In: ICC 2023 - IEEE International Conference on Communications, 28 May - 01 June 2023, Rome, Italy, pp. 2909-2914
DOI: 10.1109/ICC45041.2023.10278950

Reconfigurable Intelligent Surface-induced Randomness for mmWave Key Generation

Shubo Yang, Han Han, Yihong Liu, *Graduate Student Member, IEEE*, Weisi Guo, *Senior Member, IEEE*, Zhibo Pang, and Lei Zhang, *Senior Member, IEEE*

***Abstract*—Secret key generation in physical layer security exploits the unpredictable random nature of wireless channels. The millimeter-wave (mmWave) channels have limited multipath and channel randomness in static environments. In this paper, for mmWave secret key generation of physical layer security, we use a reconfigurable intelligent surface (RIS) to induce randomness directly in wireless environments, without adding complexity to transceivers. We consider RIS to have continuous individual phase shifts (CIPS) and derive the RIS-assisted reflection channel distribution with its parameters. Then, we propose continuous group phase shifts (CGPS) to increase the randomness specifically at legal parties. Since the continuous phase shifts are expensive to implement, we analyze discrete individual phase shifts (DIPS) and derive the corresponding channel distribution, which is dependent on the quantization bit. We then derive the secret key rate (SKR) to evaluate the randomness performance. With the simulation results verifying the analytical results, this work explains the mathematical principles and lays a foundation for future mmWave evaluation and optimization of artificial channel randomness.**

***Index Terms*—Physical layer security, secret key generation, reconfigurable intelligent surface, intelligent reflecting surface.**

I. Introduction

WIRELESS networks are becoming ubiquitous nowadays and in the future Internet of Things (IoT) systems. However, their broadcast nature makes them vulnerable to malicious attacks. Classic encryption schemes, such as advanced encryption standard and public key cryptography, are dependent on cryptography computation techniques [1]. The applications of classic schemes to IoT devices and wireless sensor networks (WSNs) bring challenges, since the devices and sensor nodes have small sizes and limited computational capability. Thus, extensive research is carried out in secret key generation of physical layer security, where the legitimate users extract keys from their correlated observations of the reciprocal channel in a lightweight manner [2]. The correlation of channels makes it possible to generate keys without key exchange, and the dynamic uniqueness of the channel prevents eavesdroppers from mimicking. While in dynamic environments the movements of users or objects are sufficient to produce randomness, the randomness is limited in static environments, such as in open terrain with no moving objects. Besides, the millimeter wave (mmWave) communication is envisioned as a significant technology for the fifth generation (5G) networks and beyonds [3]. Thus, the security in mmWave static environments needs to be researched.

The newly developed reconfigurable intelligent surface (RIS), also known as Intelligent Reflecting Surface (IRS), has the potential to produce artificial randomness in mmWave static environments. RIS is a two-dimensional surface consisting of a large number of passive low-cost reflecting elements [4]. Each scattering element of RIS is independently capable of altering the amplitude and/or phase of the incident signals. Additionally, RIS becomes more important in high-frequency band communications, e.g., mmWave and THz communications that have severe coverage issues. The existing RIS applications mainly target indoor static scenarios [5]. Therefore, RIS can be easily incorporated in mmWave static environments. By adding RIS, artificial randomness can be produced. The randomness does not rely on dynamic environments and is produced directly in the channel, without needing increased transceiver costs.

Research has been done on RIS-assisted key generation. Random shifting RIS is applied to increase the secure transmission rate, and the time allocation for key generation and transmission is designed [6]. RIS with discrete phase shifts is adopted to generate secret keys, and the secret key rate (SKR) is derived [7]. The practical implementation of using RIS in the OFDM system is conducted [8]. However, most existing literature focuses on sub-6 GHz systems and models on Gaussian channels. The mmWave channels have a poor scattering nature and exhibit limited multipath, so they may not conform to Gaussian channels. Moreover, the channel distribution resulted from RIS phase shifts and element number is still unknown. Besides, most previous works assume each RIS element phase shift is independent and identically distributed (i.i.d), without changing phase shift distributions to improve randomness.

Therefore, in this paper, the RIS-assisted mmWave key generation is proposed. We model RIS-induced randomness in mmWave key generation, and we focus on the fundamental analytical derivations of channel distribution with random RIS weights. For the random weights, we consider applying continuous individual phase shifts (CIPS) on each element

S. Yang is with the Glasgow College, University of Glasgow (e-mail: 2429400y@student.gla.ac.uk). H. Han is with Electrical and Computer Engineering Department, University of Toronto, ON M5S 3G4, Canada (e-mail: johnny.han@mail.utoronto.ca). Y. Liu and L. Zhang are with James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K. (e-mail: y.liu.6@research.gla.ac.uk; lei.zhang@glasgow.ac.uk). W. Guo is with School of Aerospace, Transport and Manufacturing, Cranfield University, MK43 0AL Cranfield, U.K. (e-mail: weisi.guo@cranfield.ac.uk). Z. Pang is with Department of Automation Technology, ABB Corporate Research Sweden, Vasteras, Sweden, and Department of Intelligent Systems, Royal Institute of Technology (KTH), Stockholm, Sweden. (e-mail: pang.zhibo@se.abb.com, zhibo@kth.se).

