2P_{a,k}+\widehat{\sigma}_b^2+\frac{\widehat{\sigma}_a^2\widehat{\sigma}_b^2}{M\sigma_g^2\sigma_{f,k,l}^2}}\right)$$
$$s.t.\ \sum\nolimits_{k=1}^{K}P_{a,k}\le P_a. \quad (28)$$

The objective function of (P1) is the key rate of K UEs, where a $\log(\cdot)$ function denotes the key rate that a UE obtains from a path of its beam-domain channel. Notably, the beam-domain channel is sparse when the number of elements and antennas is large. With the sparsity, the design method of the phase shift matrix at RIS and precoding vector at the RIS can be applied so that the objective function of (P1) is valid.

When the channel variances of complex gains in $\mathbf{f}_k$ are equal, the optimization function is simplified as

$$(P2):\ \max_{P_k}\ \sum_{k=1}^{K}\log_2\left(1+\frac{M\sigma_g^2\sigma_{f,k}^2P_{a,k}}{\widehat{\sigma}_a^2P_{a,k}+\widehat{\sigma}_b^2+\frac{\widehat{\sigma}_a^2\widehat{\sigma}_b^2}{M\sigma_g^2\sigma_{f,k}^2}}\right)$$
$$s.t.\ \sum\nolimits_{k=1}^{K}P_{a,k}\le P_a. \quad (29)$$

Next, we will design the full-array configuration with power allocation (FA w/ PA) scheme to solve (P2), which is elaborated in Section V-E. When the channel variances of beams are equal, (P2) can be solved by the classical Lagrangian multiplier method. Regarding (P1) considering channel variances are not equal, it is much more complicated, which cannot be solved by the Lagrangian multiplier method. Because the $P_{a,k}$ allocated to the k-th UE for extracting secret keys is coupled in the objective function, we proposed a full-array configuration with a deep learning-based power allocation (FA w/ DLPA) scheme to solve it, which is explained in Section V-F.

E. Full-Array Configuration with Power Allocation for (P2)

For simplicity, we define the objective function of (P2) as f. Based on [27], the solution of the Lagrangian multiplier is a global maximum when the objective function, f, is concave over a convex set. We sort to verify whether the objective function of (P2) is concave. We derive the first-order and second-order partial derivatives of f, given by

$$\begin{aligned}\frac{\partial f}{\partial P_k}&=\frac{x_{b,k}/\ln 2}{(x_{a,k}P_{a,k}^2+x_{b,k}(2x_{a,k}+1)P_{a,k}+x_{b,k}^2(x_{a,k}+1))},\\\frac{\partial^2 f}{\partial P_k^2}&=\frac{-x_{b,k}(2x_{a,k}P_{a,k}+x_{b,k}(2x_{a,k}+1))/\ln 2}{(x_{a,k}P_{a,k}^2+x_{b,k}(2x_{a,k}+1)P_{a,k}+x_{b,k}^2(x_{a,k}+1))^2},\end{aligned} \quad (30)$$

Algorithm 1 Bisection Algorithm

Input: $\{p_{h,i}\}$, P_a, μ_{max}, μ_{min}, $x_{a,k}$, $x_{b,k}$, ϵ;
Output: $\{p_i\}$, μ.
1: Set $\mu = (\mu_{min} + \mu_{max})/2$;
2: Calculate $P_{a,k}$ according to (33);
3: **repeat**
4: **if** $\sum_{k=1}^{K} P_{a,k} < P_a$ **then**
5: $\mu_{max} = (\mu_{min} + \mu_{max})/2$;
6: **else**
7: $\mu_{min} = (\mu_{min} + \mu_{max})/2$;
8: **end if**
9: Set $\mu = (\mu_{min} + \mu_{max})/2$;
10: Calculate $P_{a,k}$ according to (33);
11: **until** $|\sum_{k=1}^{K} P_{a,k} - P_a| \leq \epsilon$.

where $x_{b,k} = \frac{\widehat{\sigma}_b^2}{M\sigma_g^2\sigma_{f,k}^2}$ and $x_{a,k} = \frac{\widehat{\sigma}_a^2}{M\sigma_g^2\sigma_{f,k}^2}$. According to (30), $\frac{\partial f}{\partial P_{a,k}} \geq 0$. It is indicated that K functions of mutual information are monotonically increasing. What is more, based on (30), $\frac{\partial^2 f}{\partial P_{a,k}^2} \leq 0$, which means the K functions are concave. We can find the optimal value of (P2) by the watering filling algorithm for the KKT conditions [28].

With the water-filling level μ, we derive the corresponding KKT conditions as

$$g_k(P_{a,k}) = \frac{\partial f}{\partial P_{a,k}} = \frac{\partial I(\mathbf{z}_{a,k}; \mathbf{z}_{b,k})}{\partial P_{a,k}} = \mu, \tag{31}$$

$$\mu \left(\sum_{k=1}^{K} P_{a,k} - P_a \right) = 0, \ \sum_{k=1}^{K} P_{a,k} \leq P_a. \tag{32}$$

According to [28], $g_1(P_{a,1}) = ... = g_K(P_{a,K})$, which means the increasing rates of the transmit power assigned to the k-th UE are the same with the optimal $P_{a,k}$. Therefore, the KKT conditions (31) and (32) can be transformed to using the water-filling algorithm to find the optimal power $P_{a,k}$ and multiplier μ. Based on (31), we calculate the $P_{a,k}$ in a function of μ as

$$P_{a,k} = \frac{\sqrt{x_{b,k}^2(2x_{a,k}+1)^2 - 4x_{a,k}x_{b,k}(x_{b,k}(x_{a,k}+1) - \frac{1}{\ln 2\mu})}}{2x_{a,k}} + \frac{-x_{b,k}(2x_{a,k}+1)}{2x_{a,k}}. \tag{33}$$

Substituting $P_{a,k}$ to $\sum_{k=1}^{K} P_{a,k} = P_a$, we design a bisection algorithm to find the multiplexer μ and $P_{a,k}$ in Algorithm 1.

In step 1, the initial μ is set as $\mu = (\mu_{min} + \mu_{max})/2$. In step 2, the $P_{a,k}$ is calculated according to (33). From steps 3 to 11, we apply the bisection search to find the optimal μ until $|\sum_{k=1}^{K} P_{a,k} - P_a| \leq \epsilon$. In each loop, with a given μ, the $P_{a,k}$ is derived from (33). If Algorithm 1 ends, the final $P_{a,k}$ is the optimal power assigned to the k-th UE.

F. Full-Array Configuration with Deep Learning-Based Power Allocation for (P1)

The water-filling algorithm offers an optimal solution for (P2) when the channel variances of complex gains in $\mathbf{f}_k$ are equal. However, the optimization problem (P1) can not be solved by Algorithm 1 since the transmit power of the k-th UE is coupled for $J_{f,k}$ beams with different channel variances. Inspired by [10], a deep learning-based algorithm provides a solution for more complex problems. In order to solve (P1), we design an unsupervised DNN-based power allocation algorithm, referred to as KGPA-Net. The objective is to develop a DNN that can effectively learn the correlation between the power information and channel variance of UEs, and subsequently determine the optimal values of $P_{a,k}, k = 1, 2, \cdots, K$, that maximize the SNR at the receiver.

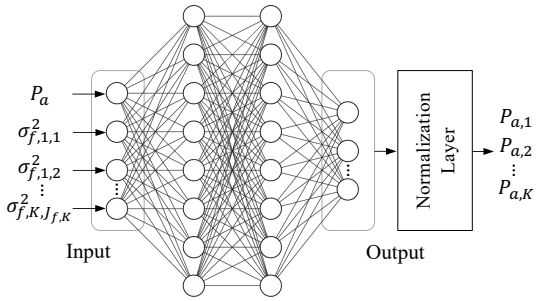

Fig. 3. KGPA-Net.

