Joint Precoding and Phase Shift Design in Reconfigurable Intelligent Surfaces-Assisted Secret Key Generation

Tianyu Lu, *Graduate Student Member, IEEE,* Liquan Chen, *Senior Member, IEEE,*
Junqing Zhang, *Member, IEEE,* Chen Chen, *Member, IEEE* and Aiqun Hu, *Senior Member, IEEE*

***Abstract*—Physical layer key generation (PLKG) is a promising technique to establish symmetric keys between resource-constrained legitimate users. However, PLKG suffers from a low key rate in harsh environments where channel randomness is limited. To address the problem, reconfigurable intelligent surfaces (RISs) are introduced to reshape the channels by controlling massive reflecting elements, which can provide more channel diversity. In this paper, we design a channel probing protocol to fully extract the randomness from the cascaded channel, i.e., the channels through reflecting elements. We derive the analytical expressions of the key rate and design a water-filling algorithm based on the Karush-Kuhn-Tucker (KKT) conditions to find the upper bound. To find the optimal precoding and phase shift matrices, we propose an algorithm based on the Grassmann manifold optimization methods. The system is evaluated in terms of the key rate, bit disagreement rate (BDR) and randomness. Simulation results show that our protocols significantly improve the key rate as compared to existing protocols. Compared to multiple-antennas systems without a RIS, our proposed method achieves an average 9.51 dB performance gain when the side length of an element is $1/4$ wavelength and the Rician factor is 0 dB.**

***Index Terms*—Physical layer security, physical layer key generation, reconfigurable intelligent surface, key rate.**

I. Introduction

THE advent of the Internet of Things (IoT) and the development of 5G raise concerns for security in communication networks [1]. The number of IoT devices will approach 75 billion by 2025 [2]. The information security of current communication and computer systems is protected by symmetric encryption and public key cryptography (PKC). Symmetric encryption, e.g., advanced encryption standard (AES), requires the same key at legitimate users. Key management and sharing are usually handled by PKC for computer networks. PKC relies on complicated mathematical algorithms such as discrete logarithms, which, however, cannot be scaled and will be threatened by quantum computers [3]. While the complexity of PKC is affordable by computer networks, it may not be applicable to many resource-constrained IoT devices with limited storage and computational power [4]. While many IoT protocols, including WiFi, ZigBee, LoRaWAN, specify AES for data encryption, they do not define key distribution approaches. In practice, the pre-shared keys are often manually configured to IoT devices and are never or very rarely refreshed, which becomes the vulnerabilities of IoT networks, as exemplified in [5].

In contrast, physical layer key generation (PLKG) from wireless channels is a promising candidate for establishing symmetric keys between two IoT devices, namely Alice and Bob [2]. PLKG does not involve computationally-expensive operations and is suitable for low-cost IoT devices. Benefiting from the temporal variation, channel reciprocity and spatial diversity properties of wireless media, PLKG achieves information-theoretical security.

- *Temporal variation*: When wireless channels change dynamically, there is sufficient randomness to be extracted.
- *Channel reciprocity*: The reciprocity between uplink and downlink channels enables Alice and Bob to share a common secret key.
- *Spatial diversity*: An eavesdropper, Eve, who is half wavelength away from Alice and Bob, cannot derive any information about the secret key.

Exploiting these features, key generation techniques can achieve information-theoretic security.

There are research explorations both from theoretical and experimental aspects, which demonstrate the potential of key generation [6]–[12]. In the seminal papers of Maurer [6] and Ahlswede and Csiszar [7] dated back to 1993, the authors laid an information-theoretic foundation for key generation and proved that Alice and Bob can use correlated randomness source to extract secret keys. Later, Maurer and Wolf investigated the secret key generation over unauthenticated public channels [8]. There have also been many works on realizing practical key generation systems, with experimental exploration using WiFi [9], ZigBee [10], LoRa [11] and Bluetooth [12].

As key generation relies on channel randomness and correlated channel measurements, it is challenging to operate well in harsh environments. Firstly, the channel variation is limited in static/quasi-static environments, which cannot

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

J. Zhang and C. Chen are with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom. (email: junqing.zhang@liverpool.ac.uk; c.chen77@liverpool.ac.uk)

A. Hu is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China. (e-mail: aqhu@seu.edu.cn)

L. Chen and A. Hu are also with the Purple Mountain Laboratories for Network and Communication Security, Nanjing, 211111, China.

provide sufficient randomness [2]. Secondly, when received signals experience a low signal-to-noise ratio (SNR), the key rate will be reduced too [13]. Therefore, it is necessary to develop new techniques to improve the key rate in harsh environments.

Recently, reconfigurable intelligent surfaces (RISs) have been introduced to address the poor channel conditions in key generation. A RIS is regarded as an emerging transmission technology to realize the concept of smart radio environments [14]. The deployment of RISs in wireless communication is attractive due to their cost-efficiency and energy-saving benefits, despite the incremental load it imposes on the system. A RIS is a passive technology comprised of reflecting elements arranged on a planar surface, which results in lower hardware and power consumption costs compared to traditional active transmitters [15]. The massive reflecting elements in RISs reflect incoming signals without complex signal processing, reducing the need for RF transceiver hardware [16]. A cost-effective RIS prototype system was achieved by using a low-cost printed circuit board with 64 PIN diodes, where each element consumed 1.5 mW of power when activated [17]. Moreover, the RISs can be installed on various surfaces, such as building facades, indoor walls, and ceilings, for providing connectivity to users [14]. Compared to traditional full-duplex relays, RISs are passive and capable of receiving and transmitting data simultaneously without sophisticated self-interference cancellation [18].

Therefore, RISs is a cost-effective and energy-efficient technology that has been adopted to solve the problem of low entropy for key generation techniques in static environments [19]–[21], where the channel remains near-constant in a long coherence time. Ji *et al.* proposed a one-time pad (OTP) encryption scheme based on the artificial randomness from the random configuration of the phase shift vector [19]. Hu *et al.* derive the theoretical upper bound of the key rate for the scheme of RIS-induced artificial randomness, where the channels of Eve are uncorrelated with the legitimate channels [20]. Lu *et al.* derive the upper bound and lower bound of the key rate affected by eavesdropping attacks in static environments [21]. When the direct channel is inadequate to generate secret keys, the implementation of RISs has been proposed as a means to establish a reflected channel, thereby enhancing the SNR and ultimately improving the key rate [22]–[25]. Ji *et al.* designed the passive beamforming of the phase shift vector at the RIS to improve the SNR at the receiver and suppress the SNR at the eavesdroppers so that the key rate can be improved [22]. Lu *et al.* found the optimal location of the active elements under the constraint that the number of reflecting elements operating simultaneously is limited so as to improve the SNR [23]. Li *et al.* extended the scheme in [23] to multiple-user systems [24]. Liu *et al.* investigated the optimization of the phase shift matrix in the multiple-input and multiple-output (MIMO) system, while they did not optimize the precoding matrix at the BS [25].

Key generation from fine-grained channel features can significantly improve the key rate [26]–[29]. Received signal strength indicator (RSSI) is a popular channel parameter for key generation [30]–[32], but its coarse-grained nature limits the key generation. Compared to RSSI, channel state information (CSI) is a fine-grained channel feature that provides more channel information. Liu *et al.* [27] analyzed the key rate extracted from the channel coefficients of all subcarriers in orthogonal frequency-division multiplexing (OFDM) systems. Later, Zhang *et al.* [26] achieved a practical key generation protocol based on IEEE 802.11 OFDM systems. In addition, randomness in the spatial domain can also be employed. Wallace *et al.* in [28] proposed to exploit the randomness from multiple antennas. In the RIS-based key generation, there are multiple channels.

- Direct channel is between Alice and Bob consisting of line-of-sight (LoS) (when there is) and non-LoS (NLoS) components not involving RIS.
- RIS-reflected subchannels: each subchannel refers to a channel from Alice to a RIS element and then to Bob.

Existing RIS-empowered key generation works to extract keys from the equivalent channel, which is combined by the direct channel and RIS-reflected subchannels. Li *et al.* [24] designed the phase shift matrix and modified the reflected channel so that Alice and Bob can extract more key bits from the equivalent channels. However, the equivalent channel is coarse-grained in nature, which limits the key rate since the dimension of reflecting elements is far larger than that of the antennas. Inspired by the multiple antenna-based and OFDM-based key generation, it is reasonable to envisage generating keys from each RIS-reflected subchannel, which is fine-grained and can provide more diversity. Surprisingly, such research effort is missing.

The joint design of beamforming and RIS will provide more channel diversity for key generation. Classical key generation systems used multiple-input and multiple-output (MIMO) techniques to improve the key rate [33], which is achieved by beamforming techniques that combine received signals from multiple antennas to improve the SNR. Similar to beamforming techniques in MIMO systems, a RIS can achieve passive beamforming to enhance the SNR at the receiver, where a RIS combines the signals from reflecting elements and automatically modifies the reflection coefficients. Previous works involved the design of the passive beamforming of RIS in systems with a single-antenna BS [22]–[24] or a multiple-antenna BS [25], but they did not consider the joint design of the transmit beamforming of the BS and the passive beamforming of the RIS. What is more, these works have overlooked the crucial aspect of spatial correlation between the channels from the elements of RIS and the antennas of BS, which greatly influences the key rate.

In this paper, we jointly optimize the precoding matrix at the multiple-antenna base station (BS) and the phase-shift matrix at the RIS and use the fine-grained channel feature for key generation. Our main technical contributions are as follows:

- We design a channel probing protocol for RIS-assisted key generation systems to fully extract randomness from the direct and cascaded channels. Since the RIS is not capable of estimating channels, our protocol decomposes the channel into the cascaded channel which can be measured by transceivers.

- We derive the analytical expression of the key rate in a RIS-assisted multi-antenna system. We optimize the precoding and phase shift matrices to improve the key rate. In order to tackle the coupling problem of two matrix variables, we optimize an equivalent matrix variable that is a combination of the precoding and phase-shift matrices. Furthermore, we introduce a water-filling algorithm based on Karush-Kuhn-Tucker (KKT) conditions to find the optimal equivalent matrix variable.
- We propose a practical algorithm to decouple the optimal equivalent matrix variable into precoding and phase shift matrices. We first obtain the optimal phase shift matrix and then resort to the Grassmann manifold optimization method to find the optimal precoding matrix.
- We validate the analytical expressions of the key rate by Monte Carlo simulations. Taking into account the spatial correlation coefficients, the transmit power, the number of elements and the Rician factor, we demonstrate that our algorithm achieves a higher key rate than the existing algorithms.

The remaining part of this paper is organized as follows. In Section II, we present the system model of RIS-assisted key generations. In Section III, we propose a RIS-assisted channel probing algorithm. Section IV studies the design of the precoding and phase shift matrices to maximize the key rate. In Section V, a key generation protocol is designed. In Section VI, numerical results are presented. Section VII offers a discussion on eavesdropping attacks and different channel conditions. In Section VIII, conclusions are drawn.

Notations: Litalic letters $(A, B, a, b, \dots)$, boldface lowercase letters $(\mathbf{a}, \mathbf{b}, \dots)$ and boldface upper-case letters $(\mathbf{A}, \mathbf{B}, \dots)$ denote scalars, vectors and matrices, respectively. Calligraphic letters $(\mathcal{A}, \mathcal{B}, \dots)$ denote sets. $\frac{\partial f}{\partial x}$ denotes the partial derivative of f with respect to x. $\mod(\cdot)$ is the modulus operator and $\lfloor \cdot \rfloor$ is the floor function. $|\cdot|$ and $\Re\{\cdot\}$ denote the magnitude and real part of a complex number, 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. $\text{Tr}(\cdot)$ is the trace operator. $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. $\mathbf{0}_N$ and $\mathbf{1}_N$ are the zero and one matrices of $N \times 1$ dimension, respectively. $\mathbf{A}_{i,j} = \mathbf{A}((i-1)m+1 : im, (j-1)n+1 : jn)$ is the submatrix of $\mathbf{A}$, with row indices spanning from $(i-1)m+1$ to im and column indices spanning from $(j-1)n+1$ to jn. $[\mathbf{A}]_{m,n}$ denotes the (m,n)-th element of matrix $\mathbf{A}$. $||\cdot||_2$ and $||\cdot||_F$ denote the Euclidean norm and Frobenius norm, respectively. $\mathcal{CN}(\mu, \sigma^2)$ 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. $\mathbb{H}$ denotes the differential entropy.

II. System Model

A. Overview

This paper considers a RIS-assisted key generation system which consists of a BS (Alice), a user equipment (UE) (Bob), and a RIS, as shown in Fig. 1. The BS is equipped with multiple antennas, while the UE is equipped with a single antenna. We consider the BS that is linked to a RIS. The BS designs an algorithm for controlling the phase shift matrix of the RIS and its precoding matrix to assist the key generation process, which will be elaborated in Section IV-B. Key generation protocol comprises five stages, namely channel probing, preprocessing, quantization, information reconciliation and privacy amplification. During channel probing, the UE and BS operate in the time division duplex (TDD) mode; they transmit pilots to each other in turn and measure the channels between them. These transmissions will be reflected by the RIS, which can bring more randomness. This paper focuses on the design of channel probing, which will be explained in Section III.

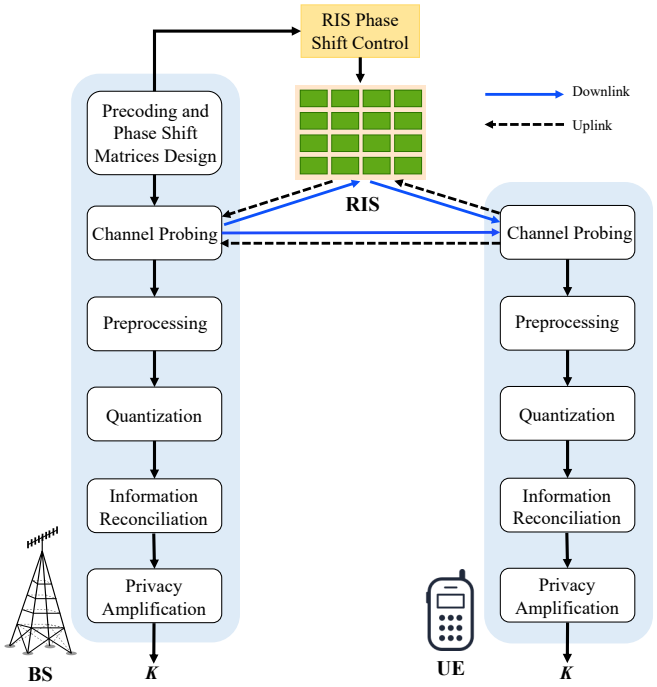


Fig. 1. System model.

