Reconfigurable Intelligent Surface: Reflection Design Against Passive Eavesdropping

Junshan Luo, Fanggang Wang, *Senior Member, IEEE*, Shilian Wang, *Member, IEEE*, Hao Wang, and Dong Wang

***Abstract*— The reconfigurable intelligent surface (RIS) is envisioned to create ultra-secure wireless networks. Previous works on the RIS-assisted security provisioning techniques assumed wiretap channel information at the transmitter, which is practically unavailable in a passive eavesdropping scenario. In this article, we consider a point-to-point anti-eavesdropping system in which a RIS is used to enable the secure transmission from a multi-antenna transmitter to a multi-antenna legitimate receiver. A passive eavesdropper, whose channel state information is completely unknown, attempts to decode the secret messages. We propose a security approach by using the reflection at the RIS as multiplicative randomness against the wiretapper. Specifically, the reflection coefficients in terms of amplitude and phase are updated in each transmission and kept private at the RIS. Through the reflection designs, the effective channel matrix is diagonalized at the legitimate receiver. In contrast, the eavesdropper receives coupled signals with the weights of the randomness at RIS. The main contributions of this article are three reflection designs and correspondingly three secure transmission schemes, which fulfills diverse requirements of the balance amongst performance metrics including the degrees of randomness, spectral efficiency, and reliability. The main benefits of the proposed secure transmission schemes are four-fold. First, the transmitter does not need to know the eavesdropper's channel states. Second, closed-form solutions for the reflection coefficients are provided. Third, the legitimate receiver has a linear decoding complexity. Fourth, the unauthorized wiretapper is unable to cancel out the multiplicative randomness and thus cannot extract much useful information. Numerical results show that exploiting the RIS as a source of multiplicative randomness provides a new perspective to improve the security of the wireless networks.**

***Index Terms*— Multiplicative interference, passive eavesdropper, physical layer security, reconfigurable intelligent surface.**

Manuscript received March 9, 2020; revised June 9, 2020, August 21, 2020, and November 15, 2020; accepted December 29, 2020. Date of publication January 18, 2021; date of current version May 10, 2021. This work was supported in part by the National Key Research and Development Program of China under Grant 2020YFB1806903, in part by the National Natural Science Foundation under Grant U1834210, in part by the State Key Laboratory of Rail Traffic Control and Safety under Grant RCS2019ZT011, and in part by the Research Plan Program of National University of Defense Technology under Grant ZK20-40. The associate editor coordinating the review of this article and approving it for publication was T. Q. Duong. *(Corresponding authors: Fanggang Wang; Shilian Wang.)*

Junshan Luo, Shilian Wang, and Hao Wang are with the College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China (e-mail: ljsnudt@foxmail.com; wangsl@nudt.edu.cn; wanghao08@nudt.edu.cn).

Fanggang Wang and Dong Wang are with the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China (e-mail: wangfg@bjtu.edu.cn; 17111034@bjtu.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TWC.2021.3049312.

Digital Object Identifier 10.1109/TWC.2021.3049312

I. Introduction

THE continuing growth of security-sensitive wireless applications will be demanding a hyper-secured wireless network in the future. Cryptographic methods are effective solutions at higher layers of the protocol stack. However, the advancement of powerful computing technologies and the growing of wireless devices are challenging the cryptographic approaches. Recently, as pointed out in [1], the strongest security protection may be achieved at the physical layer. In particular, the physical-layer security techniques exploit the randomness of the wireless channels to safeguard the confidentiality of the transmission. In this article, we introduce a reconfigurable intelligent surface (RIS)-based solution for wireless networks to achieve physical-layer security.

The concept of RIS has received considerable attention due to its appealing ability to customize the propagation of the electromagnetic waves [2], [3]. Specifically, the RIS is a massive integration of passive and reflecting units, each of which can independently tune the incident signal in terms of amplitude and phase, and reflect it in a full-duplex manner. Compared to the contemporary relaying techniques, the RIS has two main advantages. First, the RIS is a passive device that avoids power-hungry radio frequency processing and thus consumes much less energy to perform the reflection. Second, the RIS can be integrated on a thin and light-weight film and thus is allowed to easily mount on various environmental objects, such as street signs, building facades, and advertisement boards, which enables the previously uncontrollable communication participants to assist in the transmission collaboratively [4]. Furthermore, the reflection pattern of the RIS can also be explored to achieve the function of information transfer [5]–[7].