The KGPA-Net architecture, as depicted in Fig. 3, takes as input a 1×1 tensor representing the power range of UEs, denoted as $[p_{min}, p_{max}]$, and K 4×1 tensors representing the channel variances of paths. The model then utilizes two fully connected (FC) layers as hidden layers for feature extraction, with ReLu serving as the activation function. The output layer comprises one $K \times 1$ FC layer and one $K \times 1$ normalization layer. The output of the FC layer is denoted by $\mathbf{p}' = \left[P'_{a,1}, P'_{a,2}, \cdots, P'_{a,K}\right]^T$. To satisfy the total power constraint, the normalization layer performs

$$P_{a,k} = P_a \frac{P'_{a,k}}{\sum_{k=1}^{K} P'_{a,k}}, k = 1, 2, \cdots, K. \tag{34}$$

In the training phase, KGPA-Net updates parameters by unsupervised learning with the aim of maximizing KR. This is accomplished by minimizing the loss function given by

$$Loss = -\frac{1}{N_m} \sum_{n=1}^{N_m} \sum_{k=1}^{K} I(\mathbf{z}_{a,k,n}; \mathbf{z}_{b,k,n}), \tag{35}$$

where N_m is the number of training samples, $\mathbf{z}_{a,k,n}$ and $\mathbf{z}_{b,k,n}$ are the measurements in the n-th training. A smaller loss function corresponds to a higher average SKR. The DNN is updated using the stochastic gradient descent method (Adam optimizer) with a learning rate of 0.001. The training process is performed offline. In the online inference phase, the BS allocates power directly to UEs based on the output of the trained neural network, as soon as it receives the power and channel variances of the UEs.

Our proposed neural network exclusively utilizes fully connected layers, also known as a multilayer perceptron [29], which is simpler compared to other deep learning architectures like convolutional neural networks and recurrent neural networks. This simplicity is sufficient for our purposes, as our network is designed to learn the relationship between power

allocation, beam domain power variance, and total power, without the need for more complex structures. In the future, if the complexity of the optimization problem increases, we may consider exploring other network architectures.

G. Complexity Analysis

We analyze the complexity of the FA w/ PA scheme. Firstly, the BS uses the OMP algorithm to estimate the spatial angles. The complexity of the OMP algorithm is given by $\mathcal{O}(nml)$, where n is the measurement length, m is sparse signal length with sparsity level l [12], [30]. For a UE, the BS uses V packets to estimate $J_g J_{f,k}$ paths from a $MN \times 1$ sparse vector. Therefore, the complexity is $\mathcal{O}(VMNJ_gJ_{f,k})$. Assume K UEs with the same number of paths J_f. The complexity is $\mathcal{O}(KVMNJ_gJ_f)$. Secondly, the BS and UEs use the LS estimator to measure the beam-domain channels. The complexity is $\mathcal{O}(2L)$, where $L = \sum_{k=1}^{K} J_{f,k}$ is the sum of all paths [12].

Finally, the BS uses Algorithm 1 to find the power allocation. The complexity of Algorithm 1 is determined by the precision parameter ϵ. In Algorithm 1, the bisection algorithm seeks to find μ to satisfy $\sum_{k=1}^{K} P_{a,k} = P_{\max}$. The search interval is $[\mu_{\min}, \mu_{\max}]$. If the accuracy of the bisection search is ϵ, then $\frac{\mu_{\max}-\mu_{\min}}{2^{T_P}} \leq \epsilon_2$, where T_P is the iteration count. The total complexity of Algorithm 1 is $\mathcal{O}(T_P)$.

In the FA w/ DLPA scheme, the BS employs the KGPA-Net for the allocation of transmit powers. The offline training complexity remains a challenge due to the intricate implementation of the backpropagation process during training, as noted in [31]. Hence, our focus lies solely on the complexity of the online deployment, which relies on straightforward matrix-vector multiplications. In the KGPA-Net, there are two FC layers, where the first layer has $L_1 = 400$ units and the second layer has $L_1 = 200$ units. Also, the dimension of the input of the KGPA-Net is $4K+1$, and the dimension of the output is K. According to [32], the computational complexity of a linear layer is $\mathcal{O}(U_1U_2)$, where U_1 and U_2 represent the dimensions of the input and output. The complexity of the first layer, the second layer and the output layer are $\mathcal{O}((4K+1)L_1)$, $\mathcal{O}(L_1L_2)$ and $\mathcal{O}(L_2K)$, respectively. Therefore, the total complexity is $\mathcal{O}((4K+1)L_1 + L_1L_2 + L_2K)$.

VI. Sub-Array Configuration

When the number of UEs gets larger, the total pilot overhead $2KL$ is heavy in the full-array configuration with power allocation (FA w/ PA) in Section IV. Besides, as analyzed in (24), the estimated beam-domain channel of different UEs are correlated if their beams are overlapping. To reduce the pilot overhead and relieve the channel correlation, the k-th UE can extract secret keys from the $L_{n,k}$ non-overlapping beams. The total number of packets for the channel probing is $2L_n = 2\sum_{k=1}^{K} L_{n,k}$. However, the pilot overhead is still linear to the number of UEs. To further relieve the pilot overhead in multi-user systems, we use the sub-array configuration (SA) [33], where a sub-array serves a UE. A sub-array consisting of parts of elements configures the reflection coefficients to a dedicated UE. A RIS can be subdivided into sub-arrays, enabling the simultaneous reflection of signals towards K UEs.

A. Channel Model

We divide the horizontal reflecting elements of RIS into K adjacent groups, each of which has $L = M_y/K$ elements. The cascaded channel of the k-th UE (5) in the full-array configuration is decomposed to $R = K$ sub-cascaded channel since the RIS is divided into a set of R sub-arrays. The cascaded channel from the k-th UE to the r-th sub-array is

$$\mathbf{H}_{r,k} = \mathbf{A}_N(\mathbf{c}_{f,k}^T \otimes \mathbf{\Lambda}_g^H)\mathbf{A}_{M,r,k}^H, \tag{36}$$

where $\mathbf{A}_{M,r,k} = \mathbf{A}_{f,r,k}^* \diamond \mathbf{A}_{g,r} \in \mathbb{C}^{M_s \times L_g J_{f,k}}$, $\mathbf{A}_{g,r} = [\mathbf{a}_s(\theta_1^g, \varphi_1^g), \ldots, \mathbf{a}_s(\theta_{L_g}^g, \varphi_{L_g}^g)] \in \mathbb{C}^{M_s \times L_g}$, $\mathbf{A}_{f,r,k} = [\mathbf{a}_s(\theta_{1,1,k}^f, \varphi_{1,1,k}^f), \ldots, \mathbf{a}_s(\theta_{L_{f,k},J_{L_{f,k}},k}^f, \varphi_{L_{f,k},J_{L_{f,k}},k}^f)] \in \mathbb{C}^{M \times J_{f,k}}$, $\mathbf{H}_{r,k} \in \mathbb{C}^{N \times M_s}$, and $M_s = LM_z$ is the number of elements of a sub-array. Notably, $\mathbf{a}_s(\theta, \varphi) = \mathbf{a}_z(\varphi) \otimes \mathbf{a}_{y,s}(\theta, \varphi)$ is the ARV of the r-th sub-array, where $\mathbf{a}_s \in \mathbb{C}^{M_s \times 1}$ and $\mathbf{a}_{y,s}(\theta_{n_y}, \varphi_{n_z}) = \frac{1}{\sqrt{M_y}}[1, \ldots, e^{j2\pi(L-1)\frac{d}{\lambda}\cos\varphi_{n_z}\sin\theta_{n_y}}]^T$ is the ARV of L adjacent elements along the y-axis.