Since the spatial correlation will cause self-correlation between measurements, preprocessing methods are introduced to eliminate the self-correlation between raw channel measurements. Furthermore, they convert the channel measurements into binary sequences by quantization algorithms. Due to noise, hardware mismatch, etc., there exist disagreements between quantized sequences, which can be corrected during information reconciliation. Finally, the privacy amplification algorithms are used to wipe off possible information leakage in the previous stages. The BS and UE agree on a unique secret key, $\boldsymbol{K}$. These four steps will be introduced in Section V.

B. Channel Model

1) Device Configuration: We consider a three-dimensional Cartesian coordinate system, where the RIS is deployed parallel to $y-z$ plane, as shown in Fig. 2. The RIS is modelled as a uniform planar array that has $M = M_y \times M_z$ reflecting elements with M_y elements per row and M_z elements per

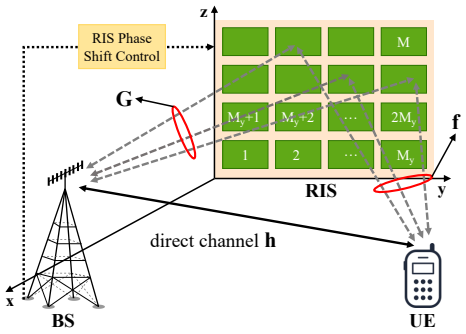


Fig. 2. Channel model.

column. The area of the RIS is MA, where d_r is the side length of an element and $A = d_r \times d_r$ is the area of an element. The location of the first reflecting element is $\mathbf{u}_1$ and the location of the other elements are denoted as $\mathbf{u}_m = \mathbf{u}_1 + d_r[0, y_m, z_m]^T$, $m = 2, \ldots, M$, where $y_m = \mod(m-1, M_y)$ and $z_m = \left\lfloor \frac{m-1}{M_y} \right\rfloor$ are the horizontal and vertical indices, respectively.

When a wave impinges on the RIS from the azimuth angle, θ, and the elevation angle, φ, the array response vector of the RIS is given by

$$\mathbf{a}(\theta, \varphi) = \mathbf{a}_z(\varphi) \otimes \mathbf{a}_y(\theta, \varphi), \tag{1}$$

where $\mathbf{a}_y(\theta, \varphi) = [1, \ldots, e^{j2\pi(M_z-1)d_r \cos\varphi \sin\theta/\lambda}]^T$, $\mathbf{a}_z(\varphi) = [1, \ldots, e^{j2\pi(M_y-1)d_r \sin\varphi/\lambda}]^T$ and λ is the wavelength.

Each element of the RIS can control the wave impinging on it. We denote the reflection coefficients of the elements as

$$\mathbf{v} = [\phi_1, \ldots, \phi_M]^T, \tag{2}$$

where ϕ_m is the reflection coefficient of the m-th element. Notably, $\phi_m = e^{j\omega_m}$, where ω_m is its phase shift which is generated from uniform quantization of $[0, 2\pi)$. The set representing all possible configurations of phase shifts is $\mathcal{K} = \{0, \frac{2\pi}{K_q}, \ldots, \frac{2\pi(K_q-1)}{K_q}\}$, where $K_q = 2^{N_q}$ is the quantization level and N_q is the number of controlling bits.

The BS is equipped with a uniform linear array (ULA) consisting of N antennas and located on the x-axis with d_a antenna spacing. When a wave impinges on the ULA from an azimuth angle, ψ, the array response vector is given by

$$\mathbf{b}(\psi) = [1, \ldots, e^{j2\pi(N-1)d_a \sin\psi/\lambda}]^T. \tag{3}$$

The BS applies a precoding matrix, $\mathbf{P}^T \in \mathbb{C}^{N_s \times N}$, for transmission or reception, where N_s is the length of the packet.

2) Individual Channel: There are three individual channels, including BS-RIS, UE-RIS, and UE-BS channels. The small-scale fading for all channels is assumed to be Rician fading, which is described as follows.

According to [34], the BS-RIS channel can be modelled as

$$\mathbf{G} = \sqrt{\frac{K_{ar}\beta_{ar}}{1+K_{ar}}}\mathbf{G}^{LoS} + \sqrt{\frac{\beta_{ar}}{1+K_{ar}}}\mathbf{G}^{NLoS}, \tag{4}$$

where $\mathbf{G}^{LoS} = \mathbf{a}(\theta_{ar}, \varphi_{ar})\mathbf{b}^H(\psi_{ar})$ is the LoS component, $\mathbf{G}^{NLoS} = \sum_l^{L_{ar}} \frac{c_{ar}^l}{\sqrt{L_{ar}}}\mathbf{a}(\theta_{ar}^l, \varphi_{ar}^l)\mathbf{b}^H(\psi_{ar}^l)$ is the NLoS component, K_{ar} is the Rician factor and β_{ar} is the distance-dependent path-loss effect.

- For the LoS component from the BS to the RIS, $\psi_{ar} \in [0, 2\pi)$ denotes the angle of departure (AoD). $\theta_{ar} \in [0, 2\pi)$ and $\varphi_{ar} \in [-\pi/2, \pi/2)$ denote the azimuth and elevation angles of arrival (AoA), respectively.
- For the NLoS component from the BS to the RIS, L_{ar} is the number of paths and c_{ar}^l denotes the corresponding complex gain associated with the l-th path. ψ_{ar}^l denotes the AoD of the l-th path. θ_{ar}^l and φ_{ar}^l denote the azimuth and elevation AoA of the l-th path, respectively. The complex gain c_{ar}^l is identically and independently distributed (i.i.d.) with zero mean and variance $A\mu_1$, where μ_1 is the average intensity attenuation.

The UE-RIS channel is modelled as

$$\mathbf{f} = \underbrace{\sqrt{\frac{K_{br}\beta_{br}}{1+K_{br}}}\mathbf{a}_r(\theta_{br}, \varphi_{br})}_{LoS} + \underbrace{\sqrt{\frac{\beta_{br}}{1+K_{br}}}\sum_{l=1}^{L_{br}}\frac{c_{br}^l}{\sqrt{L_{br}}}\mathbf{a}_{br}(\theta_{br}^l, \varphi_{br}^l)}_{NLoS}, \tag{5}$$

where K_{br} is the Rician factor and β_{br} is the path-loss effect.

- For the LoS component from the UE to the RIS, θ_{br} and φ_{br} denote the azimuth and elevation AoA, respectively.
- For the NLoS component, θ_{br}^l and φ_{br}^l denote the azimuth and elevation AoA of the l-th path, respectively. L_{br} is the number of paths and c_{br}^l denotes the complex gain associated with the l-th path.

Similarly, we model the UE-BS channel, also termed direct channel in this paper, as

$$\mathbf{h} = \underbrace{\sqrt{\frac{K_{ba}\beta_{ba}}{1+K_{ba}}}\mathbf{b}(\psi_{ba})}_{LoS} + \underbrace{\sqrt{\frac{\beta_{ba}}{1+K_{ba}}}\sum_{l=1}^{L_{ba}}\frac{c_{ba}^l}{\sqrt{L_{ba}}}\mathbf{b}(\psi_{ba}^l)}_{NLoS}, \tag{6}$$

where K_{ba} is the Rician factor and β_{ba} is the path-loss effect.

- For the LoS component from the UE to the BS, ψ_{ba} denotes the azimuth AoA.
- For the NLoS component, φ_{ba}^l denotes the azimuth AoA of the l-th path. L_{ba} is the number of paths and c_{ba}^l denotes the complex gain associated with the l-th path.

3) Cascaded Channel: When the RIS configures the phase shift vector, $\mathbf{v}$, the BS and UE can observe the combined version of individual channels, namely $\mathbf{h}$, $\mathbf{f}$ and $\mathbf{G}$. Given $\mathbf{v}$, we define the equivalent channel, $\mathbf{h}_e(\mathbf{v}) \in \mathbb{C}^{N\times 1}$, as

$$\mathbf{h}_e(\mathbf{v}) = \mathbf{h} + \mathbf{G}^T\mathrm{diag}(\mathbf{v})\mathbf{f}, \tag{7}$$

where $\mathbf{h} \in \mathbb{C}^{N\times 1}$, $\mathbf{G}^T = [\mathbf{g}_1, \ldots, \mathbf{g}_M] \in \mathbb{C}^{N\times M}$, and $\mathbf{f} = [f_1, \ldots, f_M]^T \in \mathbb{C}^{M\times 1}$. Here, $\mathbf{g}_m \in \mathbb{C}^{N\times 1}$, $m = 1, \ldots, M$, is the channel from the m-th element to the BS. The equivalent channel is composed of $\mathbf{h}$ and $\mathbf{G}^T\mathrm{diag}(\mathbf{v})\mathbf{f}$, where $\mathbf{h}$ is the UE-BS channel that does not involve the RIS and $\mathbf{G}^T\mathrm{diag}(\mathbf{v})\mathbf{f}$ is the channel that can be adjusted by the RIS. The BS and UE can directly estimate the equivalent channel and convert the measurements to secret keys, which is commonly adopted by previous works [22]–[24]. However, the equivalent channel is coarse-grained and the dimension of channel features is restricted by the number of antennas, which fundamentally limits the key rate. The equivalent channel can be decomposed to the cascaded channel composed of subchannels associated

with reflecting elements. The fine-grained subchannels greatly extend the dimension of channel features and improve the key rate.

The equivalent channel can be decomposed into the UE-BS channel, $\mathbf{h}$, and a set of channels associated with each element, $\mathbf{h}_m$. The equivalent channel in (7) can be rewritten as

$$\mathbf{h}_e(\mathbf{v}) = \mathbf{h} + \mathbf{G}^T \text{diag}(\mathbf{f})\mathbf{v}. \tag{8}$$

$\mathbf{G}^T\text{diag}(\mathbf{f}) = [\mathbf{h}_1 \ldots, \mathbf{h}_M]$ is the channel associated with elements, where $\mathbf{h}_m = \mathbf{g}_m f_m$ is the channel from the UE to the m-th element of the RIS and then to the BS. Therefore, we propose to exploit the randomness from the UE-BS channel and the channels associated with each element, which is finer-grained and can improve the key rate.

Although $\mathbf{h}$ and $\mathbf{h}_m$ provide more channel coefficients for extracting secret keys, there is a spatial correlation between $\mathbf{h}_m$ and $\mathbf{h}_n$, $m \neq n$ or between $\mathbf{h}$ and $\mathbf{h}_m$. Since the spatial correlation influences the actual secret keys, we cannot simply estimate these channels, individually quantize the measurements from each channel and then convert them to the secret keys. To analyze the secret keys influenced by the spatial correlation, we stack $\mathbf{h}$ and $\mathbf{h}_m$, $m = 1, \ldots, M$, into $\mathbf{h}_r = [\mathbf{h}^T, \mathbf{h}_1^T \ldots, \mathbf{h}_M^T]^T$. We define $\mathbf{h}_r \in \mathbb{C}^{D\times 1}$ as the BS-RIS-UE cascaded channel, which is given by

$$\mathbf{h}_r = [\mathbf{h}^T, \mathbf{h}_1^T \ldots, \mathbf{h}_M^T]^T = \text{vec}([\mathbf{h}\ \mathbf{G}^T\text{diag}(\mathbf{f})]), \tag{9}$$

where $D = N(M+1)$ is the dimension of the cascaded channel. We define the m-th entry of $\mathbf{h}_r$ as the m-th subchannel. $\mathbf{h}_r$ is composed of D subchannels.

Since the RIS is passive, we cannot directly estimate $\mathbf{G}$ and $\mathbf{f}$ at the RIS and construct the cascaded channel. In order to measure the cascaded channel, we decompose the equivalent channel as

$$\mathbf{h}_e(\mathbf{v}) \overset{(a)}{=} \left[\mathbf{h}\ \mathbf{G}^T\text{diag}(\mathbf{f})\right]\begin{bmatrix}1\\ \mathbf{v}\end{bmatrix} \overset{(b)}{=} (\bar{\mathbf{v}}^T \otimes \mathbf{I}_N)\mathbf{h}_r, \tag{10}$$

where (a) holds due to $\text{diag}(\mathbf{a})\mathbf{b} = \text{diag}(\mathbf{b})\mathbf{a}$, (b) holds due to $\text{vec}(\mathbf{ABC}) = (\mathbf{C}^T \otimes \mathbf{A})\text{vec}(\mathbf{B})$ [35] and $\bar{\mathbf{v}} = [1, \mathbf{v}^T]^T$ is the augmented phase shift vector. In Section III, we will propose a channel probing protocol in which the UE and BS design $\bar{\mathbf{v}}$ in (10) to measure the cascaded channel and extract the randomness from it.

C. Correlation Modeling

The side length of an element and the antenna spacing affects the spatial correlation between subchannels of the cascaded channel. In order to model the spatial correlation between subchannels, we analyze the correlation matrices between transmit antennas and elements.

The NLoS channel observed from RIS is spatially correlated. According to [36] and [34], the correlation matrix of the elements, $\mathbf{R}_r$, in isotropic scattering environments is modelled as

$$[\mathbf{R}_r]_{n,m} = \gamma \frac{\sin(\frac{2\pi}{\lambda}||\mathbf{u}_n - \mathbf{u}_m||_2)}{\frac{2\pi}{\lambda}||\mathbf{u}_n - \mathbf{u}_m||_2}\ n, m = 1, \ldots, M, \tag{11}$$

where $[\mathbf{R}_r]_{n,m}$ is the entry in the n-th row and the m-th column of $\mathbf{R}_r$ and $\gamma = A\mu_1$ is a normalizing factor.