Funding information: Zhibo Pang's work is partly funded by the Swedish Foundation for Strategic Research (SSF) through the project APR20-0023.

and continuous group phase shifts (CGPS) on elements in groups to produce higher randomness. In addition, we consider channels for both continuous[1] and discrete phase shifts and compare their performance. To summarize, the main contributions of this paper are as follows.

- The RIS-induced channel distribution and its parameters are derived, given RIS is a uniform rectangular array (URA) and the elements have CIPS. As the result, an artificial Rayleigh/Rician fading is induced directly in the environments.
- To increase the amount of induced randomness, CGPS is proposed and the channel is derived. The channel variance for legal parties increases, and there is a tradeoff between group number and group size. The discrete individual phase shifts (DIPS) is also discussed based on quantization bits.
- The SKR is derived for CIPS, CGPS, and DIPS, to evaluate the performance of artificial randomness.

Notations: Bold-faced letters are used to denote matrix or column vectors, while lightfaced letters are used to denote scalar quantities. Superscripts $(\cdot)^T$, $(\cdot)^*$, and $(\cdot)^H$ represent the transpose, conjugate and conjugate transpose operations, respectively. $\odot$ denotes the point-wise multiplication. We use the notations shown in Table I in this paper.

TABLE I: Notations

Symbol	Definition
λ	Wavelength
k	Wave number, where $k = \frac{2\pi}{\lambda}$
d	Element spacing in RIS
M	Element number of the RIS
m	An integer in range $[1, M]$
ϕ_m	The phase shift of the m-th RIS element weight
ψ	The incident or reflected azimuth angle
θ	The incident or reflected elevation angle
B	RIS discrete weight quantization bit
$\boldsymbol{R}$	The covariance between the real and imaginary parts of a complex Gaussian distribution
R_s	Secret key rate
$U(a,b)$	Indicate a uniform distribution on interval (a,b)
$N(\mu,\sigma^2)$	Indicate a Gaussian distribution with mean μ and variance σ^2
$h_{(\cdot)}$	Indicate the channel
$(\cdot)_x, (\cdot)_y$	Indicate physical quantities on x-axis and y-axis, respectively
$(\cdot)_{real}, (\cdot)_{imag}$	Indicate quantities of the real and imaginary parts, respectively
$(\cdot)_{cos}, (\cdot)_{sin}$	Indicate quantities of cosine and sine functions, respectively
$(\cdot)_i, (\cdot)_o$	Indicate incident and reflected angles, respectively
$(\cdot)_{CI}$	Indicate quantities when RIS weights have continuous individual phase shifts
$(\cdot)_{CG}$	Indicate quantities when RIS weights have continuous group phase shifts
$(\cdot)_{DI}$	Indicate quantities when RIS weights have discrete individual phase shifts

II. System Model

Consider an RIS-assisted wireless communication between legitimate parties, Alice and Bob. There is also an eavesdropper Eve, who passively listens to the communication. Assume all the parties are operated under a mmWave static environment. We consider the narrowband line-of-sight (LOS) transmission in the far field between Alice/Bob and RIS. This assumption can be justified since the multipath effect is constrained and the high path loss makes non-line-of-sight (NLOS) paths' power small. The RIS provides cascaded LOS paths. Additionally, the path loss is a constant related to distance and can be easily predicted by eavesdropper [7]. Since the transmission channel between Alice and Bob is reciprocal, we only consider the situation where Alice is transmitting signals to Bob to avoid redundancy.

[1]The continuous RIS weights are difficult to implement. This is because more levels of weight phase shift result in more costs, which is not scalable to a large number of elements [9]. The continuous weights' performance is the upper limit for discrete weights when weights' quantization bits approach infinity.

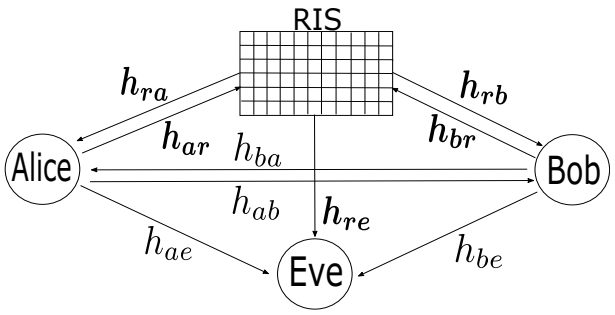


Fig. 1: RIS-assisted secret key generation model.

As shown in Fig. 1. Alice and Bob aim at establishing a random secret cryptographic key based on their reciprocal communication channel and reducing the key leakage to Eve. They measure the common channel through their exchanged signals and generate keys using parameters of the received signals, e.g. channel state information (CSI) and received signal strength (RSS). When Alice transmits signal s, the received signal at Bob can be expressed as

$$y = (h_{ab} + \boldsymbol{h_{rb}^H W h_{ar}})s + z \ , \tag{1}$$

where $h_{ab} \in \mathbb{C}^{1\times 1}$, $\boldsymbol{h_{ar}} \in \mathbb{C}^{M\times 1}$, $\boldsymbol{h_{rb}} \in \mathbb{C}^{M\times 1}$ represent the direct channel between Alice and Bob, the channel between Alice and RIS, and the channel between RIS and Bob, $z \sim \mathcal{CN}(0, \sigma_z^2)$ is the additive white Gaussian noise (AWGN), and $\boldsymbol{W}$ is the diagonal weight matrix with each entity on the diagonal being the RIS weight of each surface element. The weight of the m-th surface element is represented as $e^{j\phi_m}$.