Using RIS to enhance physical-layer security is one of the emerging applications. The aim is to leverage the extra spatial degrees of freedom, provided by the reflection of the RIS, to improve the secrecy rate. In particular, multiple-input single-output single-eavesdropper (MISOSE) systems with the assistance of RIS were considered in [8]–[12], while [13] focused on a multiple-input multiple-output multiple-eavesdropper system. The beamforming vector at the transmitter and the phase shifts of the RIS were collectively designed to maximize the secrecy rate subject to the transmit power constraint, or to minimize the transmit power subject to the secrecy rate constraint [12]. Due to the non-convexity and coupled variables of the optimization problem, semidefinite relaxation and

alternating optimization were employed to iteratively solve for suboptimal solutions. In contrast to the assumption adopted in [8]–[12] that the RIS has continuous phase shifts, the authors of [13] also investigated the scenario where the reflecting elements take discrete phase shifts. Incorporating artificial noise (AN) at the transmitter was studied in a multiple-input single-output multiple-eavesdropper system [14], [15]. Specifically, the work in [14] formulated the problem as a joint design of transmit beamforming with AN and phase shifts at the RIS to maximize the secrecy rate. The problem was solved by an alternating optimization again, and the results revealed that consuming additional power to send jamming signals was beneficial for improving the secrecy performance especially when the number of eavesdroppers is large. In [15], the maximization of the minimum secrecy rate among several single-antenna legitimate receivers was investigated. In contrast to [14], the optimization was performed in terms of both amplitudes and phases of the reflecting units. A key assumption for the secrecy rate maximization in [8]–[15] was that the transmitter knows the channel state information (CSI) of the wiretap channels perfectly. Considering the imperfect CSI of the eavesdropper, the authors of [16] proposed a robust scheme, in which the system sum-rate was optimized subject to the constraint of maximum information leakage to unintended receivers. However, it is usually difficult to obtain the eavesdropper's CSI, especially when a passive listener tries to hide its existence from the network. Furthermore, as the transmitted power grows, the eavesdropper is more likely to extract useful information and thus the secrecy is vulnerable.

As a response to the aforementioned problems, in this article, we propose an anti-eavesdropping system in which a multi-antenna transmitter communicates secretly to a multi-antenna legitimate receiver with the assistance of a RIS. A potential malicious listener overhears the transmission and attempts to decode the confidential information. We assume the listener does not interact with other nodes in the systems, and thus the CSI of the wiretap channel is unknown. We address the security issues by using the reflection at the RIS as multiplicative randomness against the eavesdropper. In particular, the reflection coefficients are updated in each transmission and kept private at the RIS, while guaranteeing that the effective channel matrix observed at the authorized receiver is diagonalized. In contrast, the eavesdropper receives coupled signals with the weights of the randomness at RIS. This random reflection enables the secret information to be reliably recovered at the legitimate user while being undecodable at the wiretapper.

More explicitly, we provide three reflection designs and correspondingly three secure transmission schemes. The first scheme is based on diagonalizing the legitimate channel matrix and using the indices of the transmit antennas to convey confidential messages, i.e., the space-shift keying (SSK) modulation. Since the legitimate channel matrix is diagonalized, the carrier signal sent from one of the transmit antennas can be observed at the paired receive antenna only, of which the index is then used to recover data bits. The detection, therefore, does not rely on the exact knowledge of the channel responses. Based on channel diagonalization, the second scheme enforces the diagonal elements of the equivalent legitimate channels to take real values, and a quadrature space-shift keying (QSSK) modulation is employed for information transmission. Similarly, the demodulation of the QSSK symbols does not require the knowledge of the channels. Finally, the third scheme further converts the diagonal elements into positive real numbers, and the secret bits are modulated into multiple phase-shift keying (PSK) symbols. Since the legitimate channel matrix is diagonal with the diagonal elements being positive real numbers, all the transmitter-receiver links incur no phase changes to the ongoing signals. Thus, the PSK symbols can be detected non-coherently.