The sub-array codebooks of sub-arrays are set differently. The r-th sub-array codebook is $\mathbf{U}_{s,r} \in \mathbb{C}^{LM_z \times J}$ that comprises $J = M$ codewords, i.e., $\mathbf{U}_{s,r} = [\mathbf{u}_r(1), \ldots, \mathbf{u}_r(J)]$. Notably, $\mathbf{u}_r(j) = \mathbf{u}_z(j) \otimes \mathbf{u}_{y,r}(j)$ is the codeword of the j-th direction for the r-th sub-array. We have $\mathbf{u}_z(j) = \mathbf{a}_z(\varphi_{n_z})$ and $\mathbf{u}_{y,r}(j) = [\mathbf{a}_y(\theta_{n_y}, \varphi_{n_z})]_{(r-1)L+1:rL} = e^{j(r-1)L\bar{\theta}_{n_y}}\mathbf{a}_{y,r}(\theta_{n_y}, \varphi_{n_z})$, where $\bar{\theta}_{n_y} = \frac{d}{\lambda}\cos\varphi_{n_z}\sin\theta_{n_y} = \frac{1}{M_y}(n_y - \frac{M_y+1}{2})$. Thus, the virtual beam-domain channel of the k-th UE through the r-th sub-array is $\widetilde{\mathbf{H}}_{r,k} = \mathbf{U}_N^H\mathbf{H}_{r,k}\mathbf{U}_{s,r}$.

B. Channel Sampling

1) Uplink Channel Sampling: K UEs simultaneously transmit uplink packets to the BS. The received signal of BS is

$$\mathbf{Y}_a^s(t) = \sum\nolimits_{r=1}^{R}\sum\nolimits_{k=1}^{K}\mathbf{H}_{r,k}\mathbf{v}_r(t)\mathbf{s}_k^H + \mathbf{N}_a^s(t), \tag{37}$$

where $\mathbf{v}_r(t)$ is the phase shift vector of the r-th sub-array, $\mathbf{Y}_a^s(t) \in \mathbb{C}^{N \times K}$, and $\mathbf{N}_a^s(t) \in \mathbb{C}^{N \times K}$ is the complex Gaussian noise matrix with zero mean and σ_a^2 variance.

The BS measures the cascaded channel of the k-th UE as

$$\widehat{\mathbf{z}}_{a,k}^s(t) = \sum\nolimits_{r=1}^{R}\mathbf{H}_{r,k}\mathbf{v}_r(t) + \widehat{\mathbf{n}}_{a,k}^s, \tag{38}$$

where $\widehat{\mathbf{n}}_{a,k}^s = \mathbf{N}_a^s(t)\mathbf{s}_k(\mathbf{s}_k^H\mathbf{s}_k)^{-1}$ is the LS estimation noise, $\widehat{\mathbf{n}}_{a,k}^s \sim \mathcal{CN}(0, \widehat{\sigma}_a^2\mathbf{I})$, and $\widehat{\sigma}_a^2 = \sigma_a^2/(KP_b)$ is the MSE of UE.

The BS applies the precoding vector, $\mathbf{p}_{s,k} = \mathbf{F}_{RF}\mathbf{f}_{BB,k}$, $\mathbf{p}_{s,k} \in \mathbb{C}^{N \times 1}$, to the k-th UE and gets

$$\widehat{z}_{a,k}^s(t) = \mathbf{p}_{s,k}^H\widehat{\mathbf{z}}_{a,k}^s(t) = \mathbf{p}_{s,k}^H\sum\nolimits_{r=1}^{R}\mathbf{H}_{r,k}\mathbf{v}_r(t) + \widehat{n}_{a,k}^s, \tag{39}$$

where $\widehat{n}_{a,k}^s = \mathbf{p}_{s,k}^H\widehat{\mathbf{n}}_{a,k}^s$ is the estimation noise after precoding and $\widehat{n}_{a,k}^s \sim \mathcal{CN}(0, P_{a,k}\widehat{\sigma}_a^2)$.

After UEs transmit L_s packets, the BS receives L_s packets and stacks them into a vector $\mathbf{z}_{a,k}^s = [\widehat{z}_{a,k}^s(1), \ldots, \widehat{z}_{a,k}^s(L_s)] = \mathbf{p}_{s,k}^H\sum_{r=1}^{R}\mathbf{H}_{r,k}\mathbf{V}_r + \bar{\boldsymbol{\eta}}_{a,k}^s$, where $\mathbf{z}_{a,k}^s \in \mathbb{C}^{1 \times L_s}$ and $\bar{\boldsymbol{\eta}}_{a,k}^s = [\widehat{n}_{a,k}^s(1), \ldots, \widehat{n}_{a,k}^s(L_s)] \in \mathbb{C}^{1 \times L_s}$. We replace $\mathbf{z}_{a,k}^s$ by its conjugate transpose and substitute (36) to it, given by

$$\mathbf{z}_{a,k}^s = \sum\nolimits_{r=1}^{R}\mathbf{V}_r^H\mathbf{A}_{M,r,k}(\mathbf{c}_{f,k}^* \otimes \mathbf{\Lambda}_g)\mathbf{A}_N^H\mathbf{p}_{s,k} + \boldsymbol{\eta}_{a,k}^s, \tag{40}$$

where $\mathbf{z}^s_{a,k} \in \mathbb{C}^{L_s \times 1}$ and $\boldsymbol{\eta}^s_{a,k} \in \mathbb{C}^{L_s \times 1} \sim \mathcal{CN}(0, P_{a,k}\widehat{\sigma}^2_a \mathbf{I})$.

We define $\mathbf{V}_r = [\mathbf{v}_r(1), \ldots, \mathbf{v}_r(L_s)] \in \mathbb{C}^{M \times L_s}$ as the phase shift matrix to model the configuration of the phase shift vector of the r-th sub-array over L_s packets. The total number of packets for the uplink channel sampling in the sub-array configuration is L_s, where $L_s = \max\{L_{n,k}\}$ and $L_{n,k}$ equals the number of non-overlapping beams of the k-th UE. With K packet length, the uplink pilot overhead is KL_s.

2) Downlink Channel Sampling: In the t-th slot, the BS transmits downlink packets to UEs. The RIS controls $\mathbf{v}_r(t)$ to reflect the downlink packet and then the k-th UE receives the signal as $y^s_{b,k}(t) = \sum_{r=1}^{R} \mathbf{v}^H_r(t)\mathbf{H}^H_{r,k}\mathbf{p}x + n^s_{b,k}(t)$, where $\mathbf{p} = \mathbf{F}_{RF}\mathbf{f}_{BB}$ is the downlink precoding vector shared by all UEs, $\|\mathbf{p}\|^2_F = P_a$, and x is the symbol with $x * x^H = 1$.

The k-th UE conducts the LS estimation to measure the cascaded channel as $\widehat{z}^s_{b,k}(t) = \sum_{r=1}^{R} \mathbf{v}^H_r(t)\mathbf{H}^H_{r,k}\mathbf{p} + \widehat{n}^s_{b,k}(t)$, where $\widehat{n}^s_{b,k}(t) = n^s_{b,k}(t)x^H(xx^H)^{-1} \sim \mathcal{CN}(0, \widehat{\sigma}^2_b)$ and $\widehat{\sigma}^2_b = \sigma^2_b$ is MSE of UE. The k-th UE collects L_s measurements as $\mathbf{z}^s_{b,k} = [\widehat{z}^s_{b,k}(1); \ldots; \widehat{z}^s_{b,k}(L_s)]$, which is given by

$$\mathbf{z}^s_{b,k} = \sum\nolimits_{r=1}^{R} \mathbf{V}^H_r \mathbf{A}_{M,r,k}(\mathbf{c}^*_{f,k} \otimes \mathbf{\Lambda}_g)\mathbf{A}^H_N \mathbf{p} + \boldsymbol{\eta}^s_{b,k}, \quad (41)$$

where $\mathbf{z}^s_{b,k} \in \mathbb{C}^{L_s \times 1}$, $\boldsymbol{\eta}^s_{b,k} = [\widehat{n}_{b,k}(1); \ldots; \widehat{n}_{b,k}(L_s)]$ and $\boldsymbol{\eta}^s_{b,k} \sim \mathcal{CN}(0, \widehat{\sigma}_b \mathbf{I})$. The pilot overhead for the downlink channel sampling in the SA configuration is L_s. Therefore, the total pilot overhead of the SA configuration is $(K+1)L_s$.