To generate shared keys in static environments and reduce the key leakage to Eve, it is crucial to increase the channel randomness through RIS. As in (1), though $\boldsymbol{h_{ar}}$ and $\boldsymbol{h_{rb}}$ are static in mmWave static environments, when RIS weights $\boldsymbol{W}$ vary, $\boldsymbol{h_{rb}^H W h_{ar}}$ becomes dynamic. Thus, RIS becomes the major source of channel randomness through varying the reflection channel $\widetilde{H} = \boldsymbol{h_{rb}^H W h_{ar}}$. In this case, we focus on $\widetilde{H}$, which can be expressed using steering vectors and weight vector [10] as

$$\widetilde{H} = \boldsymbol{w}^H \cdot [\boldsymbol{a}(\boldsymbol{\Omega}_i) \odot \boldsymbol{a}(\boldsymbol{\Omega}_o)] \ , \tag{2}$$

where $\boldsymbol{w}$ is the weight vector with each entity being the diagonal entity of $\boldsymbol{W}$, i.e., weight of each surface element. Besides, the steering vector of the channels between Alice and RIS and between RIS and Bob are

$$\boldsymbol{a}(\boldsymbol{\Omega}_i) = [a(\boldsymbol{\Omega}_{i,1}), \cdots, a(\boldsymbol{\Omega}_{i,m}), \cdots, a(\boldsymbol{\Omega}_{i,M})]^T \tag{3}$$

$$\boldsymbol{a}(\boldsymbol{\Omega}_o) = [a(\boldsymbol{\Omega}_{o,1}), \cdots, a(\boldsymbol{\Omega}_{o,m}), \cdots, a(\boldsymbol{\Omega}_{o,M})]^T \ , \tag{4}$$

where $\boldsymbol{\Omega}_{i,m}$ and $\boldsymbol{\Omega}_{o,m}$ are the terms characterizing the incident spatial information from Alice at RIS m-th element and the reflected spatial information from m-th element to Bob, respectively. Since the environment is static, $\boldsymbol{\Omega}_i$ and $\boldsymbol{\Omega}_o$ are fixed, and $\widetilde{H}$ becomes a function of solely $\boldsymbol{w}$. Note that averaging $\widetilde{H}$ derived from all possible pairs of $\boldsymbol{\Omega}_i$ and $\boldsymbol{\Omega}_o$ provides an estimation of the overall channel distribution.

III. RIS-Assisted Key Generation

In this section, we first derive the probability density function (p.d.f) of reflection channel $\widetilde{H}$ with a given random RIS having CIPS and CGPS. Individual shifting means that the RIS phase shifts $\{\boldsymbol{\phi} = [\phi_1, \cdots, \phi_m, \cdots, \phi_M], m \in [1, M]\}$ are i.i.d. Group shifting means the elements phase shifts in a group are first implemented maximum ratio transmission (MRT) and then added a random phase shift. Next, we consider DIPS. The channel for 1-bit is found different from other quantization bits. Since group phase shifts need MRT to compensate for the phase difference caused by element distance, the discrete group phase shifts (DGPS) need multiple levels to realize the compensation. Implementing multiple-level discrete phase shifts is expensive compared to low-level phase shifts. Thus, we only discuss CGPS, and DGPS will be our future work.

Note that a uniform linear array (ULA) can be considered a special case of URA while URA is a typical planar array structure. Thus, we consider RIS in URA configuration, which can be further extended into other complex RIS shapes.

A. Continuous Individual Phase Shifts

Consider a URA RIS with M_x and M_y elements equally spaced on x-axis and y-axis, respectively, where the total element number is $M = M_x \cdot M_y$. The incident and reflected angles are described by $\boldsymbol{\Omega}_i = (\psi_i, \theta_i)$ and $\boldsymbol{\Omega}_o = (\psi_o, \theta_o)$. Assume the i.i.d RIS weight phase shifts $\boldsymbol{\phi}$ are continuous uniformly distribution $\phi_m \sim U(0, 2\pi)$. Then, the multiplication of steering vectors in (2) with elements spacing along x-axis d_x and y-axis d_y can be expressed as

$$\begin{aligned}\boldsymbol{a}(\boldsymbol{\Omega}_i) \odot \boldsymbol{a}(\boldsymbol{\Omega}_o) =& [1, \cdots, e^{j(\xi_x \cdot (m_x-1)+\xi_y \cdot (m_y-1))}, \\ & \cdots, e^{j(\xi_x \cdot (M_x-1)+\xi_y \cdot (M_y-1))}]^T ,\end{aligned} \tag{5}$$

where $m_x \in [1, M_x]$ and $m_y \in [1, M_y]$ are integers [11]. Additionally, $k = \frac{2\pi}{\lambda}$ is the wave number and