There is a correlation between transmit antennas. According to [37], the correlation coefficient between the i-th and the j-th transmit antennas is given by $[\mathbf{R}_a]_{i,j} = r^{|i-j|}$, where r is the correlation coefficient and $\mathbf{R}_a$ is the covariance matrix. Therefore, $\mathbf{h} \sim \mathcal{CN}(\mathbf{0}, \gamma_h \mathbf{R}_a^{1/2})$, $\mathbf{f} \sim \mathcal{CN}(\mathbf{0}, \gamma_f \mathbf{R}_r^{1/2})$ and $\mathbf{G} = \gamma_G \mathbf{R}_r^{1/2}\mathbf{H}\mathbf{R}_a^{1/2}$, where $\mathbf{H} \in \mathbb{C}^{M\times N}$ is the random muti-path CSI matrix with identically independent distributed (i.i.d.) entries, $\gamma_h = \beta_{ba}/(K_{ba}+1)$, $\gamma_f = \beta_{br}/(K_{br}+1)$ and $\gamma_G = \beta_{ar}/(K_{ar}+1)$. The LoS component that affects the mean value can be eliminated by preprocessing [28], which will be discussed in Section V-A. The assumption of the Gaussian channel model is widely used to model the full-scattering propagation environments, e.g., in [36] and [34], where the paths are scattered from all possible directions to the receiver. However, the Gaussian assumption may not be valid in sparse environments where the number of paths is not very large, which should be explored in future.

Based on [38], the theoretical channel covariance matrix of the subchannels is given by

$$\mathbf{R}_h = \begin{bmatrix} \gamma_h \mathbf{R}_a & \mathbf{0}^T \\ \mathbf{0} & \gamma_G\gamma_f \mathbf{R}_r \odot \mathbf{R}_r \otimes \mathbf{R}_a \end{bmatrix}. \tag{12}$$

We assume the BS has knowledge of the channel covariance matrix. Let $\mathbf{R}_h = \mathbf{U}_h\mathbf{\Lambda}_h\mathbf{U}_h^H$, $\mathbf{R}_h \in \mathbb{C}^{D\times D}$, denote the eigenvalue decomposition of $\mathbf{R}_h$. Especially, $\mathbf{\Lambda}_h$ is the diagonal matrix whose diagonal entries are the eigenvalues of D subchannels and $\mathbf{U}_h$ is a unitary matrix whose columns are eigenvectors corresponding to eigenvalues. We define $\mathbf{\Lambda}_h = \text{diag}(\mathbf{p}_h)$ with $\mathbf{p}_h = [p_{h,1}, p_{h,2}, \ldots, p_{h,D}]$, where the elements in $\mathbf{p}_h$ are sorted in the descending order.

III. RIS Assisted Channel Probing

In this section, a channel probing protocol is designed to measure the cascaded channel of (9) from which the secret keys are extracted. The main difficulty is that a RIS can neither send nor receive pilots since it does not have any radio resources. Also, the dimension of the cascaded channel is D, so the BS and UE cannot measure it by only conducting one round of channel probing. However, the UE and BS can obtain partial information on the cascaded channel from (10) when they estimate the equivalent channel, so they can collect multiple measurements of the equivalent channel to recover the cascaded channel. The phase shift vector and precoding matrix are appropriately configured in each round. Furthermore, we derive the key rate of the measurements of the cascaded channel.

A. Channel Probing

As shown in Fig. 3, the channel probing consists of the uplink and downlink phases. In the uplink (downlink) phase, the UE (BS) transmits V packets to BS (UE) in fading block i. In order to recover the cascaded channel, the BS configures a combination of V phase shift vectors for V packets in the uplink or downlink phases, where the combination in the uplink phase is the same as the combination in the downlink phase.

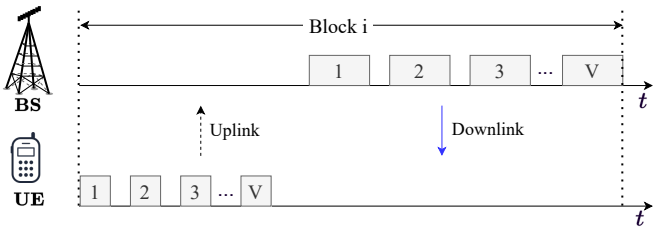


Fig. 3. Channel probing in a fading block.

In the uplink phase, each packet is $\mathbf{s} \in \mathbb{C}^{Q\times 1}$ of length Q. After receiving the uplink packet, the BS measures the channel from N antennas and applies a $N_s \times N$ precoding matrix, $\mathbf{P}^T$, to the measurements. In the downlink phase, each downlink packet, $\mathbf{P}\mathbf{S}_d^H$, is derived from multiplying the downlink pilot matrix, $\mathbf{S}_d \in \mathbb{C}^{N_s\times N_s}$, by the $\mathbf{P}$. Since the BS is equipped with N antennas, we set $Q = 1$ to let the BS observe N channel coefficients from an uplink packet. Since the UE has a single antenna, the length of a downlink packet should be larger than the number of antennas to recover the measurements. In order to let the UE observe the N channel coefficients, we set N_s as N.

1) Uplink Channel Probing: In the t-th uplink packet, the UE transmits an uplink packet to the BS when the RIS configures the phase shift vector $\mathbf{v}(t)$ to reflect it. The received signal at the BS (Alice) is given by

$$\mathbf{y}_a(t) = \mathbf{h}_e(\mathbf{v}(t))\mathbf{s}^H + \mathbf{n}_a(t), \tag{13}$$

where $\mathbf{y}_a(t) \in \mathbb{C}^{N\times 1}$ and $\mathbf{n}_a(t) \in \mathbb{C}^{N\times 1}$ is the complex Gaussian noise.

The BS then applies $\mathbf{P}^T$ to transform $\mathbf{y}_a(t)$ as

$$\widetilde{\mathbf{y}}_a(t) = \mathbf{P}^T\mathbf{y}_a(t) = \mathbf{P}^T\mathbf{h}_e(\mathbf{v}(t))\mathbf{s}^H + \mathbf{P}^T\mathbf{n}_a(t), \tag{14}$$

where $\widetilde{\mathbf{y}}_a(t) \in \mathbb{C}^{N\times 1}$.

By the least square (LS) channel estimation, the BS measures the equivalent channel as

$$\widehat{\mathbf{z}}_a(t) = \widetilde{\mathbf{y}}_a(t)\mathbf{s}(\mathbf{s}^H\mathbf{s})^{-1}, \tag{15}$$

where $\widehat{\mathbf{z}}_a(t) \in \mathbb{C}^{N\times 1}$. According to (10), the measurement obtained from the t-th packet can be expanded as

$$\begin{aligned}\widehat{\mathbf{z}}_a(t) &= \mathbf{P}^T\mathbf{h}_e(\mathbf{v}(t))\mathbf{s}^H\mathbf{s}(\mathbf{s}^H\mathbf{s})^{-1} + \mathbf{P}^T\mathbf{n}_a(t)\mathbf{s}(\mathbf{s}^H\mathbf{s})^{-1}\\ &= \mathbf{P}^T(\bar{\mathbf{v}}^T(t)\otimes\mathbf{I}_N)\mathbf{h}_r + \frac{1}{P_b}\mathbf{P}^T\mathbf{n}_a(t)\mathbf{s}\\ &= (\bar{\mathbf{v}}^T(t)\otimes\mathbf{P}^T)\mathbf{h}_r + \frac{1}{\sqrt{P_b}}\widehat{\mathbf{n}}_a(t),\end{aligned} \tag{16}$$

where $\widehat{\mathbf{n}}_a(t) = \mathbf{P}^T\mathbf{n}_a(t)\widetilde{\mathbf{s}}$ and P_b is UE's transmit power. $\widetilde{\mathbf{s}} = \frac{1}{\sqrt{P_b}}\mathbf{s}$ is the normalized uplink packet which has unit transmit power, i.e., $\mathbb{E}\{\widetilde{\mathbf{s}}\widetilde{\mathbf{s}}^H\} = \mathbf{I}$. Since the $\mathbf{P}$ is unitary, $\widehat{\mathbf{n}}_a(t)$ has covariance matrix, $\sigma_a^2\mathbf{I}_N$.

We define $\bar{\mathbf{\Phi}} = [\bar{\mathbf{v}}(1),\ldots,\bar{\mathbf{v}}(V)] \in \mathbb{C}^{(M+1)\times V}$ as the phase shift matrix to model the configuration of the phase shift vector over V packets. After collecting the V measurements in (16) and stacking them into a vector, the BS obtains the measurement of the cascaded channel, which is given by

$$\begin{aligned}\mathbf{z}_a &= \left[\widehat{\mathbf{z}}_a^T(1),\ldots,\widehat{\mathbf{z}}_a^T(V)\right]^T\\ &= (\bar{\mathbf{\Phi}}^T\otimes\mathbf{P}^T)\mathbf{h}_r + \frac{1}{\sqrt{P_b}}\boldsymbol{\eta}_a,\end{aligned} \tag{17}$$

where $\mathbf{z}_a \in \mathbb{C}^{VN\times 1}$, and $\boldsymbol{\eta}_a = [\widehat{\mathbf{n}}_a^T(1),\ldots,\widehat{\mathbf{n}}_a^T(V)]^T$ with covariance matrix, $\sigma_a^2\mathbf{I}_{VN}$. The cascaded channel consists of D subchannels. Therefore, $NV \geq D$ should be satisfied to meet the requirement of the channel dimension. With $D = N(M+1)$, we have $V \geq (M+1)$.

2) Downlink Channel Probing: In the t-th downlink packet, the BS applies $\mathbf{P}$ to send a downlink packet, $\mathbf{P}\mathbf{S}_d^H$, to the UE. With the assumption of equal power allocation, we have $\mathbf{S}_d^H\mathbf{S}_d = NP_a\mathbf{I}_N$, where P_a is BS's transmit power. The RIS configures $\mathbf{v}(t)$ to reflect the downlink packet and then the UE (Bob) gets the received signal as

$$\mathbf{y}_b(t) = \mathbf{h}_e^T(\mathbf{v}(t))\mathbf{P}\mathbf{S}_d^H + \mathbf{n}_b(t), \tag{18}$$

where $\mathbf{y}_b(t) \in \mathbb{C}^{1\times N}$ and $\mathbf{n}_b(t) \in \mathbb{C}^{1\times N}$ is the noise vector.

By the LS estimation, the UE measures the equivalent channel as

$$\widehat{\mathbf{z}}_b(t) = \mathbf{y}_b(t)\mathbf{S}_d(\mathbf{S}_d^H\mathbf{S}_d)^{-1}, \tag{19}$$

where $\widehat{\mathbf{z}}_b(t) \in \mathbb{C}^{1\times N}$.

Based on (10), the measurement can be expanded as

$$\begin{aligned}\widehat{\mathbf{z}}_b(t) &= \mathbf{h}_e^T(\mathbf{v}(t))\mathbf{P} + \mathbf{n}_b(t)\mathbf{S}_d(\mathbf{S}_d^H\mathbf{S}_d)^{-1}\\ &= \mathbf{h}_r^T(\bar{\mathbf{v}}(t)\otimes\mathbf{I}_N)\mathbf{P} + \mathbf{n}_b(t)\mathbf{S}_d(\mathbf{S}_d^H\mathbf{S}_d)^{-1}\\ &= \mathbf{h}_r^T(\bar{\mathbf{v}}(t)\otimes\mathbf{P}) + \frac{1}{\sqrt{NP_a}}\widehat{\mathbf{n}}_b(t),\end{aligned} \tag{20}$$

where $\widehat{\mathbf{n}}_b(t) \in \mathbb{C}^{1\times N}$, $\widehat{\mathbf{n}}_b(t) = \mathbf{n}_b(t)\widetilde{\mathbf{S}}_d$ and $\widetilde{\mathbf{S}}_d$ is the normalization of $\mathbf{S}_d$ with $\widetilde{\mathbf{S}}_d = \frac{1}{\sqrt{NP_a}}\mathbf{S}_d$.

The UE computes the transpose of the above equation and replaces $\widehat{\mathbf{z}}_b(t)$ with $\widehat{\mathbf{z}}_b^T(t)$, which is given by

$$\bar{\mathbf{z}}_b(t) = \widehat{\mathbf{z}}_b^T(t) = (\bar{\mathbf{v}}^T(t)\otimes\mathbf{P}^T)\mathbf{h}_r + \widehat{\mathbf{n}}_b^T(t). \tag{21}$$

After collecting V measurements in (21) and stacking them into a vector, the UE obtains

$$\begin{aligned}\mathbf{z}_b &= \left[\bar{\mathbf{z}}_b(1)^T,\ldots,\bar{\mathbf{z}}_b^T(V)\right]^T\\ &= (\bar{\mathbf{\Phi}}^T\otimes\mathbf{P}^T)\mathbf{h}_r + \frac{1}{\sqrt{NP_a}}\boldsymbol{\eta}_b,\end{aligned} \tag{22}$$

where $\mathbf{z}_b \in \mathbb{C}^{VN\times 1}$ and $\boldsymbol{\eta}_b = [\mathbf{n}_b^T(1),\ldots,\mathbf{n}_b^T(V)]^T$ with $\mathbb{E}\{\boldsymbol{\eta}_b\boldsymbol{\eta}_b^H\} = \sigma_b^2\mathbf{I}_{VN}$.

B. Key Rate

After channel probing, the BS and UE distil secret keys from their measurements, $\mathbf{z}_a$, and $\mathbf{z}_b$, respectively. We assume eavesdroppers are more than half-wavelength away from the legitimate terminals, which means Eve's measurements are independent of BS's or UE's measurements. Therefore, the key rate is $I(\mathbf{z}_a;\mathbf{z}_b)$, i.e., the mutual information of the measurements.