C. Key Rate of the Sub-Array Configuration

Similar to the precoding vector design in full-array configuration, the uplink and downlink precoding vector in sub-array configuration is set as $\mathbf{p} = \sqrt{P_a}\mathbf{p}_{n,k}$ and $\mathbf{p}_{s,k} = \sqrt{P_{a,k}}\mathbf{p}_{n,k}$, respectively. Define $\mathbf{h}_{r,k} = \mathbf{H}^H_{k,r}\mathbf{p}_{n,k}$, $\mathbf{h}_{r,k} \in \mathbb{C}^{M \times 1}$, and $\mathbf{R}_{r,k} = \mathbb{E}\{\mathbf{h}_{k,r}\mathbf{h}^H_{k,r}\}$. When the channels of different UEs become independent, we calculate the covariance matrices as

$$\mathbf{R}^r_{a,k} = P_{a,k} \sum\nolimits_r \mathbf{V}^H_r \mathbf{R}_{r,k} \sum\nolimits_r \mathbf{V}_r + P_{a,k}\widehat{\sigma}^2_a \mathbf{I}, \quad (42)$$

$$\mathbf{R}^r_{b,k} = P_a \sum\nolimits_r \mathbf{V}^H_r \mathbf{R}_{k,r} \sum\nolimits_r \mathbf{V}_r + \widehat{\sigma}^2_b \mathbf{I}, \quad (43)$$

$$\mathbf{R}^r_{ab,k} = \mathbf{R}_{ba,k} = \sqrt{P_{a,k}P_a} \sum\nolimits_r \mathbf{V}^H_r \mathbf{R}_{r,k} \sum\nolimits_r \mathbf{V}_r, \quad (44)$$

Therefore, we have (45), which is shown at the top of the next page. In order to cancel the interference from other UEs, $\mathbf{V}_r$ should be designed as $\mathbf{R}_{r,k}\mathbf{V}_r = 0$, for $r \neq k$. Consequently, the objective function can be simplified as (46), which is shown at the top of the next page, where $\xi_{a,k,l} = \frac{\widehat{\sigma}^2_a}{M_s \sigma^2_g \sigma^2_{f,k,l}}$ and $\xi_{b,k,l} = \frac{\widehat{\sigma}^2_b}{M_s \sigma^2_g \sigma^2_{f,k,l} P_a}$ are the MSE of the l-th beam of BS and the k-th UE, respectively.

VII. Key Generation Protocol

A. Quantization

BS and the k-th UE convert channel measurements, $\mathbf{z}_{a,k}(t)$ and $\mathbf{z}_{b,k}(t)$, respectively, to binary sequences. We apply a single threshold quantization, $\mathcal{Q}(\cdot)$, which is a common practice in the key generation field [34], [35]. Each UE carries out quantization independently, given by $\boldsymbol{K}_{b,k} = \mathcal{Q}(\mathbf{z}_{b,k})$. We use the bit disagreement rate (BDR) to quantify the difference between the sequences of BS and the k-th UE. The BDR is defined as BDR $= \frac{\sum_{i=1}^{l_k} |\boldsymbol{K}_{a,k}(i) - \boldsymbol{K}_{b,k}(i)|}{l_k}$, where l_k is the sequence length. To mitigate the BDR, alternative quantization methods, such as the guardband-based method [36] or the correlation-based method [37], can be employed. Interested readers can refer to various quantization methods in [38].

B. Information reconciliation and privacy amplification

Due to noise, disparities arise between the sequences of BS and UEs after quantization. To address these discrepancies, both BS and UEs apply information reconciliation methods such as Cascade and secure sketch to remove inconsistencies [3]. A comprehensive overview of various information reconciliation methods is available in [39].

During the preceding information reconciliation process, BS and UEs must exchange partial information over a public channel. An eavesdropper could exploit this exchanged information to make educated guesses about the secret keys. Consequently, the eavesdropper gains an advantage in finding the secret keys more efficiently. BS and UEs utilize privacy amplification methods to transform the sequences into shorter secret keys to wipe off the leaked information. Widely adopted privacy amplification techniques include the leftover hash lemma, cryptographic hash functions, and the Merkle-Damgard hash function, as detailed in [3].

VIII. Security Analysis

In our paper, we assume eavesdroppers are located half-wavelength distance from the UEs so that the wireless channels of eavesdroppers are uncorrelated with UEs. However, if an Eve is near a UE, the beam-domain channel of the Eve may be correlated with that of a UE. According to [14], if an Eve is too close to the k-th UE, parts of their beams may overlap. We define $\mathcal{L}$ as the set of l_{leak} overlapping beams. The beam-domain channel of the k-th UE and the Evs is $\mathbf{c}_{f,k}$ and $\mathbf{c}_{f,e}$, respectively. We define the l-th beam of $\mathbf{c}_{f,k}$ and $\mathbf{c}_{f,e}$ are $z_{e,l}$ and $z_{b,l}$, respectively. If $z_{e,l}$ and $z_{b,l}$ are overlapping, the cross-correlation between $z_{e,l}$ and $z_{b,l}$ is given by $\rho = \mathbb{E}\{z_{e,l}z^*_{b,l}\}/\sqrt{\mathbb{E}\{z_{e,l}z^*_{e,l}\}\mathbb{E}\{z_{b,l}z^*_{b,l}\}}$.

If Eve is near to the k-th UE and is capable of the ability of the UE to estimate the downlink channel as described in Section IV, parts of beams are overlapping and there is leaked information of secret keys. According to [40], if Eve possesses less knowledge regarding the measurement of k-th UE $\mathbf{z}_{b,k}$ compared to the BS, or similarly, has less information about the measurement of the BS $\mathbf{z}_{a,k}$ than the k-th UE, this disparity in information can be effectively utilized for key generation. We calculate the achievable KR as follows:

$$\begin{aligned} C_{k,o} &= I(\mathbf{z}_{a,k}; \mathbf{z}_{b,k}) - \min\{I(\mathbf{z}_e; \mathbf{z}_{b,k}), I(\mathbf{z}_e; \mathbf{z}_{a,k})\} \\ &\overset{(a)}{=} I(\mathbf{z}_{a,k}; \mathbf{z}_{b,k}) - I(\mathbf{z}_e; \mathbf{z}_{b,k}) = C_k - \sum\nolimits_{l \in \mathcal{L}} I(\widehat{z}_{e,l}; \widehat{z}_{b,l}) \\ &= \sum_{l=1}^{J_{f,k}} \log_2\left(1 + \frac{1}{\eta_{a,k,l} + \eta_{b,k,l} + \eta_{a,k,l}\eta_{b,k,l}}\right) \\ &\quad - \sum_{l \in \mathcal{L}} \log_2\left(1 + \frac{\rho^2}{1 - \rho^2 + \eta_{b,k,l} + \eta_{e,k,l} + \eta_{b,k,l}\eta_{e,k,l}}\right), \end{aligned} \quad (47)$$

$$C_{s,k} = \log_2\left(\frac{|\sum_r \mathbf{V}_r\mathbf{R}_{r,k}\sum_r \mathbf{V}_r + P_{a,k}\widehat{\sigma}^2_{a,k}\mathbf{I}||\sum_r \mathbf{V}_r\mathbf{R}_{r,k}\sum_r \mathbf{V}_r + \widehat{\sigma}^2_{b,k}\mathbf{I}|}{|(P_{a,k}\widehat{\sigma}^2_{a,k}+\widehat{\sigma}^2_{b,k})\sum_r \mathbf{V}_r\mathbf{R}_{k,r}\sum_r \mathbf{V}_r + P_{a,k}\widehat{\sigma}^2_{a,k}\widehat{\sigma}^2_{b,k}\mathbf{I}|}\right) \tag{45}$$