Compared to the current RIS-enabled security provisioning techniques, the proposed secure transmission schemes have four main advantages. First, the transmitter does not need to know the CSI of the wiretap channel at all. Previous works for maximizing the secrecy rate are based on the availability of the eavesdropper's CSI. However, this idealized assumption is usually invalid when the eavesdropper is a passive listener and the transmitter might be even unaware of its existence. Second, closed-form solutions for the reflection coefficients are provided. For an energy-constrained wireless network with low computational capability, closed-form solutions might be more desirable than iteratively optimized solutions. Third, the authorized receiver does not require any channel knowledge and has a linear decoding complexity. The diagonalization of the legitimate channel matrix significantly reduces the decoding complexity at the receiver side by allowing simple non-coherent detection. Fourth, the eavesdropper is unable to cancel out the multiplicative randomness even at high signal-to-noise ratio (SNR). The conventional additive randomness, such as the AN methods, is power-inefficient due to the emission of additional artificial interference. The security is vulnerable if the additive randomness is weaker than the useful signals. In contrast, the multiplicative randomness distorts the received signals via attenuation and phase shifting, which does not rely on extra power and thus is a good choice for the RIS. It has been demonstrated in [17] that the multiplicative noise can provide satisfactory secrecy performance in MISOSE channels. The main contributions of this article are

- *Principle:* The reflection coefficients of the RIS have been designed as multiplicative randomness against a passive eavesdropper. The secrecy is achieved by diagonalizing the legitimate channel matrix while leaving the wiretap channel intractable. Neither full nor partial CSI of the eavesdropper is required at the transmitter.
- *Approach:* We provide three reflection designs with closed-form solutions and correspondingly three secure transmission schemes, which fulfills diverse requirements of the balance amongst performance metrics including the degree of randomness (DoR), spectral efficiency, and reliability. Moreover, the legitimate receiver has a linear decoding complexity.
- *Evaluation:* The secrecy rate, bit-error-rate (BER), and DoR are analyzed to characterize the secrecy performances of the proposed schemes. We also provide numerical results to validate the analysis and make

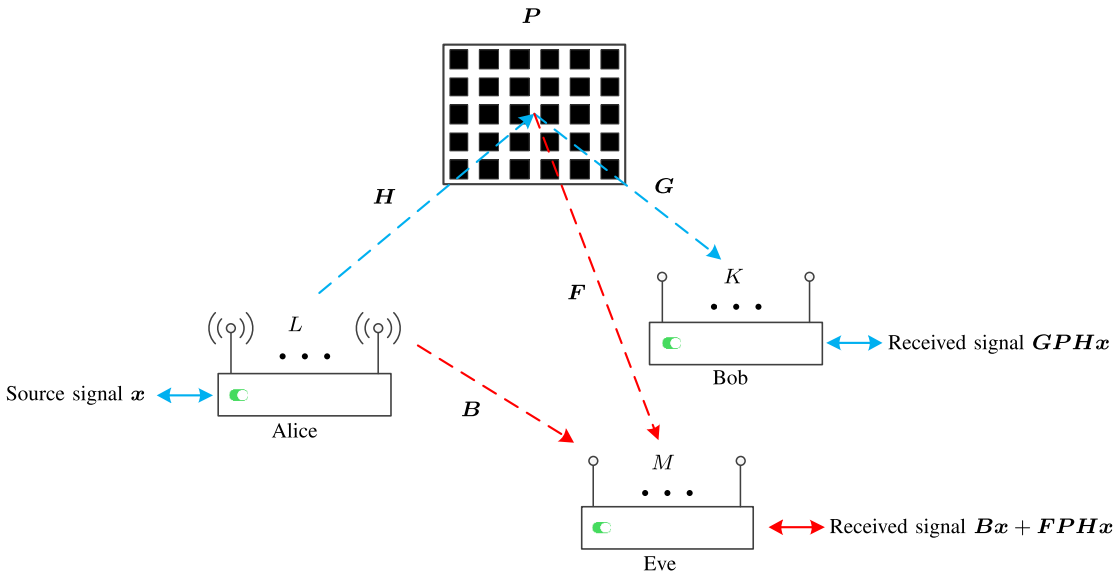


Fig. 1. RIS-enabled secure communication scheme.

comparison with the beamforming and artificial noise schemes.