In order to calculate the $I(\mathbf{z}_a;\mathbf{z}_b)$, we construct the covariance matrix of the measurements, $\mathbf{z}_a$ and $\mathbf{z}_b$. Let $\mathbf{R}_{\mathbf{z}_a} =$

$\mathbb{E}\{\mathbf{z}_a\mathbf{z}_a^H\}$ and $\mathbf{R}_{\mathbf{z}_b} = \mathbb{E}\{\mathbf{z}_b\mathbf{z}_b^H\}$ denote the covariance matrices of BS's and UE's measurements, respectively. Let $\mathbf{R}_{\mathbf{z}_a\mathbf{z}_b} = \mathbb{E}\{\mathbf{z}_a\mathbf{z}_b^H\}$ denote the cross-covariance matrix of $\mathbf{z}_a$ and $\mathbf{z}_b$. According to (17) and (22), $\mathbf{R}_{\mathbf{z}_a}$, $\mathbf{R}_{\mathbf{z}_b}$ and $\mathbf{R}_{\mathbf{z}_a\mathbf{z}_b}$ can be expressed as

$$\mathbf{R}_{\mathbf{z}_a} = (\bar{\mathbf{\Phi}} \otimes \mathbf{P})^T \mathbf{R}_h (\bar{\mathbf{\Phi}} \otimes \mathbf{P})^* + \frac{\sigma_a^2}{P_b}\mathbf{I}_D, \tag{23}$$

$$\mathbf{R}_{\mathbf{z}_b} = (\bar{\mathbf{\Phi}} \otimes \mathbf{P})^T \mathbf{R}_h (\bar{\mathbf{\Phi}} \otimes \mathbf{P})^* + \frac{\sigma_b^2}{NP_a}\mathbf{I}_D, \tag{24}$$

$$\mathbf{R}_{\mathbf{z}_a\mathbf{z}_b} = \mathbf{R}_{\mathbf{z}_b\mathbf{z}_a} = (\bar{\mathbf{\Phi}} \otimes \mathbf{P})^T \mathbf{R}_h (\bar{\mathbf{\Phi}} \otimes \mathbf{P})^*. \tag{25}$$

The full covariance matrix of both measurements is

$$\mathbf{K}_{\mathbf{z}_a\mathbf{z}_b} = \mathbb{E}\left\{ \begin{bmatrix} \widehat{\mathbf{z}}_a \\ \widehat{\mathbf{z}}_b \end{bmatrix} [\widehat{\mathbf{z}}_a^H, \widehat{\mathbf{z}}_b^H] \right\} = \begin{bmatrix} \mathbf{R}_{\mathbf{z}_a} & \mathbf{R}_{\mathbf{z}_a\mathbf{z}_b} \\ \mathbf{R}_{\mathbf{z}_b\mathbf{z}_a} & \mathbf{R}_{\mathbf{z}_b} \end{bmatrix}. \tag{26}$$

The key rate is given by

$$\begin{aligned} I(\mathbf{z}_a;\mathbf{z}_b) &= \mathbb{H}(\mathbf{z}_a) + \mathbb{H}(\mathbf{z}_b) - \mathbb{H}(\mathbf{z}_a,\mathbf{z}_b) \\ &= \log_2\left(\frac{|\mathbf{R}_{\mathbf{z}_a}||\mathbf{R}_{\mathbf{z}_b}|}{|\mathbf{K}_{\mathbf{z}_a\mathbf{z}_b}|}\right) \\ &\overset{(a)}{=} \log_2\Big(\frac{|\mathbf{R}_{\mathbf{z}_b}|}{|\mathbf{R}_{\mathbf{z}_b} - \mathbf{R}_{\mathbf{z}_b\mathbf{z}_a}\mathbf{R}_{\mathbf{z}_a}^{-1}\mathbf{R}_{\mathbf{z}_a\mathbf{z}_b}|}\Big), \end{aligned} \tag{27}$$

where (a) holds due to the determinant of the block matrix. Substituting (23)-(26) into the above equation, we have

$$\begin{aligned} I(\mathbf{z}_a;\mathbf{z}_b) &= \log_2\left(\frac{|\mathbf{R}_W + \mathbf{\Gamma}_b|}{|\mathbf{R}_W + \mathbf{\Gamma}_b - \mathbf{R}_W(\mathbf{R}_W + \mathbf{\Gamma}_a)^{-1}\mathbf{R}_W|}\right) \\ &= -\log_2\left(|\mathbf{I} - \mathbf{R}_W(\mathbf{R}_W + \mathbf{\Gamma}_a)^{-1}\mathbf{R}_W(\mathbf{R}_W + \mathbf{\Gamma}_b)^{-1}|\right), \end{aligned} \tag{28}$$

where $\mathbf{R}_W = (\bar{\mathbf{\Phi}}\otimes\mathbf{P})^T\mathbf{R}_h(\bar{\mathbf{\Phi}}\otimes\mathbf{P})^*$ is the channel covariance matrix and $\mathbf{\Gamma}_a = \frac{\sigma_a^2}{P_b}$ and $\mathbf{\Gamma}_b = \frac{\sigma_b^2}{NP_a}$ are the noise covariance matrix of the BS and the UE, respectively.

IV. Key Rate Optimization

The objective is to jointly design the phase shift matrix, $\bar{\mathbf{\Phi}}$, and the precoding matrix, $\mathbf{P}$, to maximize the key rate when the BS has the information of the channel spatial covariance matrix. We formulate the following optimization problem:

$$\begin{aligned} \text{(P1)}\ \max_{\bar{\mathbf{\Phi}},\mathbf{P}}\ & I(\mathbf{z}_a;\mathbf{z}_b) \\ s.t.\ & |\phi_{m,t}| = 1, && (29)\\ & \bar{\phi}_{m,t} \in \mathcal{K},\ 2 \le m \le M+1, 1 \le t \le V, && (30)\\ & \bar{\phi}_{1,t} = 1,\ 1 \le t \le V, && (31)\\ & \text{rank}(\bar{\mathbf{\Phi}}) = M+1, && (32)\\ & \mathbf{P}^H\mathbf{P} = \mathbf{I}_N. && (33) \end{aligned}$$

The phase shift and precoding matrices, $\bar{\mathbf{\Phi}}$ and $\mathbf{P}$, should meet the following five constraints.

- The RIS is passive and each reflection coefficient cannot modify the amplitude but the phase shift. The RIS should meet the unit-module constraint of $|\phi_{m,t}| = 1$.
- The m-th row and the t-th column entry of the $\bar{\mathbf{\Phi}}$ should meet $\bar{\phi}_{m,t} \in \mathcal{K}$, $2 \le m \le (M+1)$, $1 \le t \le V$, which means that the RIS can select the reflection coefficient of the m-th element from $\mathcal{K}$ in the t-th packet.
- The first row of the phase shift matrix, $\bar{\mathbf{\Phi}}$, represents the phase shift that the RIS configured for the direct channel. However, the direct channel which does not pass through the RIS is uncontrollable, so the first row of $\bar{\mathbf{\Phi}}$ should meet $\bar{\phi}_{1,t} = 1,\ 1 \le t \le V$.
- The equation $\text{rank}(\bar{\mathbf{\Phi}}) = M+1$ should satisfy to ensure the BS and UE can measure the cascaded channel.
- With the assumption of equal power allocation, the precoding matrix should meet the constraint of $\mathbf{P}^H\mathbf{P} = \mathbf{I}_N$.

Note that (P1) is difficult to solve because the constraints of (29) and (32) are non-convex and the Kronecker product structure in the objective function. Therefore, we transform the $\bar{\mathbf{\Phi}} \otimes \mathbf{P}$ into an equivalent matrix variable, $\mathbf{W} \in \mathbb{C}^{D\times(N_sV)}$, and relax some constraints to formulate an approximate optimization problem. We design an algorithm to find the optimal solution, $\mathbf{W}^\dagger$, of the approximate optimization problem, as presented in Section IV-A. $\mathbf{W}^\dagger$ reaches the upper bound of (P1) but it cannot be applied in practice. Therefore, we will design an algorithm to divide $\mathbf{W}^\dagger$ into $\bar{\mathbf{\Phi}}$ and $\mathbf{P}$, which is done in Section IV-B.

A. Upper Bound of Key Rate

The rank constraint of the phase shift matrix and the unit-modulus constraint of the reflection coefficient are non-convex. Therefore, we relax the constraints and transform (P1) into (P2) to find the upper bound of the problem (P1). The (P1) can be reformulated as

$$\begin{aligned} \text{(P2)}\ \max_{\mathbf{W}}\ & I(\mathbf{z}_a;\mathbf{z}_b) \\ s.t.\ & \|\mathbf{W}\|_F^2 = (M+1)^2N. \end{aligned} \tag{34}$$

Next, we will discuss how to find the optimal $\mathbf{W}$. Firstly, to simplify the objection function of (P2), we transform the matrix variable, $\mathbf{W}$, into a set of scalar variables, p_i, $i = 1,\ldots,D$. Secondly, we analyze the concavity of the objective function in terms of p_i. Finally, we derive the KKT condition of the optimization problem based on the concavity and design an algorithm to find the optimal p_i, which allows us to find the optimal $\mathbf{W}$.

1) Converting $\mathbf{W}$ to Scalar Variables p_i: Define $\mathbf{R}_W = \mathbf{W}^T\mathbf{R}_h\mathbf{W}^*$. We do the Cholesky factorization of the spatial correlation matrix, $\mathbf{R}_h$, as $\mathbf{R}_h = \mathbf{R}_h^{1/2}(\mathbf{R}_h^{1/2})^H$, where $\mathbf{R}_h^{1/2} = \mathbf{U}_h\mathbf{\Lambda}_h^{1/2}$, $(\mathbf{R}_h^{1/2})^H = \mathbf{\Lambda}_h^{1/2}\mathbf{U}_h^H$ and $\mathbf{R}_W = \mathbf{W}^T\mathbf{R}_h^{1/2}(\mathbf{R}_h^{1/2})^H\mathbf{W}^* = ((\mathbf{R}_h^{1/2})^H\mathbf{W}^*)^H((\mathbf{R}_h^{1/2})^H\mathbf{W}^*)$. To simplify the objective function of (P2), we resort to the following singular value decomposition (SVD).

$$(\mathbf{R}_h^{1/2})^H\mathbf{W}^* = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^H, \tag{35}$$

$$\mathbf{W} = (\mathbf{R}_h^{-H/2}\mathbf{U}\mathbf{\Lambda}\mathbf{V}^H)^* = (\mathbf{U}_h\mathbf{\Lambda}_h^{-1/2}\mathbf{U}\mathbf{\Lambda}\mathbf{V}^H)^*, \tag{36}$$

$$\mathbf{R}_W = \mathbf{V}\mathbf{\Lambda}^H\mathbf{\Lambda}\mathbf{V}^H, \tag{37}$$

where $\mathbf{U} \in \mathbb{C}^{D\times D}$, $\mathbf{\Lambda} \in \mathbb{C}^{D\times N_sV}$ and $\mathbf{V} \in \mathbb{C}^{N_sV\times N_sV}$ are the new matrices to be optimized. Specially, $\mathbf{\Lambda} = [\text{diag}\{\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{N_sV}}\}; \mathbf{0}_{(D-N_sV)\times N_sV}]$, where the non-zero values are in descending order. According to (35)-(37), the objective function of (P2) can be simplified as

$$\begin{aligned} I(\mathbf{z}_a;\mathbf{z}_b) = -\log_2\big(&|\mathbf{I} - \mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H(\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H + \mathbf{\Gamma}_a)^{-1} \\ &\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H(\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H + \mathbf{\Gamma}_b)^{-1}|\big), \end{aligned} \tag{38}$$

where $\mathbf{\Lambda}^2 = \mathbf{\Lambda}\mathbf{\Lambda}^T$.

Applying the Woodbury matrix inversion lemma, we further simplify (38) as a function of $\mathbf{\Lambda}$ which is present at the top of the next page. (a) holds due to $\mathbf{P}(\mathbf{I}+\mathbf{P})^{-1} = \mathbf{I} - (\mathbf{I}+\mathbf{P})^{-1}$. (b) holds because the determinant of a unitary matrix equals 1, i.e. $|\mathbf{V}| = 1$.

Since $\mathbf{I}$ and $\mathbf{\Lambda}^2$ are diagonal matrices, the component $\mathbf{I} + \hat{\sigma}_a^{-2}\mathbf{\Lambda}^2$ in (39) equals a new diagonal matrix that the (n,n)-th diagonal entry is $1 + \hat{\sigma}_a^{-2}p_n$. The determinant of the diagonal matrix $\mathbf{I} + \hat{\sigma}_a^{-2}\mathbf{\Lambda}^2$ is the product of the diagonal entry, i.e., $|\mathbf{I} + \hat{\sigma}_a^{-2}\mathbf{\Lambda}^2| = (1 + \hat{\sigma}_a^{-2}p_1)\dots(1 + \hat{\sigma}_a^{-2}p_D)$. Similarly, we can calculate $|\mathbf{I} + \hat{\sigma}_b^{-2}\mathbf{\Lambda}^2|$ as $(1 + \hat{\sigma}_b^{-2}p_1)\dots(1 + \hat{\sigma}_b^{-2}p_D)$. Also, we can calculate $|\mathbf{I} + \hat{\sigma}_a^{-2}\mathbf{\Lambda}^2 + \hat{\sigma}_b^{-2}\mathbf{\Lambda}^2)|$ as $(1 + (\hat{\sigma}_a^{-2} + \hat{\sigma}_b^{-2})p_1)\dots(1 + (\hat{\sigma}_a^{-2} + \hat{\sigma}_b^{-2})p_D)$. Therefore, Eq. (39) can be simplified as

$$\begin{aligned} I(\mathbf{z}_a;\mathbf{z}_b) &= \sum_{i=1}^{D} \log_2\left(\frac{(1+\hat{\sigma}_a^{-2}p_i)(1+\hat{\sigma}_b^{-2}p_i)}{(\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i + 1}\right) \\ &= \sum_{i=1}^{D} \log_2\left(1 + \frac{\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}p_i^2}{(\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i + 1}\right), \end{aligned} \tag{40}$$

where $\hat{\sigma}_a^2 = \frac{\sigma_a^2}{P_b}$, $\hat{\sigma}_b^2 = \frac{\sigma_b^2}{NP_a}$.