$$\xi_x = k d_x (\cos\psi_i \sin\theta_i + \cos\psi_o \sin\theta_o) , \tag{6}$$

$$\xi_y = k d_y (\sin\psi_i \sin\theta_i + \sin\psi_o \sin\theta_o) . \tag{7}$$

Consequently, the reflection channel following (2) can be constructed as

$$\begin{aligned}\widetilde{H} =& 1 + \cdots + e^{j[\phi_m + (\xi_x \cdot (m_x-1)+\xi_y \cdot (m_y-1))]} \\ & + \cdots + e^{j[\phi_M + (\xi_x \cdot (M_x-1)+\xi_y \cdot (M_y-1))]} \\ =& \sum_{m_y=1}^{M_y} \sum_{m_x=1}^{M_x} e^{j(\phi_m+\alpha)} \\ =& \sum_{m_y=1}^{M_y} \sum_{m_x=1}^{M_x} \cos(\phi_m+\alpha) + j \sum_{m_y=1}^{M_y} \sum_{m_x=1}^{M_x} \sin(\phi_m+\alpha) ,\end{aligned} \tag{8}$$

where

$$m = (m_y-1) \cdot M_x + m_x , \ \alpha = (m_x-1) \cdot \xi_x + (m_y-1) \cdot \xi_y . \tag{9}$$

According to the central limit theorem (CLT), $\widetilde{H}$ converges to a complex Gaussian distribution when M is large enough. This assumption could be justified since a practical RIS usually has an extremely large number of elements, e.g. more than tens of elements [5]. Therefore, the real and imaginary parts both converge to Gaussian distributions that are fully determined by means and variances. The mean and variance of the real part of $\widetilde{H}_{CI}$ can be expressed as

$$\mu_{real,CI} = \sum_{m_y=1}^{M_y} \sum_{m_x=1}^{M_x} \mu_{cos,CI} , \ \sigma^2_{real,CI} = \sum_{m_y=1}^{M_y} \sum_{m_x=1}^{M_x} \sigma^2_{cos,CI} , \tag{10}$$

where

$$\mu_{cos,CI} = \int_0^{2\pi} \cos(\phi_m + \alpha) f(\phi_m) d\phi_m = 0 . \tag{11}$$

$$\sigma^2_{cos,CI} = \int_0^{2\pi} \cos^2(\phi_m + \alpha) f(\phi_m) d\phi_m - \mu^2_{cos,CI} = \frac{1}{2}. \tag{12}$$

The imaginary part can be derived similar to the real part. By substituting (11) (12) into (10), the channel real and imaginary parts are

$$\Re(\tilde{H}_{CI}) \sim N(0, \frac{M}{2}) , \ \Im(\tilde{H}_{CI}) \sim N(0, \frac{M}{2}) . \tag{13}$$

Since the real and imaginary parts of $\widetilde{H}_{CI}$ constitute a joint Gaussian distribution and the covariance of them equals 0, the real and imaginary parts are independent. The distribution of $\widetilde{H}_{CI}$ is also independent of $\boldsymbol{\Omega}_i$ and $\boldsymbol{\Omega}_o$. With any pair of incident and reflected angles, the mean of $\widetilde{H}_{CI}$ is $\mu_{CI} = 0$ while the variance of $\widetilde{H}_{CI}$ can be calculated as

$$\sigma^2_{CI} = \mathbb{E}[(\widetilde{H}_{CI} - \mu_{CI})(\widetilde{H}_{CI} - \mu_{CI})^*] = M . \tag{14}$$

Due to the channel parameters CSI and RSS are normally used to generate keys, the magnitude and phase distributions are also important. According to the joint Gaussian distribution, the result magnitude p.d.f and phase p.d.f of $\widetilde{H}_{CI}$ are Rayleigh and uniform distributions. When the direct path and reflection path are both considered, the direct path adds a non-zero mean, and the induced Rayleigh fading will turn into Rician fading. Hence, the CIPS RIS produces randomness by inducing an artificial Rayleigh/Rician fading in the environments.

B. Continuous Group Phase Shifts

Different from the i.i.d elements in CIPS, group shifting means first using MRT to achieve maximum transmission rate at Alice and Bob, then shifting the phase randomly. This induces more randomness at Alice and Bob.

The total elements M is divided into groups of q elements. There are $N = \lfloor \frac{M}{q} \rfloor$ groups in total. The n-th group has the added random phase $\phi_{n,rand} \sim U(0, 2\pi)$. When the m-th element is in n-th group, the phase shift for m-th element is

$$\phi_{m,CG} = \phi_{m,MRT} + \phi_{n,rand} , \tag{15}$$

where

$$\phi_{m,MRT} = \frac{[\boldsymbol{a}(\boldsymbol{\Omega}_{i,m}) \cdot \boldsymbol{a}(\boldsymbol{\Omega}_{o,m})]^H}{||\boldsymbol{a}(\boldsymbol{\Omega}_{i,m}) \cdot \boldsymbol{a}(\boldsymbol{\Omega}_{o,m})||} . \tag{16}$$

The $\phi_{m,MRT}$ compensates the steering vector phase difference of elements in the same group n to achieve larger signal strength. The random phase shift $\phi_{n,rand}$ produces the randomness. Then, according to the channel in (8), the channel

for CGPS can be expressed as

$$\widetilde{H}_{CG} = \sum_{n=1}^{N} q\cos(\phi_{n,rand}) + \ j\sum_{n=1}^{N} q\sin(\phi_{n,rand}) \ . \quad (17)$$