The remainder of this article is organized as follows: Section II introduces the problem description of a RIS-enabled secure communication scheme. Reflection coefficients and transceiver architectures design are studied in Section III. Section IV focuses on the BER analyses. Numerical results are presented in Section V. Finally, Section VI concludes this article.

Notation: Variables, vectors, and matrices are written as italic letters x, bold italic letters $\boldsymbol{x}$, and bold capital italic letters $\boldsymbol{X}$, respectively. For any vector $\boldsymbol{x}$, $\mathrm{diag}\{\boldsymbol{x}\}$ denotes a diagonal square matrix whose diagonal consists of the elements of $\boldsymbol{x}$; $\dim\{\boldsymbol{x}\}$ denotes the dimension of the vector. For any square matrix $\boldsymbol{X}$, $[\boldsymbol{X}]_{\mathrm{diag}}$ denotes a diagonal square matrix formed by the diagonal elements of $\boldsymbol{X}$. The operators $\mathbb{E}$, $\mathbb{E}_{\boldsymbol{x}}$, $\mathrm{Tr}[\cdot]$, $(\cdot)^{\mathrm{T}}$, $(\cdot)^{\dagger}$, $(\cdot)^{-1}$, $\|\cdot\|$, and $\|\cdot\|_{\infty}$ denote the expectation with respect to all the randomness, the expectation with respect to $\boldsymbol{x}$, the trace, the transpose, the Hermitian, the inverse, the Frobenius norm, and the infinity norm of their arguments, respectively. $\odot$ is the Hadamard product. $p(A)$ denotes the probability of the event A. Define $\mathcal{I}_N = \{1, 2, \ldots, N\}$ as a shorthand as the index set. $\boldsymbol{I}_k$ and $\boldsymbol{0}_k$ denote the k-by-k identity and zero matrices, respectively. The default base of the logarithm is 2.

II. Problem Description

In this section, we first introduce the system model of a RIS-enabled secure communication scheme. Then, a RIS reflection coefficients design problem is formulated.

A. System Model

The system model is illustrated in Figure 1. We consider a wireless transmission system, which includes a transmitter (Alice) with L antennas, a legitimate receiver (Bob) with K antennas, and a passive eavesdropper (Eve) with M antennas. We assume $L \geq K \geq 2$. A RIS with N reflecting elements is deployed to guarantee the secure transmission from Alice to Bob by properly adjusting the reflection coefficients in terms of amplitude and phase. Assume that the direct links from Alice to Bob are blocked.[1] Thus, each transmission consists of two stages. In the first stage, Alice transmits the signals to the RIS. In the second stage, the RIS manipulates the amplitudes and the phases of the incident signals, which reach Bob and Eve, respectively.

Let the matrices $\boldsymbol{H} = [\boldsymbol{h}_1, \ldots, \boldsymbol{h}_L] \in \mathbb{C}^{N \times L}$, $\boldsymbol{B} \in \mathbb{C}^{M \times L}$, $\boldsymbol{G} \in \mathbb{C}^{K \times N}$, and $\boldsymbol{F} \in \mathbb{C}^{M \times N}$ be the channel responses from Alice to the RIS, from Alice to Eve, from the RIS to Bob, and from the RIS to Eve, respectively. We assume that $\boldsymbol{H}$ and $\boldsymbol{G}$ are perfectly known to Alice and unknown to Bob.[2] Since Eve does not provide any information about her channel, the channels $\boldsymbol{F}$ and $\boldsymbol{B}$ are completely unknown to the legitimate communication parties. We assume that Eve knows the perfect knowledge of $\boldsymbol{B}$ and performs maximum-likelihood detection based on $\boldsymbol{B}$. We further assume that Eve is unaware of $\boldsymbol{F}$ due to the following reasons. First, the RIS will not reveal any public signal to Eve. Second, the reflection coefficients of the RIS are always varying and thus it is a challenging task for Eve to track $\boldsymbol{F}$. Third, we may use secret channel estimation methods [18] to protect the legitimate channel information. Let $\boldsymbol{P} = \mathrm{diag}\{\boldsymbol{p}\} \in \mathbb{C}^{N \times N}$ denote a diagonal matrix,

[1]The existence of the direct link will result in a different system model. For example, in the relay systems, the direct links were considered in [33], [34], while the works [35], [36] assumed the absence of the direct links. If the direct link exists, the effective legitimate channel would not be a diagonal matrix because the direct channel is a full matrix and the reflected channel is a diagonal matrix. That is, the signals sent by one transmit antenna can be observed at all receive antennas. Thus it requires new reflection designs to achieve the secure transmission.