We substitute the (36) into the constraint of (P2) and get

$$\begin{aligned} \|\mathbf{W}\|_F^2 &= \mathrm{Tr}(\mathbf{W}\mathbf{W}^H) \\ &= \mathrm{Tr}\left((\mathbf{U}_h\mathbf{\Lambda}_h^{-H/2}\mathbf{U}\mathbf{\Lambda}\mathbf{V}^H)^*(\mathbf{U}_h\mathbf{\Lambda}_h^{-H/2}\mathbf{U}\mathbf{\Lambda}\mathbf{V}^H)^T\right) \\ &= \mathrm{Tr}(\mathbf{\Lambda}_h^{-1}\mathbf{U}^*\mathbf{\Lambda}\mathbf{\Lambda}^T\mathbf{U}^T) \overset{(a)}{=} \mathrm{Tr}(\mathbf{\Lambda}_h^{-1}\mathbf{\Lambda}^2) \\ &= (M+1)^2N, \end{aligned} \tag{41}$$

where $\mathbf{\Lambda}_h^{-1} = \mathbf{\Lambda}_h^{-T/2}\mathbf{\Lambda}_h^{-1/2}$ and (a) holds when $\mathbf{U} = \mathbf{I}_D$. Therefore, the constraint of (P2) is simplified as

$$\sum_{i=1}^{D} \frac{p_i}{p_{h,i}} = (M+1)^2N. \tag{42}$$

2) Design p_i: After transforming $\mathbf{W}$ into p_i, the problem (P2) can be converted into (P3), which is given by

$$\begin{aligned} \text{(P3)} \ \max_{p_i} \ & \sum_{i=1}^{D} \log_2\left(1 + \frac{\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}p_i^2}{(\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i + 1}\right) \\ & s.t. \ \sum_{i=1}^{D} \frac{p_i}{p_{h,i}} = (M+1)^2N. \end{aligned} \tag{43}$$

We resort to finding the optimal value of the key rate by the Lagrangian multiplier solution. According to [39], the solution to a concave function over a convex solution set can be guaranteed to be a global maximum. Therefore, we first discuss the concavity of the objective function of (P3). We derive the first-order and second-order partial derivative of $I(\mathbf{z}_a;\mathbf{z}_b)$, which is shown at the top of the next page.

The first-order partial derivative of $I(\mathbf{z}_a;\mathbf{z}_b)$ is greater than zero, which means the decomposed D functions is monotonically increasing. If the objective function is concave, the Hessian matrix should be semi-negative definite. Because $\frac{\partial^2 I(\mathbf{z}_a;\mathbf{z}_b)}{\partial p_i \partial p_j} = 0$, the objective is concave if $\frac{\partial^2 I(\mathbf{z}_a;\mathbf{z}_b)}{\partial p_i^2} \leq 0$. The second-order partial derivative function is greater than zero at the interval of $[0, p_{co}]$ and less than zero at the interval of $[p_{co}, +\infty]$, where p_{co} is the solution of $\frac{\partial^2 I(\mathbf{z}_a;\mathbf{z}_b)}{\partial p_i^2} = 0$. That is, each decomposed function is convex at the interval of $[0, p_{co}]$ and concave at the interval of $[p_{co}, +\infty]$. Therefore, we will find the global maximum if we constrain the power in the concave interval. From the above analysis, we find there are two challenges in solving the problem (P3). The first is to find the active set with non-zero power. The second is to consider the convex interval of each decomposed function. In order to simplify (P3), we will derive the Karush-Kuhn-Tucker (KKT) conditions of the (P3). According to the KKT conditions, we further propose a water-filling algorithm to find the optimal p_i, $i = 1, \dots, D$.

3) Water Filling Algorithm: We first derive the KKT condition of the problem, and then we find the threshold of each decomposed function. If the power allocated to the i-th subchannel is greater than the threshold $\gamma_i = p_{h,i}p_{co}$, $i = 1, \dots, D$, the subchannel is activated with non-zero power. Finally, we propose a water-filling algorithm to solve the problem with lower-bound constraints.

The Lagrangian function with respect to p_i is given by

$$f = I(\mathbf{z}_a;\mathbf{z}_b) - \mu\left(\sum_{i=1}^{D} \frac{p_i}{p_{h,i}} - (M+1)^2N\right), \tag{46}$$

where $\mu \geq 0$ is the water-filling level. The corresponding KKT conditions are

$$\begin{cases} y_i(p_i) = p_{h,i}\dfrac{\partial f}{\partial p_i} = p_{h,i}\dfrac{\partial I(\mathbf{z}_a;\mathbf{z}_b)}{\partial p_i} = \mu, \\ \mu\left(\displaystyle\sum_i \frac{p_i}{p_{h,i}} - (M+1)^2N\right) = 0, \\ \displaystyle\sum_i \frac{p_i}{p_{h,i}} \leq (M+1)^2N, \end{cases} \tag{47}$$

where $y_i(p_i)$ is the increasing rate of the power allocated to the i-th subchannel.

Next, we transform the KKT condition into the water-filling algorithm and find the solution. According to [40], we define $\mathcal{M}_{inactive} = \{i | p_i \leq \gamma_i, i = 1, \dots, D\}$ as the set of inactive cascaded channels, i.e. the allocated power is lower than the threshold. Also, define $\mathbb{I}_i$ as the indicator function. If $p_i \in \mathcal{M}_{inactive}$, $\mathbb{I}_i = 0$, otherwise $\mathbb{I}_i = 1$. Define $g_i(\mu)$ as the inverse function of $y_i(p_i)$. Therefore, the KKT condition (47) can be transformed into the following conditions.

$$\begin{cases} p_i = g_i(\mu)\mathbb{I}_i + \gamma_i(1 - \mathbb{I}_i), \\ \displaystyle\sum_{i=1}^{D} g_i(\mu)\mathbb{I}_i + \gamma_i(1 - \mathbb{I}_i) = P, \end{cases} \tag{48}$$

where $P = (M+1)^2N$.

We use the water-filling algorithm to solve the problem (48), which is shown in Algorithm 1. In line 1, we initialize $\mathbb{I}_i = 1$ for $i = 1, \dots, D$, which means all subchannels are active in the initial phase. Specially, the m-th subchannel is the m-th element of $\mathbf{h}_r$. In line 2, according to the KKT conditions in (48), we calculate the initial p_i and the water level, μ. In line 4, we find the set of $\mathcal{M}_{inactive}$. In line 5, we set $\mathbb{I}_i = 0$ for $i \in \mathcal{M}_{inactive}$, which is the process to find the inactive

$$
\begin{aligned}
I(\mathbf{z}_a;\mathbf{z}_b) &= -\log_2\left(|\mathbf{I}-\hat{\sigma}_a^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H(\hat{\sigma}_a^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H+\mathbf{I})^{-1}\times\hat{\sigma}_b^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H(\hat{\sigma}_b^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H+\mathbf{I})^{-1}|\right)\\
&\overset{(a)}{=} -\log_2\left(|\mathbf{I}-(\mathbf{I}-(\mathbf{I}+\hat{\sigma}_a^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H)^{-1})\times(\mathbf{I}-(\mathbf{I}+\hat{\sigma}_b^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H)^{-1})|\right)\\
&= -\log_2(|(\mathbf{I}+\hat{\sigma}_a^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H)^{-1}+(\mathbf{I}+\hat{\sigma}_b^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H)^{-1}-(\mathbf{I}+\hat{\sigma}_a^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H)^{-1}(\mathbf{I}+\hat{\sigma}_b^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H)^{-1}|)\\
&= -\log_2(|(\mathbf{I}+\hat{\sigma}_a^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H)^{-1}(\mathbf{I}+\hat{\sigma}_b^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H))^{-1}\times(\mathbf{I}+\hat{\sigma}_a^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H+\hat{\sigma}_b^{-2}\mathbf{V}\mathbf{\Lambda}^2\mathbf{V}^H)|)\\
&\overset{(b)}{=} \log_2\left(|\mathbf{I}+\hat{\sigma}_a^{-2}\mathbf{\Lambda}^2|\right)+\log_2\left(|\mathbf{I}+\hat{\sigma}_b^{-2}\mathbf{\Lambda}^2|\right)-\log_2(|\mathbf{I}+\hat{\sigma}_a^{-2}\mathbf{\Lambda}^2+\hat{\sigma}_b^{-2}\mathbf{\Lambda}^2)|\big).
\end{aligned}
\tag{39}
$$

$$
\frac{\partial I(\mathbf{z}_a;\mathbf{z}_b)}{\partial p_i}=\frac{\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}(\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i^2+2\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}p_i}{\ln 2\left(\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}p_i^2+(\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i+1\right)\left((\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i+1\right)},
\tag{44}
$$

$$
\begin{aligned}
\frac{\partial^2 I(\mathbf{z}_a;\mathbf{z}_b)}{\partial p_i^2}=&\frac{2\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}}{\ln 2\left(\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}p_i^2+(\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i+1\right)}-\frac{2(\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})\times\left(\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}(\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i^2+2\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}p_i\right)}{\ln 2\left(\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}p_i^2+(\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i+1\right)\left((\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i+1\right)^2}\\
&-\frac{(\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}(\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i^2+2\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}p_i)^2}{\ln 2(\hat{\sigma}_a^{-2}\hat{\sigma}_b^{-2}p_i^2+(\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i+1)^2((\hat{\sigma}_a^{-2}+\hat{\sigma}_b^{-2})p_i+1)^2}.
\end{aligned}
\tag{45}
$$

Algorithm 1 Water-Filling Algorithm

Input: $\{p_{h,i}\}$, P, μ_{max}, μ_{min}, $\hat{\sigma}_a$, $\hat{\sigma}_b$, ϵ_1, ϵ_2, γ_i;
Output: $\{p_i\}$, $\{\mathbb{I}_i\}$.
1: Initialize $\mathbb{I}_i=1$ for $i=1,\ldots,D$;
2: Calculate $\{p_i\}$ and μ through Algorithm 2;
3: **repeat**
4: Set $\mathcal{M}_{inactive}=\{i|p_i\le\gamma_i, i=1,\ldots,D\}$;
5: Substitute $\mathbb{I}_i=0$ for $i\in\mathcal{M}_{inactive}$;
6: Calculate $\{p_i\}$ and μ through Algorithm 2;
7: **until** length(find $(p_i<\gamma_i)=0$).

Algorithm 2 Two-dimensional Bisection Algorithm

Input: $\{p_{h,i}\}$, P, μ_{max}, μ_{min}, $\hat{\sigma}_a$, $\hat{\sigma}_b$, ϵ_1, ϵ_2;
Output: $\{p_i\}$, μ.
1: Set $\mu=(\mu_{min}+\mu_{max})/2$;
2: **for** $i=1,\ldots,D$ **do**
3: **if** $\mathbb{I}_i=1$ **then**
4: Do bisection search of p_i to satisfy $|y_i-\mu|\le\epsilon_1$;
5: **else**
6: $p_i=\gamma_i$;
7: **end if**
8: **end for**
9: **repeat**
10: **for** $i=1,\ldots,D$ **do**
11: **if** $\sum\frac{p_i}{p_{h,i}}<P$ **then**
12: $\mu_{max}=(\mu_{min}+\mu_{max})/2$;
13: **else**
14: $\mu_{min}=(\mu_{min}+\mu_{max})/2$;
15: **end if**
16: Set $\mu=(\mu_{min}+\mu_{max})/2$;
17: **if** $\mathbb{I}_i=1$ **then**
18: Do bisection search of p_i to satisfy $|y_i-\mu|\le\epsilon_1$;
19: **else**
20: $p_i=\gamma_i$;
21: **end if**
22: **end for**
23: **until** $|\sum\frac{p_i}{p_{h,i}}-P|\le\epsilon_2$.

subchannels and allocate power γ_i to them. In line 6, according to $\mathbb{I}_i$, we calculate the p_i and μ. We repeat the steps from lines 4 to 6 until all $p_i\ge\gamma_i$. When the algorithm ends, the channels belonging to the active subchannel set are allocated with the optimal power, while those belonging to the inactive subchannel set are allocated with power γ_i.

In Algorithm 1, we should calculate p_i and μ in each loop. The p_i is derived from (48), where $g_i(\mu)$ is the core parameter. However, it is hard to find the closed-form expression of $g_i(\mu)$. Therefore, we introduce a two-dimensional bisection search to calculate p_i and $g_i(\mu)$, as shown in Algorithm 2. In line 1, we set the initial μ as $\mu=(\mu_{min}+\mu_{max})/2$. From lines 2 to 8, for all subchannels, if $\mathbb{I}_i=1$, we apply the bisection search to find the initial p_i to meet the requirement of $|y_i-\mu|\le\epsilon_1$; If $\mathbb{I}_i=0$, we set $p_i=\gamma_i$. From line 10 to 22, we search the p_i and μ, and repeat it until $|\sum\frac{p_i}{p_{h,i}}-P|\le\epsilon_2$. When Algorithm 2 ends, we get the final p_i and μ, which will be returned to Algorithm 1.

According to Algorithms 1 and 2, we obtain the optimal p_i, $i=1,\ldots,D$. Substituting p_i into (36), we find the optimal solution, $\mathbf{W}^\dagger$, of the problem (P1). In the next section, based on $\mathbf{W}^\dagger$, we will design an algorithm to find the optimal precoding and phase shift matrices.

B. Precoding and Phase Shift Matrices Design

In order to obtain the phase shift matrix, $\bar{\mathbf{\Phi}}_i$, and the precoding matrix, $\mathbf{P}$, we try to decompose the $\mathbf{W}^\dagger$ to $\bar{\mathbf{\Phi}}\otimes\mathbf{P}$. However, in most cases, the upper bound is not approachable because $\mathbf{W}^\dagger$ cannot be decomposed into a Kronecker product of a matrix with unit-magnitude entries and an F-norm-

constrained complex matrix. Therefore, we obtain $\bar{\mathbf{\Phi}}$ and $\mathbf{P}$ by solving the following optimization problem.

$$\begin{aligned} \text{(P4)} \ & \min_{\bar{\mathbf{\Phi}},\mathbf{P}} \|\bar{\mathbf{\Phi}} \otimes \mathbf{P} - \mathbf{W}^{\dagger}\|_F^2 \\ & \text{s.t. } (29) - (33). \end{aligned} \tag{49}$$

Next, we propose an algorithm to design the precoding and phase shift matrices. The special structure of the constraints inspires us to find a fast way to design the phase-shift matrix. According to [34], [41], the Hadamard reflection pattern for the RIS systems satisfies the requirements of the full rank and unit norm. The Hadamard matrix is full rank so that the phase shift matrix $\bar{\mathbf{\Phi}}$ is reversible to recover the subchannels associated with elements. What's more, the entries of the Hardmard matrix are -1 and 1, where the -1 and 1 denote phase shift is configured as 180° and 0°, respectively. The entries of the first row of the Hadamard matrix are 1 which means the phase shift vector can not configure for the direct channel. In channel probing, the BS configures the $\bar{\mathbf{v}}(t)$ for the t-th uplink and t-th downlink packets according to the corresponding column of the phase shift matrix, i.e., $\bar{\mathbf{v}}(t) = \bar{\mathbf{\Phi}}(:, t)$.