When RIS has a large number of elements, the number of groups N can be large when given a proper value of q. Then, $\widetilde{H}_{CG}$ converges to a complex Gaussian distribution. Similarly to Section III-A, the mean $\mu_{real,CG} = 0$ and the variance of the real part can be expressed as

$$\sigma^2_{real,CG} = \sum_{n=1}^{N} \sigma^2[q\cos(\phi_{n,rand})] = \frac{Nq^2}{2} \ . \quad (18)$$

Thus, the channel distribution for CGPS RIS is

$$\Re(\tilde{H}_{CG}) \sim N(0, \frac{Nq^2}{2}) \ , \Im(\tilde{H}_{CG}) \sim N(0, \frac{Nq^2}{2}) \ . \quad (19)$$

The channel variance can be then calculated as

$$\sigma^2_{CG} = Nq^2 \ . \quad (20)$$

There is a tradeoff between $N = \lfloor \frac{M}{q} \rfloor$ and q. When q is large the variance increases quadratically, but N may become too small to use CLT. The Gaussian distribution is the distribution that maximizes the entropy at a given variance. The CGPS variance $\sigma^2_{CG} = Nq^2$ can achieve larger randomness than the CIPS at Alice and Bob.

C. Discrete Individual Phase Shifts

Since continuous phase shifts are expensive to implement, discrete phase shifts RIS need be researched. Assume RIS has discrete weight phase shifts $\boldsymbol{\phi}$ with quantization bit B. $\boldsymbol{\phi}$ is i.i.d uniformly on discrete values $\{0, \frac{2\pi}{2^B}, \cdots, \frac{2\pi(2^B-1)}{2^B}\}$. When B approaches to infinity, the channel distribution approaches to the distribution assisted by RIS with continuous phase shifts. Similar to the CIPS, the DIPS reflection channel can be expanded as in (8) and (10). The mean and variance of the real part $\mu_{cos,DI}$ and $\sigma^2_{cos,DI}$ are expressed as

$$\mu_{cos,DI} = \mathbb{E}\{\cos(\phi_m + \alpha)\} = 0 \ , \quad (21)$$

$$\begin{aligned}\sigma^2_{cos,DI} &= \mathbb{E}\{\cos^2(\phi_m + \alpha)\} - \mu^2_{cos,DI} \\ &= \frac{1}{2} + \frac{1}{2}\mathbb{E}\{\cos(2\phi_m + 2\alpha)\} \\ &= \frac{1}{2} + \frac{1}{2}\cos(2\alpha)\mathbb{E}\{\cos(2\phi_m)\} - \frac{1}{2}\sin(2\alpha)\mathbb{E}\{\sin(2\phi_m)\},\end{aligned} \quad (22)$$

where the means of $\cos(2\phi_m)$ and $\sin(2\phi_m)$ determine $\sigma^2_{cos,DI}$. According to quantization bits B, there are two cases of $\sigma^2_{cos,DI}$.

1) $B \geq 2$: $\mathbb{E}\{\cos(2\phi_m)\} = 0$ and $\mathbb{E}\{\sin(2\phi_m)\} = 0$, which leads to $\sigma^2_{cos,DI} = \frac{1}{2}$. Therefore, same as CIPS, the channel is a complex Gaussian random variable with real and imaginary parts being same as in (13), that are, $\Re(\tilde{H}_{DI}) \sim N(0, \frac{M}{2})$ and $\Im(\tilde{H}_{DI}) \sim N(0, \frac{M}{2})$. The variance is the same as in (14) $\sigma^2_{DI} = M$.

2) $B = 1$: $\mu_{real,DI} = \mu_{imag,DI} = 0$. Different from $B \geq 2$ case, since ϕ_m only takes values $\{0, \pi\}$, $\mathbb{E}\{\cos(2\phi_m)\} = 1$ and $\mathbb{E}\{\sin(2\phi_m)\} = 0$. Thus, according to (22), the real and imaginary parts of $\widetilde{H}_{DI}$ can be expressed as

$$\begin{aligned}\Re(\tilde{H}_{DI}) &\sim N(0, \frac{M}{2} + \frac{1}{2}\sum_{m_y=1}^{M_y}\sum_{m_x=1}^{M_x}\cos(2\alpha)) \ , \\ \Im(\tilde{H}_{DI}) &\sim N(0, \frac{M}{2} - \frac{1}{2}\sum_{m_y=1}^{M_y}\sum_{m_x=1}^{M_x}\cos(2\alpha)) \ .\end{aligned} \quad (23)$$

The real and imaginary parts of $\widetilde{H}_{DI}$ are correlated, with covariance $\mathbf{R}_{DI}$ expressed as

$$\begin{aligned}\mathbf{R}_{DI} &= \mathbb{E}\{\sum_{m_y=1}^{M_y}\sum_{m_x=1}^{M_x}\cos(\phi_m + \alpha)\sin(\phi_m + \alpha)\} \\ &= \sum_{m_y=1}^{M_y}\sum_{m_x=1}^{M_x}\frac{1}{2}\sin(2\alpha) \ .\end{aligned} \quad (24)$$

The real and imaginary parts are independent when $\mathbf{R}_{DI} = 0$. Assume $m_x = m_y$ and $d_x = d_y$, which is a typical configuration of URA RIS. Then, $\mathbf{R}_{DI} = 0$ when the following condition is satisfied

$$\gamma = \frac{b\pi}{2kd_x} \ , b \in \mathbb{Z} \ , \quad (25)$$

$$\gamma = \cos\psi_i \sin\theta_i + \cos\psi_o \sin\theta_o + \sin\psi_i \sin\theta_i + \sin\psi_o \sin\theta_o \ . \quad (26)$$

Additionally, the reflection channel variance is $\sigma^2_{DI} \leq M$. The less-equal sign is due to the covariance between the real and imaginary parts. When $\mathbf{R}_{DI} = 0$, 1-bit RIS provides the same variance. The magnitude and phase distributions for 1-bit DIPS can be turned into deriving the envelope and phase of correlated Gaussian quadratures according to [12].