[2]The channels $\boldsymbol{G}$ and $\boldsymbol{H}$ can be separately estimated at Alice via a two stage channel estimation method [19]. Although $\boldsymbol{G}$ and $\boldsymbol{H}$ may be ambiguously estimated as $\boldsymbol{G}'$ and $\boldsymbol{H}'$, i.e., $\boldsymbol{G}' \triangleq \boldsymbol{G}\boldsymbol{\Phi}$ and $\boldsymbol{H}' \triangleq \boldsymbol{\Phi}^{-1}\boldsymbol{H}$ with $\boldsymbol{\Phi}$ being a full-rank diagonal matrix, the proposed reflection designs are still valid since $\boldsymbol{G}\boldsymbol{P}\boldsymbol{H} = \boldsymbol{G}'\boldsymbol{P}\boldsymbol{H}'$. For more details, we refer the reader to [19].

in which the nth, $n \in \mathcal{I}_N$, diagonal element represents the reflection coefficient of the nth unit at the RIS. More explicitly, the vector $\boldsymbol{p}$ is written as

$$\boldsymbol{p} = \eta[r_1\ e^{\jmath\theta_1}, r_2\ e^{\jmath\theta_2}, \ldots, r_N e^{\jmath\theta_N}]^{\mathrm{T}} \tag{1}$$

where $\eta \in (0,1]$ denotes the the reflection efficiency; $\jmath \triangleq \sqrt{-1}$; $r_n \in [0,1]$ and $\theta_n \in [0, 2\pi]$ are the absorption coefficient and the phase shift of the nth reflecting unit, respectively. Then, the received signals at Bob and at Eve can be respectively expressed as

$$\boldsymbol{y} = \boldsymbol{GPHx} + \boldsymbol{\mu} \tag{2}$$

$$\boldsymbol{z} = \boldsymbol{Bx} + \boldsymbol{FPHx} + \boldsymbol{\nu} \tag{3}$$

where $\boldsymbol{x} \in \mathbb{C}^L$ is transmit signal of Alice; $\boldsymbol{y} \in \mathbb{C}^K$ and $\boldsymbol{z} \in \mathbb{C}^M$ are the received signals at Bob and at Eve, respectively; $\boldsymbol{\mu} \in \mathbb{C}^K$ and $\boldsymbol{\nu} \in \mathbb{C}^M$ are the noise vectors at Bob and at Eve, with independent and identically distributed (i.i.d.) samples following the circularly symmetric complex Gaussian (CSCG) distribution, denoted by $\mathcal{CN}(0, \sigma^2)$ and $\mathcal{CN}(0, \gamma^2)$, respectively.

B. Problem Formulation

Reflecting signals via a RIS introduces in additional spatial degrees of freedom which are absent in the current communication systems. Therefore, the RIS-enabled network benefits from substantial security-aware design flexibility by manipulating the amplitudes and the phases of the reflected signals. In particular, we aim to engineer the reflection coefficient matrix $\boldsymbol{P}$ at the RIS, such that the resultant legitimate channel matrix is diagonalized

$$[\boldsymbol{GPH}]_{:,1:K} = \boldsymbol{D} \tag{4}$$

where $[\boldsymbol{GPH}]_{:,1:K}$ denotes the first K columns of the matrix $\boldsymbol{GPH}$; $\boldsymbol{D} = \mathrm{diag}\{\alpha_1, \ldots, \alpha_K\}$ is a K-dimensional diagonal matrix. From (4) and the equality $\boldsymbol{P} = \mathrm{diag}\{\boldsymbol{p}\}$, the ith diagonal element can be written as

$$\alpha_i = \boldsymbol{p}^{\mathrm{T}}(\boldsymbol{g}_{i,:}^{\mathrm{T}} \odot \boldsymbol{h}_i), \quad i \in \mathcal{I}_K \tag{5}$$

where $\boldsymbol{g}_{i,:}$ denotes the ith row of $\boldsymbol{G}$. Intuitively, α_i is the equivalent channel gain from the ith transmit antenna of Alice to the ith receive antenna of Bob, and α_i can be designed as a complex number, a real number, or a positive real number, which is the main focus of the following work. Moreover, $\boldsymbol{P}$ should be randomly determined at the RIS, and kept secret from all other communication entities. Despite this challenging scenario for signal demodulation, we will show in the following section that the diagonalized legitimate channel matrix would assist Bob in reliably recovering the transmitted information.