$$= \log_2\left(\frac{|P_{a,k}\mathbf{V}_k\mathbf{R}_{r,k}\mathbf{V}_k + P_{a,k}\widehat{\sigma}^2_{a,k}\mathbf{I}||P_a\mathbf{V}_k\mathbf{R}_{r,k}\mathbf{V}_k + \widehat{\sigma}^2_{b,k}\mathbf{I}|}{|(P_a\widehat{\sigma}^2_{a,k}+\widehat{\sigma}^2_{b,k})P_{a,k}\mathbf{V}_k\mathbf{R}_{r,k}\mathbf{V}_k + P_{a,k}\widehat{\sigma}^2_{a,k}\widehat{\sigma}^2_{b,k}\mathbf{I}|}\right) = \sum_{l=1}^{L_{n,k}}\log_2\left(1+\frac{1}{\xi_{a,k,l}+\xi_{b,k,l}+\xi_{a,k,l}\xi_{b,k,l}}\right). \tag{46}$$

where $\mathbf{z}_e$ is the measurement of Eve, $\eta_{e,k,l}$ is the MSE of the l-th beam of Eve, C_k in (27) is the KR of the k-th UE when all the beams of the UE and the Eve are non-overlapping. When $\sigma_a^2 = \sigma_b^2$ and $P_a = P_b$, the equation (a) holds due to $\eta_{a,k,l} = \sigma_a^2/(KM\sigma_g^2\sigma_{f,k,l}^2 P_b) \leq \eta_{b,k,l} = \sigma_b^2/(KM\sigma_g^2\sigma_{f,k,l}^2 P_{a,k})$.

IX. Numerical Results

This section showcases the numerical results to validate the performance of the proposed key generation schemes

A. Parameter Settings

1) Device Configuration: The BS is located on the x-axis with antenna spacing $d_a = \lambda/2$ and $\lambda = 0.01$ m, where the coordinate of the first antenna is $(9.84, 1.07, 1.37)$. The first reflecting element is located at $(29.54, 3.68, 3.68)$. The side length of an element is normalized by the wavelength and set as half-wavelength, i.e., $d_r = \frac{d_r}{\lambda} = \frac{1}{2}$. The two UEs are located at the $x-y$ plane. The transmitting powers of the BS and UEs are set identically as $P_t = P_a = P_b$ dBm. All noise powers are set as $\sigma_0^2 = \sigma_a^2 = \sigma_b^2 = -96$ 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 $\epsilon_{ar} = 2.2$ and $\epsilon_{br} = 2.8$, respectively.

The number of clusters in the BS-RIS channel is $L_g = 2$ and each cluster has 3 paths. The channel variance of the BS-RIS channel is $\sigma_g^2 = 1$. The number of clusters in each UE-RIS channel is $L_{f,k} = 2$ and each cluster has 2 paths. The channel variance of the k-th UE-RIS channel is $\sigma_{f,k,l}^2 = 1$.

B. The Proposed and Compared Schemes

The proposed schemes are summarized as:

1) **Full-array configuration with power allocation (FA w/ PA):** The LS method is employed to estimate the beam-domain channel in (6). The precoding and phase-shift vectors are configured according to Section V. The power allocation based on Algorithm 1 is used to optimize the KR in (29) in Section V-E.
2) **Full-array configuration without correlation (FA w/o C):** The configuration of phase shift and precoding vectors are the same as the full-array configuration. The pilot length is chosen based on non-overlapping beams.
3) **Sub-array configuration (SA):** The LS method is employed to estimate the beam-domain channel in (6). The precoding and phase-shift vectors are configured in Section VI. Since the KR in (46) is determined by P_a, the power $P_{a,k}$ is equally allocated.
4) **Full-array configuration with Deep learning-based power allocation (FA w/ DLPA):** The beam-domain channel in (6) is estimated. The precoding and phase-shift vectors are configured according to Section V. The deep-learning-based power allocation is shown in Section V-F to optimize the KR in (28).

The benchmark schemes are summarized as:

1) **Random configuration (RA):** Both the precoding and phase-shift vectors are randomly configured [5]. The equivalent channel in (3) is measured.
2) **CCM-based configuration (CCM):** The equivalent channel in (3) is measured. Both the precoding matrix [10] and the phase-shift vector [8] are optimized based on the CCM of subchannels in (16) to maximize (21).
3) **Hardamard-pattern configuration (HP):** According to [16], the subchannels of the cascaded channel in (5) is measured. The precoding and phase-shift vectors are configured in the Hardamard pattern [18].
4) **Full-array configuration (FA):** The beam-domain channel in (6) is measured. The precoding and phase-shift vectors are configured according to Section V. With equal power allocation, the KR in (29) is calculated.

C. Performance Analysis

The figures presented use solid or dashed lines to represent numerical results, while simulation results are denoted by markers. Monte Carlo simulations are used to verify the numerical results, and the *ITE* toolbox [41] is employed to calculate the mutual information of the measurements of the BS and the UEs for further validation.

1) Evaluation of KR: We evaluated the KR of two UEs against transmit power, the number of reflecting elements as well as antennas and then extended it to more UEs.

Figure 4 depicts the beam-domain channel of a UE. The BS-RIS channel comprises 2 clusters, each containing 3 paths. As shown in Fig. 4, three non-zero values along the y-axis represent a cluster of the BS-RIS. Additionally, the UE-RIS is composed of 2 clusters, each containing 2 paths. The two non-zero values along the x-axis represent a cluster of the UE-RIS. Given that the BS-RIS channel has a total of $2 \times 3 = 6$ paths and the UE-RIS channel has $2 \times 2 = 4$ paths, Fig. 4 exhibits a total of $6 \times 4 = 24$ non-zero values, since the beam-domain channel is the cascade of the BS-RIS and UE-RIS channels.

Figure 5 exhibits the KR that BS and two UEs can extract in each channel probing with different transmit powers. The two UEs are located at $(0, 0, 0)$ and $(150, 150, 0)$. In FA w/ PA configuration, the BS and a UE apply the channel probing

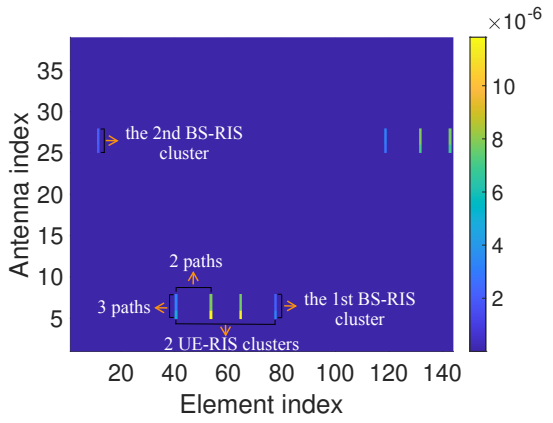

Fig. 4. The beam-domain channel of a UE. $N = 39$, $M = 144$.

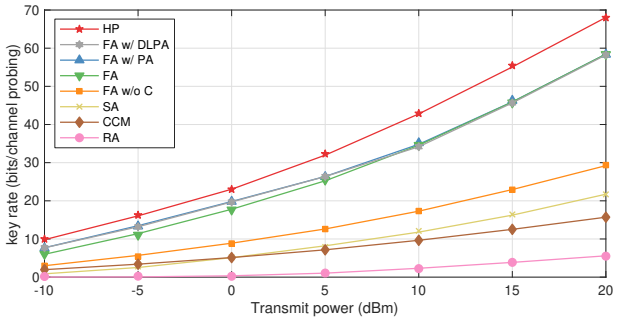

Fig. 5. KR versus transmit power. $N = 39$, $M = 144$.

protocol in Section IV to estimate a cluster of 4 paths. The increase in the transmit power has a big influence on the KR since the high power improves the similarity of their measurements. The KR of the FA w/ DLPA configuration fits the KR of the FA w/ PA configuration, which validates the performance and reduces the complexity. The KR of the RA configuration is the least favourable due to the possibility of the random phase shift vector being orthogonal to the spatial angles of the beam-domain channel, resulting in almost zero channel variance. Additionally, the average disparity between the KR of the FA w/ PA configuration and the RA configuration is substantial. This is attributed to the beam-domain channel offering more channel dimensions for key generation, thereby enhancing the overall key rate. Compared to the HP configuration, the FA w/ PA configuration also has a small decrease, since the HP configuration consumes more pilot overhead to estimate the subchannels of the cascaded channel and the estimation noise is smaller. However, there exists serious auto-correlation between the measurements from the HP configuration while the measurements from the proposed scheme are nearly uncorrelated.