Given $\bar{\mathbf{\Phi}}$, we design the precoding matrix

$$\begin{aligned} \text{(P5)} \ & \mathbf{P}^{\dagger} = \arg\min_{\mathbf{P}} \|\bar{\mathbf{\Phi}} \otimes \mathbf{P} - \mathbf{W}^{\dagger}\|_F^2 \\ & \text{s.t. } \mathbf{P}^H\mathbf{P} = \mathbf{I}_N. \end{aligned} \tag{50}$$

Given the phase shift matrix, we propose an algorithm to design the precoding matrix. To address the Kronecker product, the objective function of (P5) can be transformed as $\sum_{m=1}^{M+1}\sum_{t=1}^{V} \|\mathbf{W}_{m,t} - \phi_{m,t}\mathbf{P}\|_F^2$, where $\mathbf{W}_{m,t} \in \mathbb{C}^{N\times N_s}$ is an element of

$$\mathbf{W} = \begin{bmatrix} \mathbf{W}_{1,1} & \mathbf{W}_{1,2} & \cdots & \mathbf{W}_{1,V} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{W}_{M+1,1} & \mathbf{W}_{M+1,2} & \cdots & \mathbf{W}_{M+1,V} \end{bmatrix}. \tag{51}$$

The objective function of (P5) can be further expanded, which is shown at the top of the next page. Given $\bar{\mathbf{\Phi}}$, we design the precoding matrix by solving the following optimization problem.

$$\begin{aligned} \text{(P6)} \ & \min_{\mathbf{P}} \ \|\mathbf{P} - \sum_{m=1}^{M+1}\sum_{t=1}^{V} \frac{\phi_{m,t}^{*}\mathbf{W}_{m,t}}{(M+1)V}\|_F^2 \\ & \text{s.t. } \mathbf{P}^H\mathbf{P} = \mathbf{I}_N. \end{aligned} \tag{53}$$

Since the orthogonal constraint is non-convex, we resort to the Grassmann manifold toolbox to solve the above problem [42].

C. Update of the Channel Covariance Matrix

The proposed key rate optimization is updated according to the channel covariance matrix. We consider the wide-sense stationary (WSS) fading channel model. With WSS channel coefficients, the spatial information, e.g. the AoAs and AoDs, is unchanged over several coherence blocks and the channel gain varies from block to block [43] and [44]. The channel covariance matrix is calculated by $\mathbf{R}_h = \mathbb{E}\{\mathbf{h}_r\mathbf{h}_r^H\}$. The estimation method for the channel covariance matrix in practice can be found in [39] and [28]. Quist *et al.* design the optimal beamforming in traditional MIMO systems, where the channel covariance matrix is stationary [39]. Wallace *et al.* [28] maintained the second-order statistics in each segment stationary and obtain the channel measurements from each segment to calculate the channel covariance matrix for calculating the key rate in key generation. However, when the displacement of the transceiver to a location is distant from its original position to a certain extent in practice, the channel covariance matrix should be updated according to the spatial information, which can be found in [45].

V. Key Generation Protocol

A. Preprocessing

After the channel probing process in Section III, BS and UE acquire a series of measurements, i.e., $\mathbf{z}_a(t)$ and $\mathbf{z}_b(t)$, $t = 1, \ldots, T_d$, where T_d is the number of measurements. The LoS component of the Rician fading is not suitable for a key generation system because the LoS component is determined by the distance between BS and UE [2]. To address the issue, we need to wipe off the LoS component in the measurements and extract the NLoS components. We subtract the mean of the measurements and get $\mathbf{z}_u(t) = \mathbf{z}_u(t) - \frac{1}{T_d}\sum_{t=1}^{T_d}\mathbf{z}_u(t)$, $u \in \{a, b\}$. Furthermore, the difference between the path-loss effect of measurements from $\mathbf{z}_u(t)$ should be mitigated [28], [46]. Since there is a big difference between the channel variances of direct and RIS-reflected channels, each subchannel of the cascaded channel should be normalized separately. We normalize the measurements of the m-th subchannel as $\widehat{\mathbf{z}}_{u,m}(t) = \mathbf{z}_{u,m}(t)(\frac{1}{T_d}\sum_{t=1}^{T_d}\|\mathbf{z}_u(t)\|_F^2)^{\frac{1}{2}}$. After normalization, the measurements of BS and UE has zero mean and unit variance.

B. Quantization

After preprocessing the measurements, BS and UE convert the analog channel measurements, $\widehat{\mathbf{z}}_u(t)$, to binary sequences. According to Algorithm 1 in [9], we apply a three-bit cumulative distribution function (CDF)-based quantization, $\mathcal{Q}(\cdot)$. Each user will carry out quantization independently, given by

$$\boldsymbol{K}_u = \mathcal{Q}(\widehat{\mathbf{z}}_u). \tag{54}$$

The quantization boundary of CDF quantization with quantization bits $q = 3$ is given by

$$\eta_i = \begin{cases} -\infty, & i = 0, \\ F_x^{-1}(\dfrac{i}{2^3}), & i = 1, \ldots, 2^3 - 1, \\ +\infty, & i = 2^3, \end{cases} \tag{55}$$

where $F_x(x)$ is the CDF function of the measurements. Since the noise causes disagreements between the bit sequences of BS and UE, we use the bit disagreement rate (BDR) to quantify the difference between the bit sequences of BS and UE after quantization [26]. We define the BDR as

$$\text{BDR} = \frac{\sum_{i=1}^{l_k}|\boldsymbol{K}_a(i) - \boldsymbol{K}_b(i)|}{l_k}, \tag{56}$$

where $\boldsymbol{K}_a(i)$ and $\boldsymbol{K}_b(i)$ are the bits generated from quantization and l_k is the key length. Key generation rate (KGR) is a

$$\begin{aligned}\|\bar{\mathbf{\Phi}}\otimes\mathbf{P}-\mathbf{W}^{\dagger}\|_F^2 &= \sum_{m=1}^{M+1}\sum_{t=1}^{V}\|\mathbf{W}_{m,t}-\phi_{m,t}\mathbf{P}\|_F^2 \\ &= (M+1)V\|\mathbf{P}-\sum_{m=1}^{M+1}\sum_{t=1}^{V}\frac{\phi_{m,t}^*\mathbf{W}_{m,t}}{(M+1)V}\|_F^2+\sum_{m=1}^{M+1}\sum_{t=1}^{V}\|\mathbf{W}_{m,t}\|_F^2-\frac{1}{(M+1)V}\|\sum_{m=1}^{M+1}\sum_{t=1}^{V}\phi_{m,t}^*\mathbf{W}_{m,t}\|_F^2 \\ &\geq (M+1)V\|\mathbf{P}-\sum_{m=1}^{M+1}\sum_{t=1}^{V}\frac{\phi_{m,t}^*\mathbf{W}_{m,t}}{(M+1)V}\|_F^2. \end{aligned} \tag{52}$$

metric to quantize the number of key bits after quantization. In this paper, the 3-th bit CDF-quantization method achieves 3 bit/measurement KGR. However, the increase in quantization bits leads to an increase in the BDR. Therefore, there is a trade-off between KGR and BDR. In order to reduce the BDR, the quantization bits should be chosen according to the SNR of the measurements of different subchannels [29], or the guardband-based quantization method can be applied [28]. The BS and UE can achieve a KGR that is close to the key rate through the implementation of an effectively designed protocol [2]. The comparison of different kinds of quantization methods can be found in [47].

C. Information reconciliation and privacy amplification

Due to noise, BS and UE should further remove the disagreements between their bit sequences by information reconciliation methods. Information reconciliation methods are divided into two categories, namely error detection protocol-based approaches (EDPA), e.g. Cascade, and error correction code-based approaches (ECCA), e.g., Low-Density Parity Check (LDPC)–based reconciliation [2]. A summary of different kinds of information reconciliation methods can be found in [48].

In the previous information reconciliation process, BS and UE should exchange partial information over a public channel so an eavesdropper can guess the secret keys from this information. For instance, if the LDPC-based reconciliation method is applied, a 3-bit syndrome is exchanged over the public channel and leaked to the eavesdropper so that the search space of secret keys is shrunk by divided by eight. Consequently, the eavesdropper can find the secret keys more quickly. BS and UE apply the privacy amplification methods to map these bit sequences to shorter and more secure secret keys. The common methods used in privacy amplification contain the leftover hash lemma, the cryptographic hash functions, and the Merkle-Damgard hash function [2].

VI. Numerical Results

In this section, numerical results are given to elaborate on the performance of our proposed RIS-assisted key generation scheme.

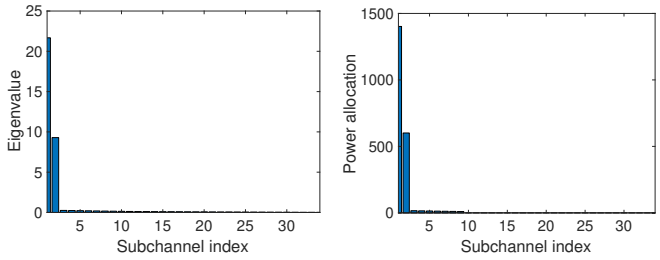
A. Setup

1) Device Configuration: The BS is located on the x-axis, $(39.4, 4.6, 5.2)$, with antenna spacing $d_a = \lambda/4$ and $\lambda = 0.1$ m. The RIS is parallel to the $y-z$ plane, where the first reflecting element is located at $(38.4, 4.8, 4.8)$. The side length of an element is normalized by the wavelength, i.e., $d_r = d_r/\lambda$. The UE is located at $(0, 0, 0)$. The transmit powers of the BS and UE are set identically as $P_t = P_a = P_b$ dBm. All noise powers are set as $\sigma^2 = \sigma_a^2 = \sigma_b^2 = -96$ dBm.

2) Channel Configuration: The Rician factor is set as $K = K_{ar} = K_{br}$ dB and $K_{ba} = -10^2$ dB. If $K \to +\infty$, the channel is equivalent to LoS fading, while if $K \to -\infty$, the channel is equivalent to Rayleigh fading. According to [49] and [50], the path-loss effect is modelled according to whether there is a LoS fading or not. The path-loss is $\beta_{uv} = \beta_0(\frac{d_{uv}}{d_0})^{-\epsilon_{uv}}$, $u, v \in \{a, b, r\}$, where ϵ_{uv} is the path-loss exponent, β_0 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, UE-RIS and UE-BS links are set as $\epsilon_{ar} = 2.2$, $\epsilon_{br} = 2.2$ and $\epsilon_{ba} = 3.67$, respectively. Also, $\beta_0 = -37.5$ dB and $\beta_0 = -35.1$ dB are set for a channel with and without an LoS component, respectively.

3) Considered Algorithms: The proposed and existing algorithms are defined as follows:

1) **Multiple antennas (MA) w/o RIS (non-optimized):** There are a BS with multiple antennas (without precoding) and a UE. The BS and UE measure the direct channel, $\mathbf{h}$, and extract the randomness from it.
2) **MA w/ RIS (non-optimized):** There are a BS with multiple antennas (without precoding), a UE and a RIS (phase shift vector not optimized). We configure the phase shift vector and precoding matrix as $\mathbf{v} = \mathbf{1}_M$ and $\mathbf{P} = \mathbf{I}_N$, respectively. The BS and UE extract the randomness from the LS estimation of the equivalent channel, $\mathbf{h}_e(\mathbf{v})$.
3) **Single antenna (SA) w/ RIS (random):** This case is to randomly configure the reflection coefficients in the phase shift vector in a single-antenna system, which is applied in [19]–[21].
4) **SA w/ RIS (optimized):** This case is to design the phase shift vector, $\mathbf{v}$, in a single-antenna system, which is applied in [22], [24]. Given the optimal $\mathbf{v}$, the BS and UE extract the randomness from $\mathbf{h}_e(\mathbf{v})$. The optimal $\mathbf{v}$ is derived in Appendix A.
5) **MA w/ RIS (optimized):** This case is to measure the cascaded channel and distil secret keys from it in a multiple-antenna system with a RIS. According to Algorithms 1 and 2, we configure the $\mathbf{W}$. This case illustrates the upper bound of the RIS-assisted key generation. We



(a) (b)

Fig. 4. (a) The eigenvalues of subchannels. (b) The power allocation for one channel realization. $P_t = 20$ dBm, $N = 2$, $M = 16$, $K = 0$ dB, $d_r = 1/4$.

calculate the key rate extracted from the measurements of the cascaded channel, $\mathbf{W}^T\mathbf{h}_r$.

6) **The proposed algorithm:** We configure the precoding matrix, $\mathbf{P}$, and phase-shift matrix, $\bar{\mathbf{\Phi}}$, based on the proposed algorithm, where $\mathbf{P}$ and $\bar{\mathbf{\Phi}}$ are decomposed from $\mathbf{W}$ that is obtained in MA w/ RIS (optimized). The BS and UE extract the randomness from the LS estimation of the cascaded channel, $(\bar{\mathbf{\Phi}}^T \otimes \mathbf{P}^T)\mathbf{h}_r$.

B. Results

In all the figures, solid lines and markers denote numerical results and simulation results, respectively. In the proposed algorithm case, the numerical results of key rate are calculated from (28), where $\bar{\mathbf{\Phi}}$ and $\mathbf{P}$ are solved from the problem (P4). In the MA w/ RIS (optimized) case, the numerical results of key rate are calculated from (28), where $\bar{\mathbf{\Phi}} \otimes \mathbf{P}$ is replaced by $\mathbf{W}$. In the MA w/o RIS (non-optimized) case, the numerical results of key rate are calculated according to [28], where the channel coefficients of the multiple-antenna system are set as $\mathbf{h}$ in this paper. In the MA w/ RIS (non-optimized) case, the numerical results of key rate are extracted from the channel coefficients in (14), where $\mathbf{v} = \mathbf{1}_M$ and $\mathbf{P} = \mathbf{I}_N$. In the SA w/ RIS (random) case, the numerical results of the key rate are calculated according to [22], [24]. In the SA w/ RIS (optimized) case, the numerical results of the key rate are calculated based on (61) in Appendix A. To verify the numerical results, we carry out Monte Carlo simulations using Matlab and employ *ITE* toolbox [51] to calculate the mutual information of the measurements of BS and UE.