In contrast, however, the reflected channel matrix of Eve, i.e., $\boldsymbol{FPH}$, is full and intractable. The elements of the channel matrix are intractable since the reflection coefficient matrix $\boldsymbol{P}$ is updated in each transmission and kept private at the RIS. Additionally, the wiretap channel matrix is full since $\boldsymbol{F}$ is different from $\boldsymbol{G}$ if Bob and Eve are apart from each other. Therefore, Eve cannot estimate the effective channel, even with blind estimation methods, and is prevented from reliably retrieving the confidential information. Next, we detail the reflection coefficients and the transceiver design, and illustrates the feasibility of the secure transmission.

III. RIS-Enabled Security Design

In this section, we introduce three RIS-enabled secure transmission schemes that are capable of resisting eavesdropping. Each scheme consists of the reflection strategy and the corresponding transceiver design.

A. RIS-Enabled Secure SSK Transmission: Scheme I

1) Reflection Coefficients Design: The aim is to find a reflection coefficient matrix $\boldsymbol{P}_{\mathrm{I}}$ which guarantees that $\boldsymbol{GP}_{\mathrm{I}}\boldsymbol{H}$ is a diagonal matrix. The problem can be formulated as

$$\boldsymbol{P}_{\mathrm{I}} = \arg\{\boldsymbol{P} | \|[\boldsymbol{GPH}]_{:,1:K} - [[\boldsymbol{GPH}]_{:,1:K}]_{\mathrm{diag}}\|^2 = 0\} \tag{6}$$

where the constraint enforces the squared sum of the off-diagonal elements in $[\boldsymbol{GP}_{\mathrm{I}}\boldsymbol{H}]_{:,1:K}$ to be zero, hence completing the diagonalization. Substituting the equality $\boldsymbol{P}_{\mathrm{I}} = \mathrm{diag}\{\boldsymbol{p}_{\mathrm{I}}\}$ into (6) yields

$$\|[\boldsymbol{GP}_{\mathrm{I}}\boldsymbol{H}]_{:,1:K} - [[\boldsymbol{GP}_{\mathrm{I}}\boldsymbol{H}]_{:,1:K}]_{\mathrm{diag}}\|^2 = \boldsymbol{p}_{\mathrm{I}}^{\dagger}\boldsymbol{W}\boldsymbol{p}_{\mathrm{I}} \tag{7}$$

where the matrix $\boldsymbol{W} \in \mathbb{C}^{N\times N}$ is given by

$$\boldsymbol{W} = \sum_{\substack{i,j=1 \\ i\neq j}}^{K} (\boldsymbol{g}_{j,:} \odot \boldsymbol{h}_i^{\mathrm{T}})^{\dagger}(\boldsymbol{g}_{j,:} \odot \boldsymbol{h}_i^{\mathrm{T}}). \tag{8}$$

Therefore, the constraint in problem (6) can be converted into

$$\boldsymbol{p}_{\mathrm{I}}^{\dagger}\boldsymbol{W}\boldsymbol{p}_{\mathrm{I}} = 0 \tag{9}$$

and the solutions of $\boldsymbol{p}_{\mathrm{I}}$ are in the null space of $\boldsymbol{W}$. The orthonormal basis of the null space of $\boldsymbol{W}$ denoted as $\boldsymbol{U} \in \mathbb{C}^{N\times(N-K^2+K)}$ here can be obtained by the singular value decomposition:

$$\boldsymbol{W} = [\boldsymbol{S}\ \ \boldsymbol{U}]\boldsymbol{\lambda}\boldsymbol{V}^{\dagger} \tag{10}$$