IV. Secret Key Rate

SKR is the upper bound of the information bits per channel sample generated between Alice and Bob. Since when Eve is several wavelengths away from Alice and Bob, its channel is considered uncorrelated with the channel between Alice and Bob, which is tested in practical experiments [13]. The SKR can be expressed as

$$R_s = I(y_A; y_B|y_E) = I(y_A; y_B) \ , \quad (27)$$

where y_A, y_B, and y_E are the channels estimated by Alice, Bob, and Eve, respectively.

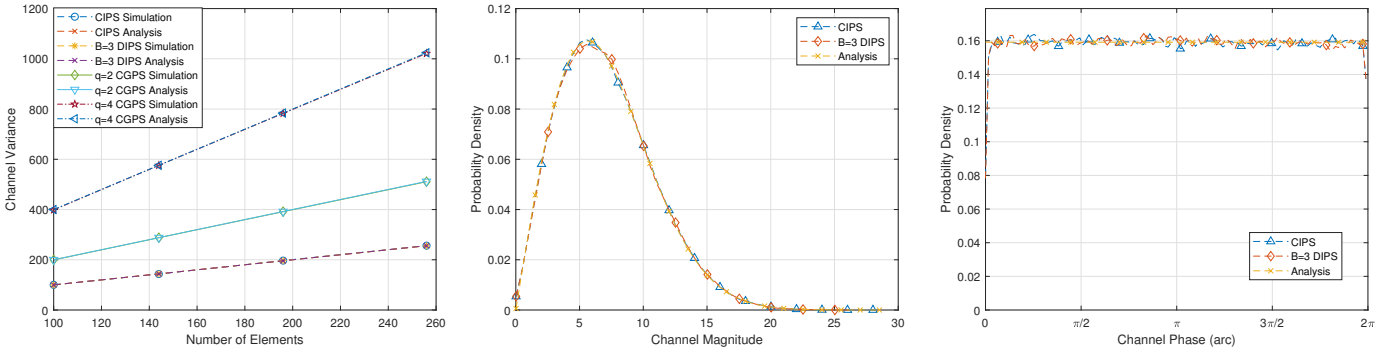
A. CIPS, CGPS, and $B \geq 2$ DIPS

The mutual information between y_A and y_B is determined by their variances. The direct channel adds a mean to the reflection channel, without influencing the variance. Therefore, based on the channel expressions in (1) and Section III-A, the SKR R_s for CIPS and $B \geq 2$ DIPS can be derived as

$$R_{s,CI} = \log_2(1 + \frac{M/2}{2\sigma_z^2 + \frac{2\sigma_z^4}{M}}) \ , \quad (28)$$

where σ_z^2 is the noise power.

The SKR for CGPS can be calculated as (28) by substituting $\sigma^2_{CI} = M$ by $\sigma^2_{CG} = Nq^2$.



(a) Variance when RIS has different element number. (b) Magnitude distribution. (c) Phase distribution.

Fig. 2: The channel variance of CIPS, $q = 2, 4$ CGPS, and $B = 3$ DIPS. The magnitude distribution and phase distribution of the CIPS and $B = 3$ DIPS.

B. $B = 1$ *DIPS*

The estimated SKR under $B = 1$ DIPS can be expressed as

$$\begin{aligned} R_{s,DI} &\leq \{I(\Re(y_A);\Re(y_B)) + I(\Im(y_A);\Im(y_B))\} \\ &= \log_2\{(1+\frac{\sigma^2_{real,DI}}{2\sigma_z^2 + \frac{\sigma_z^4}{\sigma^2_{real,DI}}})(1+\frac{\sigma^2_{imag,DI}}{2\sigma_z^2 + \frac{\sigma_z^4}{\sigma^2_{imag,DI}}})\}, \end{aligned} \tag{29}$$

where $\sigma^2_{real,D,I}$ and $\sigma^2_{imag,D,I}$ are the variances of the real and imaginary parts in (23). The less-than sign is because in (24), the 1-bit DIPS RIS channel real and imaginary parts are correlated. The sign takes eqivalence when the real and imaginary parts are independent taking the condition in (25).

V. Simulation Results

In this section, the analytical channel distributions, channel parameters, and SKR for CIPS, CGPS, and DIPS are verified by simulations.

A. Verification for CIPS and CGPS Channel

Element spacing is set to $d = \frac{\lambda}{2}$. Incident and reflection angles are set as $\boldsymbol{\Omega_i} = (30°, 30°)$, and $\boldsymbol{\Omega_o} = (150°, 60°)$. For CGPS, set group size $q = 2, 4$.