1) Evaluation of key rate: We evaluated the key rate against transmit power, the number of reflecting elements, the side length of an element and the Rician factor.

Fig. 4 exhibits the eigenvalues of subchannels and power allocation results of Algorithm 1. The number of transmit antennas and reflecting elements is set as $N = 2$ and $M = 16$, respectively, so that $D = 34$. Fig. 4 (a) shows the eigenvalues of 34 subchannels, which are in descending order. It is apparent that channel variance concentrates on two subchannels whose eigenvalues are bigger than the others. Fig. 4 (b) shows the power allocation results of Algorithm 1. It can be seen that the power is mainly allocated to the first two subchannels since the channel variance of the direct channel is larger than that of the RIS-reflected subchannels.

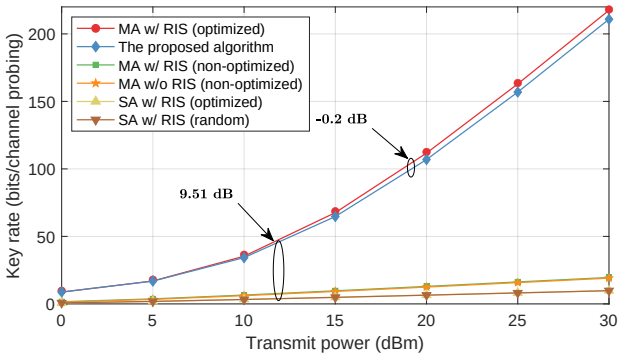


Fig. 5. Key rate versus transmit power. $N = 2$, $M = 16$, $K = 0$ dB, and $d_r = 1/4$.

Fig. 5 shows the key rate that BS and UE can achieve with each channel probing versus transmit power. The average gap between the key rate of MA w/ RIS (optimized) and MA w/o RIS (non-optimized) is about 9.51 dB, which is a quite significant improvement. Compared to the SA w/ RIS (optimized) and SA w/ RIS (random) cases, the proposed algorithm also has a great advantage, since the key rate of the cascaded channel is greater than that of the equivalent channel. Moreover, we compare the key rate of the proposed algorithm and MA w/ RIS (optimized) cases. The MA w/ RIS (optimized) scheme applies the equivalent matrix variable, $\mathbf{W}$, to extract the secret keys from subchannels, $\mathbf{h}_r$, which can not be directly implemented in practice. The equivalent matrix variable exhibits the upper bound of the key rate of the RIS-assisted key generation. For practical implementation, the proposed scheme decomposes $\mathbf{W}$ to the precoding matrix at the BS, $\mathbf{P}$, and phase-shift matrix at the RIS, $\bar{\mathbf{\Phi}}$. The average gap is about -0.2 dB, which means the key rate of the proposed algorithm case approximately approaches the upper bound. It is obvious that the key rate of SA w/ RIS (random) case is smaller than the key rate of SA w/ RIS (optimized). It is noted that the LoS component will be perturbed by the artificial randomness induced by the random phase reflection coefficients. However, this part of key bits is not secure, since the LoS component can be expected by calculation from the location of the transceivers in a three-dimensional Cartesian coordinate [52]. Therefore, we calculate the key rate attached to the NLoS fading.

Fig. 6 illustrates the key rate per channel realization for a different number of reflecting elements. It is observed that the key rate increases with the number of reflecting elements. Compared to the SA w/ RIS (optimized) and the SA w/ RIS (random) cases, the proposed algorithm exhibits considerable benefit, which means the increase of elements has a greater influence on the key rate of the cascaded channel compared to the key rate of the equivalent channel. What's more, the key rate of the MA w/o RIS (non-optimized) and MA w/ RIS (non-optimized) cases keep almost constant with the increase of the element numbers, which means element numbers cannot improve the SNR of these two cases greatly.

Fig. 7 investigates the impact of the side length of a reflecting element. The first observation is that the key rate increases

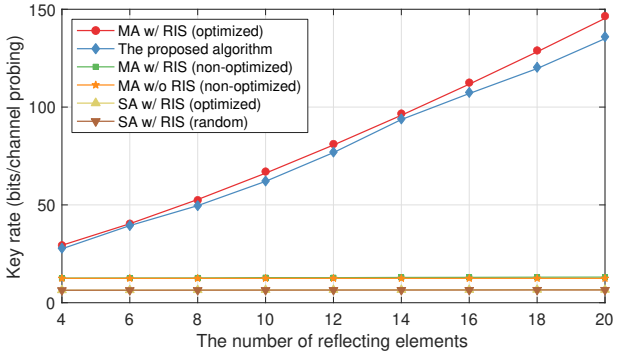


Fig. 6. Key rate versus the number of reflecting elements. $P_t = 20$ dBm, $N = 2$, $K = 0$ dB, and $d_r = 1/4$.

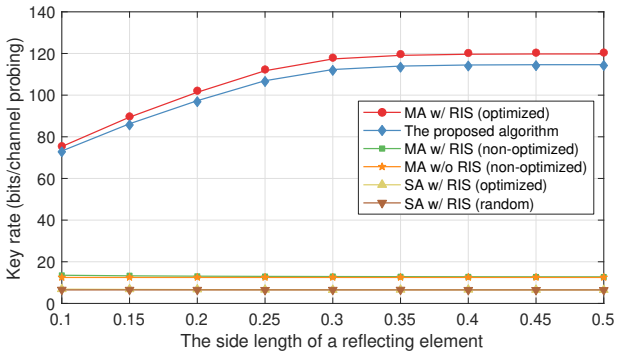


Fig. 7. Key rate versus the side length of a reflecting element. $P_t = 20$ dBm, $N = 2$, $M = 16$, $K = 0$ dB, and $d_r = 1/4$.

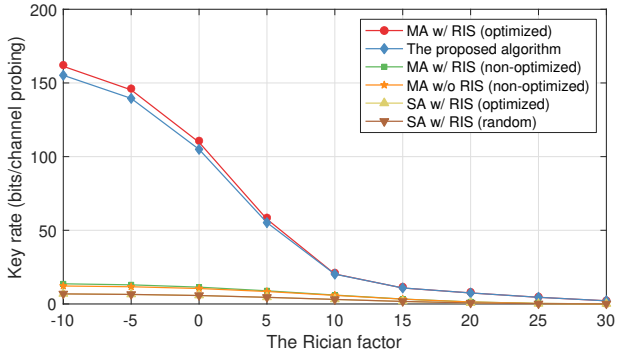


Fig. 8. Key rate versus the Rician factor. $P_t = 20$ dBm, $N = 2$, $M = 16$, and $d_r = 1/4$.

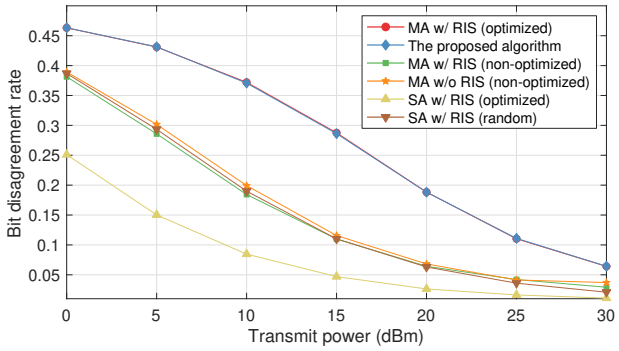


Fig. 9. BDR versus transmit power. $N = 2$, $M = 15$, $d_r = 1/4$, $K = 0$ dB.

with the side length of a reflecting element. As the side length gets larger from 0.1 to 0.5, the spatial correlation between subchannels gradually becomes lower and the subchannels eventually become uncorrelated. Therefore, the MA w/ RIS (optimized) and the proposed algorithm cases converge to a maximum value. What's more, there is a large performance gain in the proposed algorithm case compared with the SA w/ RIS (optimized) case. In the MA w/o RIS case, the key rate keeps constant because the key rate is determined by the direct channel. In the MA w/ RIS (non-optimized), SA w/ RIS (optimized) cases and SA w/ RIS (random), the key rate drops a little. We find that the quality of the equivalent channel gets worse with the increase in the side length.

Fig. 8 shows the key rate versus the Rician factor K. As K approaches infinity, the LoS component dominates. In contrast, the NLoS components dominate and the channel follows the Rayleigh distribution when K approaches zero. It is apparent that the key rate decreases with the Rician factor. When the Rician factor gets larger, the channel variance of the LoS fading becomes larger, which is not suitable for key generation. Compared to the MA w/ RIS (non-optimized) and SA w/ RIS (optimized) cases, our algorithm exhibits considerable improvement.

2) Evaluation of BDR and Randomness: We also evaluated BDR and randomness after the channel measurements are converted to key bits. The parameters of the system are set as $N = 2$, $M = 15$, $d_r = 1/4$, $K = 0$ dB. Here, we apply a three-bit CDF quantization to convert the measurements to bits.

As shown in Fig. 9, we show the BDR versus transmit power. The BDR of all schemes decreases with the transmit power since the high SNR reduces the disagreements between Alice and Bob. Since the equivalent channel is the combination of the direct and RIS-reflected channels, the channel variance of the equivalent channel is bigger than that of the subchannels of the cascaded channel. Therefore, the BDR of the proposed algorithm is higher than the SA w/ RIS (optimized) case. Since the quantization bits are set as the same for all subchannels, the BDR of the key bits quantized from the RIS-reflected subchannels decreases the average BDR. Although the BDR of the proposed scheme is poorer than the works on the equivalent channel, the key rate is better in comparison. The quantization bit can be set according to the SNR of each subchannel to let the key generation system approach the theoretical key rate [29]. Compared to the MA w/o RIS (non-optimized) case, the BDR of the proposed algorithm is similar to the BDR of the proposed scheme.

The generated key should be truly random to protect secret keys from brute-force attacks for the requirement of cryptographic applications [2]. In each fading block, the subchannels are the random source for key generation, where there is a spatial correlation between subchannels. Multiple rounds of channel probing are conducted to measure the subchannels. We generate the measurements from 5000 fading blocks, where $2 \times (15 + 1) = 32$ measurements are obtained in a block when $N = 2$, $M = 15$, $P_t = 20$ dBm, $K = 0$ dB, and $d_r = 1/4$. To verify whether the spatial correlation affects

TABLE I
RANDOMNESS TEST RESULTS

	MA w/ RIS (optimized)	The proposed algorithm
Frequency	0.27	0.79
Block frequency	0.79	0.69
Runs	0.59	0.96
Longest run of 1s	0.96	0.64
DFT	0.85	0.81
Serial	0.39	0.55
	0.74	0.67
Appro. entropy	0.47	0.97
Cum. sums. (fwd)	0.22	0.32
Cum. sums. (rev)	0.35	0.5

the randomness, we use the National Institute of Standards and Technology (NIST) test suite, which is widely in the key generation area [53], [54]. Each test returns a p value. When the p value is greater than 0.01, the sequence passes the particular randomness test. We use the toolbox [55] to perform 9 NIST statistical tests and the results are given in Table I. All the results are greater than 0.01, which means our algorithm is suitable for practical use

VII. Discussion

A. Eavesdropping Attack

In our study, we consider the scenario of a full-scattering propagation environment, where an eavesdropper is positioned half-wavelength away from the legitimate users, Alice and Bob. With the half-wavelength condition, the eavesdropper's channels are uncorrelated with legitimate users' channels, which is consistent with communication theory. Therefore, the upper and lower bounds of the secret key rate degenerate to the mutual information between the measurements of Alice and Bob, i.e. $I(\mathbf{z}_b; \mathbf{z}_a)$, which means the information leaked to the eavesdropper is nearly zero.

However, eavesdroppers will threaten the key generation systems in other harsh conditions. The eavesdropping effect has been studied both from simulations and experiments. From the theoretical aspects, He *et al.* studied different types of channel correlation models. They conduct simulations to verify that the half-wavelength assumption is only valid in rich scattering environments [56]. From the experimental aspects, eavesdropping attacks are investigated by testbeds utilizing different protocols, including ZigBee, Wi-Fi and LoRa. Zenger *et al.* [57] used the RSS parameters and carried out experiments by the IEEE 802.15.4 at 2.4 GHz. They found that the channels of Eve are correlated with that of legitimate users within three wavelengths. Zhang *et al.* [9] used both CSI and RSS parameters by IEEE 802.11 OFDM testbeds to verify the security of key generation with different channel conditions, including an indoor office (typical multipath) a reverberation chamber (very strong multipath) and an anechoic chamber (no multipath). It is found that the eavesdropper's channels a few centimetres away are uncorrelated with legitimate users' channels in a strong multipath environment. When there is a strong LoS, key generation is significantly insecure. Furthermore. Yang *et al.* [58] carried out LoRa-based experiments to verify the eavesdropping attacks on large-scale fading.

B. Static Environments

When the direct channel is static, the proposed scheme can separate the UE-BS channel from the cascaded channel so that the static UE-BS channel will not cause a correlation between the measurements. In the proposed channel probing protocol, the BS collects V measurements and stacks them into a longer vector as $\mathbf{z}_a = \left[\widehat{\mathbf{z}}_a^T(1), \ldots, \widehat{\mathbf{z}}_a^T(V)\right]^T = (\bar{\mathbf{\Phi}}^T \otimes \mathbf{P}^T)\mathbf{h}_r + \frac{1}{\sqrt{P_b}}\boldsymbol{\eta}_a$. Since $\bar{\mathbf{\Phi}}$ and $\mathbf{P}$ are reversible, $(\bar{\mathbf{\Phi}}^T \otimes \mathbf{P}^T)^{-1}$ is reversible with $(\bar{\mathbf{\Phi}}^T \otimes \mathbf{P}^T)^{-1} = (\bar{\mathbf{\Phi}}^T)^{-1} \otimes (\mathbf{P}^T)^{-1} = (\bar{\mathbf{\Phi}}^{-1})^T \otimes (\mathbf{P}^{-1})^T$. Therefore, the BS can recover the cascaded channel as $\mathbf{h}_r + (\bar{\mathbf{\Phi}}^T \otimes \mathbf{P}^T)^{-1}\frac{1}{\sqrt{P_b}}\boldsymbol{\eta}_a$. Similarly, the UE can recover the cascaded channel. Therefore, the static UE-BS can be wiped out and the other subchannels can be exploited for key generation.