where $\boldsymbol{V} \in \mathbb{C}^{N\times N}$ is the right singular matrix; $\boldsymbol{S} \in \mathbb{C}^{N\times(K^2-K)}$ and $\boldsymbol{U}$ contain the first K^2-K columns and the last $N-K^2+K$ columns of the left singular matrix, respectively. The solution to (9) is then a linear combination of the columns of $\boldsymbol{U}$ and can be written as

$$\boldsymbol{p}_{\mathrm{I}} = \frac{\eta\boldsymbol{U}\boldsymbol{a}_{\mathrm{I}}}{\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{I}}\|_{\infty}} \tag{11}$$

where $\boldsymbol{a}_{\mathrm{I}} \in \mathbb{C}^{N-K^2+K}$ is a random linear combination vector. To avoid trivial cases, we assume $\boldsymbol{a}_{\mathrm{I}} \neq \boldsymbol{0}$. Note that the denominator $\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{I}}\|_{\infty}$ is incorporated to ensure that the maximum reflection gain is η since the passive units integrated on the RIS are not supposed to intensify the impinging signals. From (11), the reflection coefficients of the RIS are obtained. Next, we provide the definition of DoR as follows to characterize the level of randomness.

Definition 1: The DoR is the number of free parameters in a vector $\boldsymbol{a}$ that are available for the RIS to generate the reflection coefficients. If $\boldsymbol{a}$ is a complex vector

$$\mathsf{DoR} = 2\mathrm{dim}\{\boldsymbol{a}\} \tag{12}$$

and if $\boldsymbol{a}$ is a real vector

$$\mathsf{DoR} = \dim\{\boldsymbol{a}\}. \tag{13}$$

Remark 1: Since $\boldsymbol{a}_{\mathrm{I}}$ in (11) is a complex vector which has $N - K^2 + K$ elements, we have

$$\mathsf{DoR} = 2(N - K^2 + K). \tag{14}$$

2) Transceiver Design: Since the random vector $\boldsymbol{a}_{\mathrm{I}}$ is determined at the RIS only, the reflection coefficient matrix $\boldsymbol{P}_{\mathrm{I}}$ remains unknown to other communication parties, leading to a one-time pad system and intractable channel responses at Bob and at Eve, respectively. Since the diagonal elements are unknown complex numbers, common signaling techniques such as the quadrature amplitude modulation (QAM) and PSK cannot be used in this case. However, as the Alice-to-Bob channels are diagonalized via the reflection of the RIS, Alice's transmit antennas and Bob's receive antennas are one-to-one paired. That is, the signals sent from one transmit antenna will be received by the paired receive antenna only. Therefore, the secret messages can be modulated into the index of an active transmit antenna, which can be detected by comparing the power profiles of the received signals. This digital modulation technology is called SSK [22], thus we name the proposed scheme as RIS-enabled secure SSK transmission. At the legitimate receiver, the demodulation can be completed by comparing the signal powers observed at the receive antennas, which does not require the knowledge of the channel responses. However, Eve cannot identify the active transmit antenna since Alice-to-Eve channels are full and intractable. Next, we detail the transceiver design for realizing secure transmission between Alice and Bob.

At the transmitter, a group of $\log K$ bits is mapped into the index of a single transmit antenna, which is then switched on to send an unmodulated carrier signal while all the other antennas being idle. Specifically, assume the ith transmit antenna is activated, which is determined by converting the $\log K$ binary bits into a decimal number. The transmit signal of Alice is given by

$$\boldsymbol{x}_{\mathrm{I}} = [\boldsymbol{e}_i^{\mathrm{T}},\ \boldsymbol{0}^{\mathrm{T}}]^{\mathrm{T}}, \quad i \in \mathcal{I}_K \tag{15}$$

where $\boldsymbol{e}_i$ is the ith column of the K-dimensional identity matrix. Upon receiving the signals from Alice, the RIS reflects the signals and then the reflected signals reach the receivers. In particular, the received signals at Bob are

$$\boldsymbol{y}_{\mathrm{I}} = \boldsymbol{D}_{\mathrm{I}}\boldsymbol{e}_i + \boldsymbol{\mu} \tag{16}$$