Figure 6 illustrates the KR per channel probing for a different number of reflecting elements. It is apparent that the KR improves with the number of reflecting elements since the increase of reflecting elements improves the SNR at the receivers. What's more, the KR of the CCM configuration does not increase greatly, because the channel dimension is limited. As shown in Fig. 6, the KR of the FA configuration

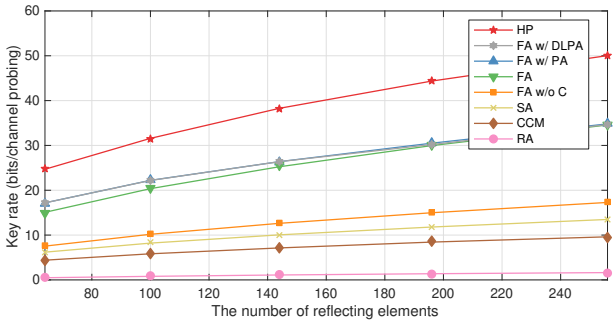

Fig. 6. KR versus the number of reflecting elements. $N = 39$, $P_t = 5$ dBm.

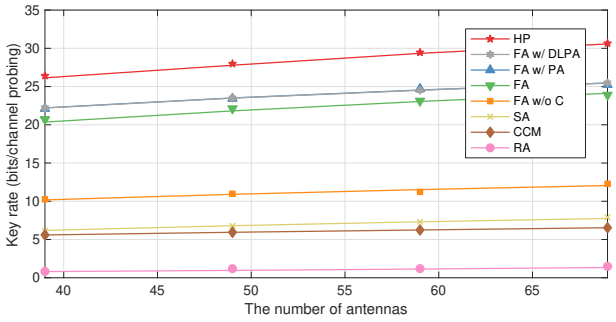

Fig. 7. KR versus the number of antennas. $M = 100$, $P_t = 5$ dBm.

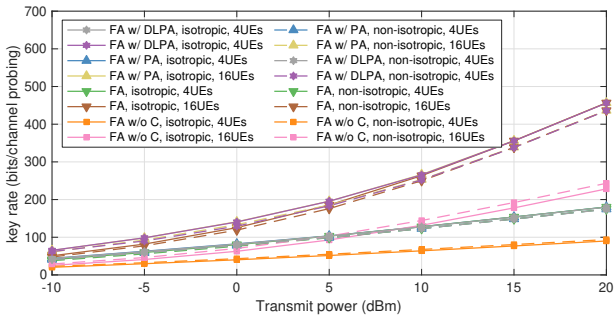

Fig. 8. KR versus transmit power in Muli-user systems. $N = 39$, $M = 256$.

approaches the KR of the FA w/ PA configuration with the increase of elements. Since when the estimation noise gets smaller, the optimal power allocation strategy for FA w/ PA generally approaches equal power allocation. Furthermore, Fig. 7 investigates the KR versus the number of antennas. It is observed that the KR increases with antennas. With the increment in the number of antennas, the estimation of the most powerful beam from the BS to the RIS is more accurate, which improves the KR.

Figure 8 extends the case of two UEs to the case of multiple UEs. The former simulation considers the isotropic environment, where the channel variances of beams are equal and the (P1) is solved. The FA w/ DLPA scheme can solve the (P2) in the non-isotropic environment, where the channel variances of beams are not equal. Therefore, Fig. 8 illustrates the performance of the FA w/ DLPA configuration for the system where the channel variances of paths in $\mathbf{f}_k$ are not equal. In the case of non-equal channel variances, the channel variances of 4 paths are set as $1.323, 1.312, 1.184, 1.181$.

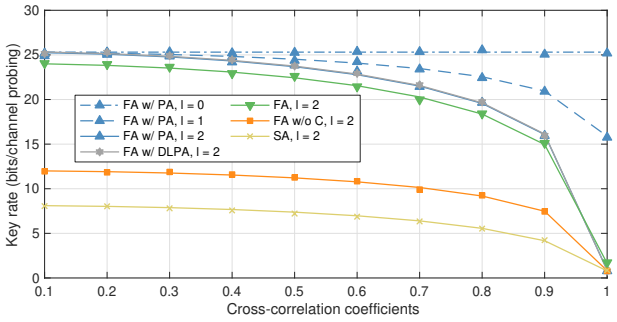

Fig. 9. KR versus cross-correlation. $N = 39$, $M = 144$, $P_t = 5$ dBm.

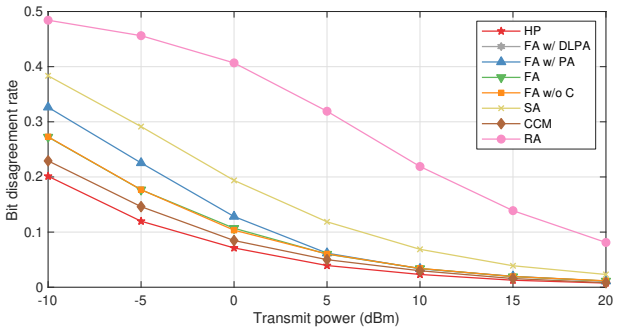

Fig. 10. BDR versus transmit power. $N = 39$, $M = 144$.

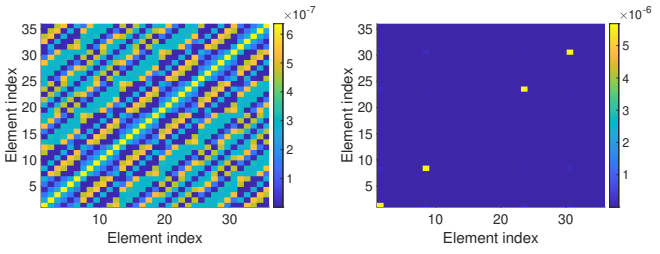

Fig. 11. (a) Correlation of channels in the antenna domain. (b) Correlation of channels in the beam domain. $N = 46$, $M = 36$.

TABLE I
RANDOMNESS TEST RESULTS

	FA w/ PA	FA w/ DLPA	FA w/o C	SA
Frequency	0.15	0.11	0.74	0.01
Block frequency	0.57	0.22	0.46	0.46
Runs	0.72	0.57	0.23	0.60
Longest run of 1s	0.86	0.83	0.16	0.66
DFT	0.83	0.80	0.81	0.08
Serial	0.65	0.36	0.39	0.73
	0.64	0.68	0.59	0.98
Appro. entropy	0.34	0.85	0.62	0.38
Cum. sums. (fwd)	0.23	0.16	0.85	0.01
Cum. sums. (rev)	0.19	0.07	0.54	0.02

Firstly, with the increase in the number of UEs, the total KR of the system is increased. Secondly, in the case of FA w/ PA, the KR extracted from the paths with equal channel powers is greater than the KR extracted from the paths with different channel powers. Finally, in the case of FA w/o C, the KR extracted from the paths with equal channel powers is smaller than the KR extracted from the paths with different channel variances, since each UEs extract KRs from the first two strongest paths.