1) Channel Variance: The simulation for the reflection channel variance with respect to M is plotted in Fig. 2(a). The simulation results match analytical results in (14) (20). The variance means the RIS has a great potential to induce channel variation since it is usually implemented with a huge number of elements. The variance for the CGPS is larger than the CIPS, and $q = 4$ CGPS variance is larger than $q = 2$ CGPS because the variance increases quadratically with q.

2) Magnitude and Phase Distributions: Set $M = 64$, with $M_x = M_y = 8$. The magnitude and phase distributions for CIPS are presented in Fig. 2(b) and Fig. 2(c), respectively. The magnitude and phase distribution simulation results match the analytical results. The magnitude and phase are a Rayleigh distribution and a uniform distribution being independent of $\boldsymbol{\Omega}_i$ and $\boldsymbol{\Omega}_o$, respectively. The independence of $\boldsymbol{\Omega}_i$ and $\boldsymbol{\Omega}_o$ means that whatever angles Alice and Bob locate in, the channel randomness remains the same. Note that the sharp drops around 0 and 2π in Fig. 2(c) result from several adjacent probability density values outside the bound $[0, 2\pi)$, being equal to 0, are averaged to plot a smoother p.d.f. Additionally, the channel distribution Eve receives stays unchanged, and no more information leakage dependent on angles. Note that if Eve locates at the same angle as Bob[2], the information is fully leaked. This is because, in the far-field environment, Eve and Bob are differentiated by their locating angles. The uniform phase distribution means that the values in $[0, 2\pi)$ are taken with equal probability. Thus, when CSI is utilized to generate keys, it greatly prevents Eve from guessing the particular phase of the channel between Alice and Bob.

B. Verification for DIPS

1) RIS Weight $B \geq 2$: Set $B = 3$. Other parameters remain the same as the continuous case. The simulations for the variance, magnitude, and phase of the reflection channel are plotted in Fig. 2(a), Fig. 2(b), and Fig. 2(c). The simulation results are the same as the ideal CIPS. This means that the ideal channel distribution and uniform phase distribution can be achieved in a more practical situation.

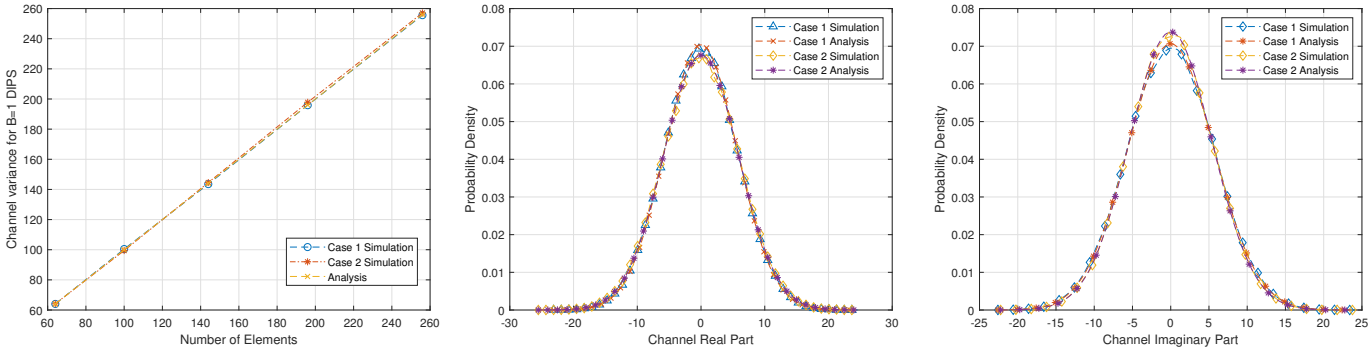
2) RIS Weight $B = 1$: Set $B = 1$, and two pairs of input and output angles, with case 1: $\boldsymbol{\Omega_i} = (30°, 30°)$, $\boldsymbol{\Omega_o} = (150°, 60°)$, and case 2: $\boldsymbol{\Omega_i} = (110°, 50°)$, $\boldsymbol{\Omega_o} = (310°, 20°)$. Other parameters are the same as continuous case. The simulation for the reflection channel variance is plotted in Fig. 3(a), where the variances increase linearly with respect to M.

The real and imaginary part of the reflection channel for two cases when $M_x = M_y = 8$ are plotted in Figure. 3(b) and Figure. 3(c), respectively. The simulation results match the analytical result in (23) well. the real and imaginary part distributions are dependent on values of $\boldsymbol{\Omega}_i$ and $\boldsymbol{\Omega}_o$.

C. Secret Key Rate

The RIS element number is set to $M = 64$. The *Information Theoretical Estimators (ITE) Toolbox* is used to simulate the

[2]The situation Eve locates at the same angle as Bob do not happen in most cases.



(a) Variance when RIS has different element number. (b) Real part distribution. (c) Imaginary part distribution.

Fig. 3: The variance, real part distribution and imaginary part distribution of the channel assisted by $B = 1$ DIPS RIS.

mutual information [14]. The SKR for CIPS, $q = 2$ CGPS, $B = 2$ DIPS, and $B = 1$ DIPS against signal-to-noise ratio (SNR) are plotted in Fig. 4. The simulation results match the analytical results in (28) and (29). The CGPS SKR is larger than the individual shifting.