C. Dynamic Environments

Our paper considers the block-fading channel models in dynamic environments, where the wireless channels vary from block to block. Our proposed method fully exploits the randomness from the subchannels associated with elements and the direct channel in the spatial domain. However, when channel fading varies rapidly, there will be a temporal correlation between the uplink and downlink channels [59]. The temporal correlation factor determines the nonreciprocal components between uplink and downlink channels. That is to say, the key rate of our proposed scheme provides a theoretical upper bound for those schemes considering the temporal correlation between uplink and downlink channels in dynamic environments. Sun *et al.* [60] modelled the spatial-temporal correlation of wireless channels in RIS systems. To extend our works to the rapid-varying block fading model, a channel probing protocol should be proposed to exploit the randomness in the time and spatial domains where the temporal correlation between uplink and downlink channels and the spatial correlation between subchannels associated with elements are jointly considered. Our future work will focus on the adaptive design of the precoding and phase shift matrices to exploit randomness in the time and spatial domains.

VIII. Conclusion

This paper investigated a RIS-assisted key generation system, which jointly considered the design of the precoding and phase shift matrices to fully exploit the randomness from the cascaded channel. We first designed a water-filling algorithm to find the upper bound on the key rate of the system. Furthermore, we proposed an algorithm to obtain the phase shift and precoding matrices, which ensures the key rate approaches the upper bound. We found that the key rate is determined by the transmit power, the number of reflecting elements, the side length of an element and the Rician factor. Simulations validated that our protocol obtained a higher key rate than the existing algorithms.

APPENDIX A
DESIGN OF PHASE SHIFT VECTOR FOR THE EFFECTIVE CHANNEL

According to (10), the equivalent channel is

$$\mathbf{h}_e(\mathbf{v}) = \left[\mathbf{h}\ \mathbf{G}^T \text{diag}(\mathbf{f})\right] \bar{\mathbf{v}}. \tag{57}$$

If the BS is equipped with a single antenna, the equivalent channel is simplified as

$$h_e(\mathbf{v}) = \left[h\ \mathbf{g}^T \text{diag}(\mathbf{f})\right] \bar{\mathbf{v}}, \tag{58}$$

where h, $\mathbf{g} \in \mathbb{C}^{M\times 1}$ and $\mathbf{f} \in \mathbb{C}^{M\times 1}$ are the UE-BS, BS-RIS and UE-RIS channels, respectively. Assume BS has the estimation noise n_a, $n_a \sim \mathcal{CN}(0, \sigma_a^2)$, and UE has the estimation noise n_b, $n_b \sim \mathcal{CN}(0, \sigma_b^2)$. Define $\widehat{h}_{e,a}(\mathbf{v})$ and $\widehat{h}_{e,b}(\mathbf{v})$ as the measurements of BS and UE, respectively. The covariance of the variable $[\widehat{h}_{e,a}(\mathbf{v}), \widehat{h}_{e,b}(\mathbf{v})]$ is given by

$$\mathbf{\Sigma} = \begin{bmatrix} p_e + \sigma_a^2 & p_e \\ p_e & p_e + \sigma_b^2 \end{bmatrix}, \tag{59}$$

where $p_e = \mathbb{E}\{h_e(\mathbf{v}) h_e(\mathbf{v})^*\}$ is the channel variance. If the direct and cascaded channels are uncorrelated, p_e is given by

$$p_e = \bar{\mathbf{v}}^T \mathbf{R}_e \bar{\mathbf{v}}^* = \bar{\mathbf{v}}^T \begin{bmatrix} \sigma_h^2 & \mathbf{0}_M^T \\ \mathbf{0}_M & \mathbf{R}_{arb} \end{bmatrix} \bar{\mathbf{v}}^*, \tag{60}$$

where $\mathbf{R}_e$ is the channel covariance of the equivalent channel and $\mathbf{R}_{arb} = \mathbb{E}\{\text{diag}(\mathbf{f}^*)\mathbf{g}^*\mathbf{g}^T \text{diag}(\mathbf{f})\}$.

According to the differential entropy of a circularly symmetric Gaussian variable, the upper bound on the key rate is

$$\begin{aligned} I(\widehat{h}_{e,a}(\mathbf{v}); \widehat{h}_{e,b}(\mathbf{v})) &= \log_2 \left(\frac{(p_e + \sigma_a^2)(p_e + \sigma_b^2)}{\mathbf{\Sigma}} \right) \\ &= \log_2 \left(1 + \frac{p_e}{\sigma_a^2 + \sigma_b^2 + \frac{\sigma_a^2 \sigma_b^2}{p_e}} \right). \end{aligned} \tag{61}$$

The key rate increases with p_e. To find the optimal key rate, we should solve the problem of $\max_{\bar{\mathbf{v}}}\ \bar{\mathbf{v}}^T \mathbf{R}_e \bar{\mathbf{v}}$, where the objective function is a quadratic form. If there is a norm constraint, the optimal value is the biggest eigenvalue of $\mathbf{R}_e$ and the $\bar{\mathbf{v}}$ is the corresponding eigenvector. However, the reflection coefficient has the constraint of $|\bar{\phi}_m| = 1$. Note that $\bar{\mathbf{v}}^T \mathbf{R}_e \bar{\mathbf{v}}^* = \text{Tr}(\mathbf{R}_e \bar{\mathbf{v}}^* \bar{\mathbf{v}}^T)$. Define $\mathbf{\Theta} = \bar{\mathbf{v}}^* \bar{\mathbf{v}}^T$ and reformulate the problem as a semidefinite programming (SDP) problem. We should meet the constraints of $\mathbf{\Theta} \succeq 0$ and $\text{rank}(\mathbf{\Theta}) = 1$. Therefore, we have the following problem.

$$\begin{aligned} \max_{\mathbf{\Theta}}\ & \text{Tr}\left[\mathbf{R}_e \mathbf{\Theta}\right] \\ \text{s.t. } & \mathbf{\Theta}_{i,i} = 1,\ i = 1, \ldots, M+1, \\ & \text{rank}(\mathbf{\Theta}) = 1. \end{aligned} \tag{62}$$

Since the rank-one constraint is non-convex, we relax it and solve the above problem by the CVX [61]. However, it may not generate a rank-one solution, i.e., $\text{rank}(\mathbf{\Theta}) \neq 1$. Furthermore, we apply the Gaussian randomization to obtain a feasible solution [62].

REFERENCES

[1] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, Mar. 2021.

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

[3] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the internet of things in a quantum world," *IEEE Commun. Maga.*, vol. 55, no. 2, pp. 116–120, Feb. 2017.

[4] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things," *IEEE Security and Privacy*, vol. 13, no. 1, pp. 14–21, Jan./Feb. 2015.

[5] E. Ronen, C. O'Flynn, A. Shamir, and A. O. Weingarten, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," in *IEEE Symposium on Security and Privacy*, San Jose, CA, USA, May 2017, pp. 195–212.

[6] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[7] R. Ahlswede and I. Csiszir, "Common randomness in information theory and cryptography-Part I : Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[8] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels — Part I : Definitions and a completeness result," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.

[9] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[10] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2763–2776, 2014.

[11] J. Zhang, A. Marshall, and L. Hanzo, "Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12 462–12 466, 2018.

[12] S. N. Premnath, P. L. Gowda, S. K. Kasera, N. Patwari, and R. Ricci, "Secret key extraction using bluetooth wireless signal strength measurements," in *Proc. IEEE Int. Conf. Sensing, Communication, and Networking (SECON)*, 2014, pp. 293–301.

[13] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," *IEEE Trans. Wireless Commun.*, vol. 26, no. 5, pp. 48–54, Oct. 2019.

[14] M. Di Renzo, A. Zappone, M. Debbah, M. S. Alouini, C. Yuen, J. De Rosny, and S. Tretyakov, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2450–2525, Nov. 2020.

[15] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

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

[17] P. Staat, H. Elders-Boll, M. Heinrichs, R. Kronberger, C. Zenger, and C. Paar, "Intelligent reflecting surface-assisted wireless key generation for low-entropy environments," in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Helsinki, Finland, Sep. 2021, pp. 745–751.

[18] E. Bjornson, O. Ozdogan, and E. G. Larsson, "Reconfigurable intelligent surfaces: Three myths and two critical questions," *IEEE Commun. Mag.*, vol. 58, no. 12, pp. 90–96, Dec. 2020.

[19] Z. Ji, P. L. Yeoh, G. Chen, C. Pan, Y. Zhang, Z. He, H. Yin, and Y. Li, "Random shifting intelligent reflecting surface for OTP encrypted data transmission," *IEEE Wireless Commun. Lett.*, vol. 10, no. 1192–1196, pp. 1–5, Jun. 2020.

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

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

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

[23] X. Lu, J. Lei, Y. Shi, and W. Li, "Intelligent reflecting surface assisted secret key generation," *IEEE Signal Process. Lett.*, vol. 28, pp. 1030–1034, Feb. 2021.

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

[25] Y. Liu, K. Huang, X. Sun, S. Yang, and L. Wang, "Intelligent reflecting surface assisted –assisted wireless secret key generation against multiple eavesdroppers," *Entropy*, vol. 24, no. 446, pp. 1–15, Mar. 2021.

[26] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, Jun. 2016.

[27] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.

[28] 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.

[29] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.

[30] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *14th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, San Francisco, CA, USA, Sep. 2008, pp. 128–139.

[31] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[32] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[33] 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.

[34] Z. Zhou, N. Ge, Z. Wang, and L. Hanzo, "Joint transmit precoding and reconfigurable intelligent surface phase adjustment: A decomposition-aided channel estimation approach," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1228–1243, Feb. 2021.

[35] G. T. De Araujo, A. L. De Almeida, and R. Boyer, "Channel estimation for intelligent reflecting surface assisted MIMO systems: A tensor modeling approach," *IEEE J. Sel. Top. Sign. Proces*, vol. 15, no. 3, pp. 789–802, Apr. 2021.

[36] 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.

[37] Q. Zhu and Y. Hua, "Optimal pilots for maximal capacity of secret key generation," in *Proc. IEEE GLOBECOM*, Hawaii, USA, Dec. 2019, pp. 1–6.

[38] A. L. Swindlehurst, G. Zhou, R. Liu, C. Pan, and M. Li, "Channel estimation with reconfigurable intelligent surfaces–A general framework," *Proc. IEEE*, vol. 110, no. 9, pp. 312–1338, Sep. 2022.

[39] 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.

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

[41] C. You, B. Zheng, and R. Zhang, "Channel estimation and passive beamforming for intelligent reflecting surface: Discrete phase shift and progressive refinement," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2604–2620, Jul. 2020.

[42] N. Boumal, B. Mishra, P.-A. Absil, and R. Sepulchre, "Manopt, a Matlab toolbox for optimization on manifolds," *Journal of Machine Learning Research*, vol. 15, no. 42, pp. 1455–1459, 2014. [Online]. Available: https://www.manopt.org

[43] H. Xie, F. Gao, S. Zhang, and S. Jin, "A unified transmission strategy for TDD / FDD massive MIMO systems with spatial basis expansion model," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3170–3184, Apr. 2017.

[44] 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, 2022.

[45] J. Ma, S. Member, S. Zhang, and H. Li, "Sparse bayesian learning for the time-varying massive MIMO channels : Acquisition and tracking," *IEEE Trans. Commun.*, vol. 67, no. 3, Mar. 2019.

[46] M. Jensen and J. Wallace, "A review of antennas and propagation for mimo wireless communications," *IEEE Trans. Antennas Propag.*, vol. 52, no. 11, pp. 2810–2824, Nov. 2004.

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

[48] C. Huth, R. Guillaume, T. Strohm, P. Duplys, I. A. Samuel, and T. Güneysu, "Information reconciliation schemes in physical-layer security: A survey," *Comput. Netw.*, vol. 109, pp. 84–104, Nov. 2016.

[49] I. Yildirim, A. Uyrus, and E. Basar, "Modeling and analysis of reconfigurable intelligent surfaces for indoor and outdoor applications in future wireless networks," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1290–1301, Feb. 2020.

[50] E. Bjornson, O. Ozdogan, and E. G. Larsson, "Intelligent reflecting surface versus decode-and-forward: How large surfaces are needed to beat relaying?" *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 244–248, Feb. 2020.

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

[52] Z. Wan, Z. Gao, and M. S. Alouini, "Broadband channel estimation for intelligent reflecting surface aided mmWave massive MIMO systems," in *IEEE Int. Conf. Commun.*, Dublin, Ireland, Jun. 2020.

[53] G. Li, C. Sun, E. A. Jorswieck, J. Zhang, A. Hu, and Y. Chen, "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.

[54] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2692–2705, Feb. 2020.

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

[56] X. He, H. Dai, W. Shen, P. Ning, and R. Dutta, "Toward proper guard zones for link signature," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2104–2117, Mar. 2016.

[57] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, "The passive eavesdropper affects my channel: Secret-key rates under real-world conditions," in *Proc. IEEE Globecom TCPLS Workshops*, Washington DC, USA, Dec. 2016, pp. 1–6.

[58] L. Yang, Y. Gao, J. Zhang, S. Camtepe, and D. Jayalath, "A channel perceiving attack on long-range key generation and its countermeasure," *Computer Communications*, pp. 108–118, Jul. 2019.

[59] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, Apr. 2017.

[60] S. Sun and H. Yan, "Small-scale spatial-temporal correlation and degrees of freedom for reconfigurable intelligent surfaces," *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2698–2702, Dec. 2021.

[61] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, Mar. 2014.

[62] A. M. C. So, J. Zhang, and Y. Ye, "On approximating complex quadratic optimization problems via semidefinite programming relaxations," *Mathematical Programming*, vol. 110, no. 1, pp. 93–110, 2007.