2) Evaluation of Evesdropping: Figure 9 illustrates the effect of cross-correlation between the beam-domain channels of a UE and an Eve on the KR. In this scenario, two clusters, each containing two paths, are shared between the UE and Eve, leading to correlated channel gains. As the cross-correlation coefficient increases from 0.1 to 1, there is a noticeable decline in the KR for the proposed schemes, denoted by solid lines. This decrease occurs because Eve intercepts more secret keys as the cross-correlation rises. Furthermore, Fig. 9 also explores the FA w/ PA scheme under two additional conditions: the presence of a single overlapping cluster and the absence of any overlapping clusters, depicted with dashed lines. The highest line represents the scenario without overlapping clusters between the UE and Eve, indicating either the absence of Eve or Eve far away from the UE. When there are one or two overlapping clusters, the KR is lower compared to the scenario without overlapping clusters.

3) Evaluation of BDR: As shown in Section VII-A, after the channel probing process, the BS and UEs quantize their measurements into binary sequences. We evaluated the BDR of two UEs against transmit power.

The plot in Fig. 10 illustrates the relationship between the BDR and the transmit power. It is observed that the BDR decreases as the transmit power increases. This can be attributed to the fact that higher SNR values result in fewer discrepancies between the measurements of Alice and Bob. The BDR of the HP configuration is smaller than other schemes since the pilot length is NM which greatly reduces the estimation power. The BDR of the RA configuration is the highest because the random phase shift vector may be orthogonal to the spatial angles of the $\mathbf{f}_k$ which makes the channel power nearly zero. The SA configuration exhibits a higher BDR compared to other proposed schemes due to the scaling of the complex gain by the inverse of the number of UEs, resulting in impaired performance. The BDR of the FA w/ PA configuration is higher than the FA configuration since the water-filling algorithm allocated more power to the UE with stronger UEs. Therefore, the BDR of the poorer UE will greatly increase the total BDR.

4) Evaluation of Randomness: We investigate the impact of spatial correlation on the randomness of measurements of beams in fading blocks, which are used as a random source for key generation. As shown in Fig. 11, the spatial correlation between channel coefficients in the antenna domain is serious, while the spatial correlation between channel coefficients in the beam domain is weak. To evaluate the randomness of the measurements, we employ the National Institute of Standards and Technology (NIST) test suite, a widely used tool in the key generation field [34]. Specifically, we generate 6000 fading blocks, where each block contains 4 measurements of 4 paths, with $N = 39$, $M = 144$, and $P_t = 20$ dBm. We apply 9 statistical tests from the NIST test suite using the toolbox [42], and for each test, we obtain a p value. A p value greater than 0.01 indicates that the sequence passes the particular randomness test. Our results, summarized in Table I, show that

all the p values are greater than 0.01. The simulation results show that the spatial correlation of beam-domain channels does not affect the randomness of measurements.

X. Discussion

A. Large-Scale UEs

When the number of UEs increases, more than one UE might have the same spatial angles. If two UEs near each other have paths of the same spatial angle, the complex gains of the paths are correlated. In the worst case, two UEs have two paths sharing the spatial angle and having highly correlated complex gain, where the complex gain is near the same. The secret keys extracted from these two paths can not be used. In such worst case, the key rate is given by

$$C_W = \sum_{k=1}^{K} \sum_{l \in \mathcal{G}_k} \log_2 \left(1 + \frac{M \sigma_g^2 \sigma_{f,k,l}^2 P_{a,k}}{\widehat{\sigma}_a^2 P_{a,k} + \widehat{\sigma}_b^2 + \frac{\widehat{\sigma}_a^2 \widehat{\sigma}_b^2}{M \sigma_g^2 \sigma_{f,k,l}^2}} \right), \tag{48}$$

where $\mathcal{G}_k$ is the set containing the indices of the paths which do not overlap with paths of other UEs.

B. The Condition for Distinguishing UEs

As described in Section IV-A, the BS uses the OMP algorithm to estimate the spatial angles. The codebook is $\mathbf{F} = \mathbf{U}_M^* \otimes \mathbf{U}_N$, where $\mathbf{U}_M$ and $\mathbf{U}_N$ predefine the spatial angles at the RIS and the BS, respectively. The number of paths of the BS-RIS and the k-th UE-RIS channels are J_g and $J_{f,k}$, respectively. A non-zero value in the beam-domain channel of the k-th UE $\mathbf{x}_k$ corresponds to a column vector of $\mathbf{F}$. Although UEs share the same BS-RIS channel, the non-zero values of $\{\mathbf{x}_k\}$ are on different entries since the spatial angles of the UE-RIS channels are different. According to [13] and [30], the total number of non-zero elements in $\mathbf{x}_k$ is $J_g J_{f,k}$, which is always much smaller than the size of the codebook MN. With the sparsity of mmWave channels, the OMP algorithm can be used to estimate $\{\mathbf{x}_k\}$ and the coordinates of $\{\mathbf{x}_k\}$ help distinguish the spatial angles of UEs.

XI. Conclusion

In conclusion, this paper addressed the challenges of optimizing PLKG in RIS-assisted mmWave multi-user systems. By transforming channels from the spatial domain to the beam domain, we proposed an effective channel probing method based on the OMP and LS algorithms to acquire angular information and channel gain. Analyzing the CCM of the beam-domain channel, we observed uncorrelated channel gains, which influenced our approach to KR optimization. Through the design of phase shift and precoding vectors, along with power allocation methods based on the water-filling algorithm and deep learning, we achieved superior key generation performance. Additionally, we introduced a sub-array configuration scheme that leveraged differences in spatial angles between users, successfully reducing pilot overhead. The presented numerical results verified the efficacy of our proposed methods, demonstrating their superiority over existing CCM-based algorithms in PLKG.

Appendix

A. Proof of the Sparsity Property

In order to prove the Eq. (7), we should prove the sparsity property of the virtual beam-domain channel from both sides of BS and RIS. If the elevation and azimuth angles of a path from RIS are φ_0 and θ_0, respectively, we have

$$\begin{aligned}
&[\mathbf{U}_M^H \mathbf{a}(\theta_0, \varphi_0)]_n = \left(\mathbf{a}_z^H(\varphi_n)\mathbf{a}_z(\varphi_0)\right) \otimes \left(\mathbf{a}_y^H(\theta_n, \varphi_n)\mathbf{a}_y(\theta_0, \varphi_0)\right) \\
&= \frac{1}{M} \sum\nolimits_{m_z} e^{-i2\pi(m_z-1)(\bar{\varphi}_0 - \bar{\varphi}_{n_z})} \sum\nolimits_{m_y} e^{-i2\pi(m_y-1)(\bar{\theta}_0 - \bar{\theta}_{n_y})} \\
&= \frac{1}{M} e^{-i\pi(M_z-1)(\bar{\varphi}_0 - \bar{\varphi}_{n_z})} \frac{\sin(-\pi M_z(\bar{\varphi}_0 - \bar{\varphi}_{n_z}))}{\sin(-\pi(\bar{\varphi}_0 - \bar{\varphi}_{n_z}))} \\
&\times e^{-i\pi(M_y-1)(\bar{\theta}_0 - \bar{\theta}_{n_y})} \frac{\sin(-\pi M_y(\bar{\theta}_0 - \bar{\theta}_{n_y}))}{\sin(-\pi(\bar{\theta}_0 - \bar{\theta}_{n_y}))},
\end{aligned} \tag{49}$$

where $\bar{\varphi}_0 = \frac{d}{\lambda} \sin\varphi_0$, $\bar{\theta}_0 = \frac{d}{\lambda} \cos\varphi_0 \sin\theta_0$, $\bar{\varphi}_{n_z} = \frac{d}{\lambda} \sin\varphi_{n_z}$, $\bar{\theta}_{n_y} = \frac{d}{\lambda} \cos\varphi_{n_z} \sin\theta_{n_y}$, $n_y = \mod(n-1, M_y)$ and $n_z = \lfloor (n-1)/M_y \rfloor$. If M_z and M_y go to infinity, we have

$$\lim_{M_z M_y \to \infty} [\mathbf{U}_M^H \mathbf{a}(\theta_0, \varphi_0)]_n = \delta(\bar{\varphi}_0 - \bar{\varphi}_{n_z}) \delta(\bar{\theta}_0 - \bar{\theta}_{n_y}), \tag{50}$$

where $\delta(x) = 0$ if $x \neq 0$; $\delta(x) = 1$ if $x = 0$.