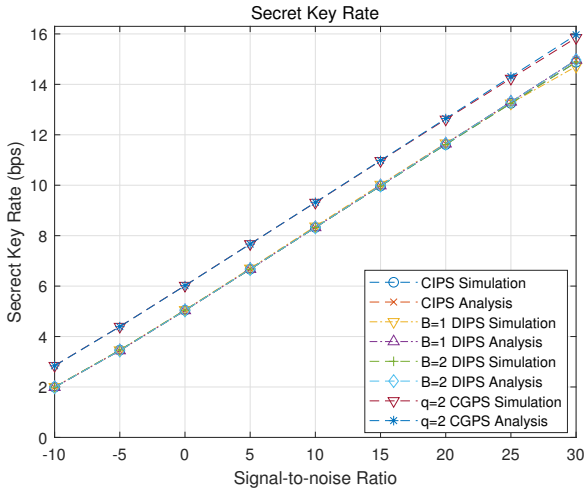


Fig. 4: Secret key rate when RIS is CIPS, $q = 2$ CGPS, $B = 2$ DIPS, and $B = 1$ DIPS.

VI. Conclusions

In this paper, we utilize RIS for mmWave physical layer security secret key generation, and completes the underlying mathematical principles by deriving the channel distribution. Though mmWave static channels lack randomness and multi-path, the RIS can induce an artificial Rayleigh/Rician fading randomness, without adding transceiver costs. Specifically, based on the RIS-assisted secret key generation model, we consider RIS weights have CIPS, CGPS, and DIPS to produce artificial channel randomness. We derive the channel distribution and its parameters. The CGPS is able to produce more randomness at legal parties Alice and Bob, compared to individual shifting. The DIPS channel distribution is dependent on the quantization bit. The SKR for the above RIS settings is derived to evaluate the performance. Our theoretical conclusions are verified by simulations. While this work focuses more on the channel between Alice and Bob, the detailed analysis of leakage to eavesdroppers and DGPS will be our future work.

References

[1] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical Layer Security for the Internet of Things: Authentication and Key Generation," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 92–98, 2019.

[2] 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.

[3] A. M. Al-samman, M. H. Azmi, and T. A. Rahman, "A Survey of Millimeter Wave (mm-Wave) Communications for 5G: Channel Measurement Below and Above 6 GHz," in *Recent Trends in Data Science and Soft Computing*, F. Saeed, N. Gazem, F. Mohammed, and A. Busalim, Eds. Cham: Springer International Publishing, 2019, pp. 451–463.

[4] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent Reflecting Surface Aided Wireless Communications: A Tutorial," *IEEE Transactions on Communications*, pp. 1–1, 2021.

[5] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, "Toward Smart Wireless Communications via Intelligent Reflecting Surfaces: A Contemporary Survey," *IEEE Communications Surveys Tutorials*, vol. 22, no. 4, pp. 2283–2314, 2020.

[6] Z. Ji, P. Lep Yeoh, G. Chen, C. Pan, Y. Zhang, Z. He, H. Yin, and Y. Li, "Random Shifting Intelligent Reflecting Surface for OTP Encrypted Data Transmission," *arXiv e-prints*, p. arXiv:2010.14268, Oct. 2020.

[7] X. Hu, L. Jin, K. Huang, X. Sun, Y. Zhou, and J. Qu, "Intelligent Reflecting Surface-Assisted Secret Key Generation With Discrete Phase Shifts in Static Environment," *IEEE Wireless Communications Letters*, vol. 10, no. 9, pp. 1867–1870, 2021.

[8] 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 *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2021, pp. 745–751.

[9] Q. Wu and R. Zhang, "Beamforming Optimization for Wireless Network Aided by Intelligent Reflecting Surface With Discrete Phase Shifts," *IEEE Transactions on Communications*, vol. 68, no. 3, pp. 1838–1851, 2020.

[10] Liu, Yihong and Zhang, Lei and Yang, Bowen and Guo, Weisi and Imran, Muhammad Ali, "Programmable Wireless Channel for Multi-user MIMO Transmission using Meta-surface," in *2019 IEEE Global Communications Conference*, 2019, pp. 1–6.

[11] H. Han, Y. Liu, and L. Zhang, "On Half-Power Beamwidth of Intelligent Reflecting Surface," *IEEE Communications Letters*, pp. 1–1, 2020.

[12] V. A. Aalo, G. P. Efthymoglou, and C. Chayawan, "On the Envelope and Phase Distributions for Correlated Gaussian Quadratures," *IEEE Communications Letters*, vol. 11, no. 12, pp. 985–987, 2007.

[13] S. Sun, H. Yan, J. MacCartney, George R., and T. S. Rappaport, "Millimeter Wave Small-Scale Spatial Statistics in an Urban Microcell Scenario," *arXiv e-prints*, p. arXiv:1703.08239, Mar. 2017.

[14] Z. Szabó, "Information Theoretical Estimators Toolbox," *Journal of Machine Learning Research*, vol. 15, pp. 283–287, 2014.

Reconfigurable intelligent surface-induced randomness for mmWave key generation

Yang, Shubo

2023-10-23

Yang S, Han H, Liu Y, et al., (2023) Reconfigurable intelligent surface-induced randomness for mmWave key generation. In ICC 2023-IEEE International Conference on Communications. 28 May - 01 June 2023, Rome, Italy, pp. 2909-2914

https://doi.org/10.1109/ICC45041.2023.10278950