If the azimuth angle of a path from BS is ψ_0, we can similarly prove $\lim_{N \to \infty} [\mathbf{U}_N^H \mathbf{b}(\psi_0)]_n = \delta(\bar{\psi}_0 - \bar{\psi}_n)$, where $\bar{\psi}_0 = \frac{d}{\lambda} \sin\psi_0$, $\bar{\psi}_n = \frac{d}{\lambda} \sin\psi_n$.

References

[1] 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.

[2] V.-l. Nguyen, P.-c. Lin, B.-c. Cheng *et al.*, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart. 2021.

[3] 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.

[4] M. Ragheb, A. Kuhestani, M. Kazemi *et al.*, "RIS-aided secure millimeter-wave communication under RF-chain impairments," *IEEE Trans. Veh. Technol.*, pp. 1–13, 2023, early access.

[5] 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.

[6] 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.

[7] 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.

[8] L. Hu, G. Li, X. Qian *et al.*, "Joint transmit and reflective beamforming for RIS-assisted secret key generation," 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2207.11752

[9] E. Björnson and L. Sanguinetti, "Rayleigh fading modeling and channel hardening for reconfigurable intelligent surfaces," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 830–834, Apr. 2020.

[10] C. Chen, J. Zhang, T. Lu *et al.*, "Machine learning-based secret key generation for IRS-assisted multi-antenna systems," in *Proc. IEEE ICC*, Rome, Italy, May 2023, pp. 1–6.

[11] L. Jiao, N. Wang, and K. Zeng, "Secret beam: Robust secret key agreement for mmWave massive MIMO 5G communication," in *Proc. IEEE GLOBECOM*, Abu Dhabi, UAE, Dec. 2018, pp. 1–6.

[12] 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.

[13] X. Wei, D. Shen, and L. Dai, "Channel estimation for RIS assisted wireless communications - part II: An improved solution based on double-structured sparsity," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1403–1407, Jan. 2021.

[14] G. Li, C. Sun, E. A. Jorswieck *et al.*, "Sum secret key rate maximization for TDD multi-user massive MIMO wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 968–982, Sep. 2021.

[15] T. Lu, L. Chen, J. Zhang *et al.*, "Reconfigurable intelligent surface-assisted key generation for millimeter wave communications," in *Proc. IEEE WCNC Workshops*, Glasgow, U. K., Mar. 2023, pp. 1–6.

[16] ——, "Joint precoding and phase shift design in reconfigurable intelligent surfaces-assisted secret key generation," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 3251 – 3266, Apr. 2023.

[17] Y. Ju, G. Zou, H. Bai *et al.*, "Random beam switching: A physical layer key generation approach to safeguard mmWave electronic devices," *IEEE Trans. Consum. Electron.*, pp. 1–15, May 2023.

[18] A. L. Swindlehurst, G. Zhou, R. Liu *et al.*, "Channel estimation with reconfigurable intelligent surfaces-A general framework," *Proceedings of the IEEE*, vol. 110, no. 9, pp. 1–27, Sep. 2022.

[19] R. Li, S. Sun, Y. Chen *et al.*, "Ergodic achievable rate analysis and optimization of RIS-assisted millimeter-wave MIMO communication systems," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 2, pp. 972–985, Feb. 2022.

[20] A. Adhikary, J. Nam, J.-y. Ahn *et al.*, "Joint spatial division and multiplexing — The large-scale array regime," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6441–6463, Oct. 2013.

[21] Z. Wan, Z. Gao, F. Gao *et al.*, "Terahertz massive MIMO with holographic reconfigurable intelligent surfaces," *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4732–4750, Jul. 2021.

[22] H. Xie, F. Gao, S. Jin *et al.*, "Channel estimation for TDD/FDD massive MIMO systems with channel covariance computing," *IEEE Trans. Wirel. Commun.*, vol. 17, no. 6, pp. 4206–4218, Jun. 2018.

[23] B. T. Quist and M. A. Jensen, "Maximization of the channel-based key establishment rate in MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5565–5573, Oct. 2015.

[24] P. Wang, J. Fang, X. Yuan *et al.*, "Intelligent reflecting surface-assisted millimeter wave communications: Joint active and passive precoding design," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14 960–14 973, Dec. 2020.

[25] C. Hu, L. Dai, S. Han *et al.*, "Two-timescale channel estimation for reconfigurable intelligent surface aided wireless communications," *IEEE Trans. Commun.*, vol. 69, no. 11, pp. 7736–7747, Nov. 2021.

[26] H. Yin, D. Gesbert, M. Filippou *et al.*, "A coordinated approach to channel estimation in large-scale multiple-antenna systems," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 264–273, Feb. 2013.

[27] B. T. Quist and M. A. Jensen, "Optimal channel estimation in beamformed systems for common-randomness-based secret key establishment," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 558–559, Jul. 2013.

[28] C. Xing, Y. Jing, S. Wang *et al.*, "New viewpoint and algorithms for water-filling solutions in wireless communications," *IEEE Trans. Signal Process.*, vol. 68, pp. 1618–1634, Feb. 2020.

[29] T. Jiang, H. V. Cheng, and W. Yu, "Learning to reflect and to beamform for intelligent reflecting surface with implicit channel estimation," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 7, pp. 1931–1945, Jul. 2021.

[30] Y. You, L. Zhang, M. Yang *et al.*, "Structured OMP for IRS-assisted mmWave channel estimation by exploiting angular spread," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 4444–4448, Apr. 2022.

[31] A. Abdallah, A. Celik, M. M. Mansour *et al.*, "RIS-aided mmWave MIMO channel estimation using deep learning and compressive sensing," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 5, pp. 3503–3521, May 2023.

[32] L. Dai and X. Wei, "Distributed machine learning based downlink channel estimation for RIS assisted wireless communications," *IEEE Trans. Commun.*, vol. 70, no. 7, pp. 4900–4909, Jul. 2022.

[33] C. You, B. Zheng, and R. Zhang, "Fast beam training for IRS-assisted multiuser communication," *IEEE Wireless Commun. Lett.*, vol. 9, no. 11, pp. 1845–1849, Nov. 2020.

[34] J. Zhang, R. Woods, T. Q. Duong *et al.*, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[35] S. Mathur, W. Trappe, N. Mandayam *et al.*, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. MobiCom*, San Francisco, CA, USA, Sep. 2008, pp. 128–139.

[36] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[37] F. Ardizzon, F. Giurisato, and S. Tomasin, "Secret-key-agreement advantage distillation with quantization correction," *IEEE Commun. Lett.*, vol. 27, no. 9, pp. 2293–2297, Sep. 2023.

[38] C. Zenger, J. Zimmer, and C. Paar, "Security analysis of quantization schemes for channel-based key extraction," in *Proc. Workshop Wireless Commun. Secur. Phys. Layer*, Coimbra, Portugal, Jul. 2015, pp. 1–6.

[39] C. Huth, R. Guillaume, T. Strohm *et al.*, "Information reconciliation schemes in physical-layer security: A survey," *Comput. Netw.*, vol. 109, pp. 84–104, Nov. 2016.

[40] F. Rottenberg, T.-H. Nguyen, J.-M. Dricot *et al.*, "CSI-based versus RSS-based secret-key generation under correlated eavesdropping," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1868–1881, Mar. 2021.

[41] Z. Szabó, "Information theoretical estimators toolbox," *Journal of Machine Learning Research*, vol. 15, pp. 283–287, Jan. 2014.

[42] K. A. Steven. Randomness testsuite. GitHub repository. Accessed Mar. 27, 2022. [Online]. Available: https://github.com/stevenang/randomness_testsuite