$$= \alpha_{\mathrm{I},i}\boldsymbol{e}_i + \boldsymbol{\mu} \tag{17}$$

where $\boldsymbol{D}_{\mathrm{I}} \triangleq \boldsymbol{G}\boldsymbol{P}_{\mathrm{I}}\boldsymbol{H}$ is the effective channel from Alice to Bob;[3] (17) follows that $\boldsymbol{D}_{\mathrm{I}}$ is a diagonal matrix with the ith diagonal element being $\alpha_{\mathrm{I},i}$, i.e., $\boldsymbol{D}_{\mathrm{I}} = \mathrm{diag}\{\alpha_{\mathrm{I},1}, \ldots, \alpha_{\mathrm{I},K}\}$. From (17), Bob can readily recover the secret messages by performing a simple non-coherent detection to estimate the index of the active antenna

$$\hat{i} = \arg\max_i |y_{\mathrm{I},i}|^2 \tag{18}$$

where $y_{\mathrm{I},i}$ is the ith element of $\boldsymbol{y}_{\mathrm{I}}$. This non-coherent detection has a complexity of $O(K)$, which scales linearly with the number of transmit/receive antennas. The transceiver procedure within one transmission frame between the legitimate communication parties is outlined as **Scheme I**.

Scheme I RIS-Enabled Secure SSK Transmission

1: Alice calculates the matrix $\boldsymbol{W}$ via (8), and performs singular value decomposition on $\boldsymbol{W}$ to identify $\boldsymbol{U}$, which is then conveyed to the RIS;[4]
2: Alice activates a single transmit antenna to send an unmodulated carrier signal according to the input data bits;
3: The RIS generates a random vector $\boldsymbol{a}_{\mathrm{I}}$ and calculates the reflection coefficients with (11);
4: Bob receives the signals reflected by the RIS and decodes the SSK symbol using (18), i.e., identifying the index of the antenna that receives the unmodulated carrier signal;

On the other hand, the reflected signals received at Eve are $\boldsymbol{F}\boldsymbol{P}_{\mathrm{I}}\boldsymbol{H}\boldsymbol{x}_i$, where the resultant channel $\boldsymbol{F}\boldsymbol{P}_{\mathrm{I}}\boldsymbol{H}$ prevents Eve from accurately estimating the index of the active transmit antenna. The reasons are two-fold. First, since $\boldsymbol{F}$ is different from $\boldsymbol{G}$, $\boldsymbol{F}\boldsymbol{P}_{\mathrm{I}}\boldsymbol{H}$ is a full matrix, which means the existence of crosstalk, i.e., signals sent from one transmit antenna will be observed at all the receive antennas. For a more clear illustration, the reflected signals received at Bob and Eve are presented in Figure 2, where we consider a wiretap system with $L = 2$, $K = 2$, $M = 2$, $N = 5$, and the SNR is 30 dB for both receiver ends. Each SSK symbol delivers a single bit. In Figure 2, the red dots and blue dots represent the received signals when Alice activates transmit antennas $\#1$ and $\#2$ to convey bits 0 and 1, respectively. From Figure 2(a), we observe that the received constellations are clearly distinguishable at the two antennas of Bob. For instance, concerning the red dots in Figure 2(a), the signal powers at receive antenna $\#1$ tend to be stronger than that at receive antenna $\#2$, which indicates that the active transmit antenna can be identified by comparing the received signal powers. In contrast, Figure 2(b) shows Eve's reception is completely messed up and thus is unable to perform the power-domain non-coherent detection. Second, since $\boldsymbol{P}_{\mathrm{I}}$ is updated at the RIS in each transmission, the resultant channel $\boldsymbol{F}\boldsymbol{P}_{\mathrm{I}}\boldsymbol{H}$ also randomly varies in each

[3]The effective channel gains can be very low in some cases. As such, Bob may predefine a threshold, which determines the minimum required power to detect the active antenna. If the maximum received power is below the threshold, Bob may feedback to Alice and then Alice re-transmits the previous signal to Bob. During the re-transmission period, the RIS re-generates a new set of random reflection coefficients. As such, the effective channel matrix is updated and very low channel gains may be avoided.

[4]Note that the RIS is controlled by the signals sent from Alice and a field programmable gate array-based controller in itself. We assume a block-fading channel model, in which $\boldsymbol{H}$ and $\boldsymbol{G}$ stay constant within a transmission block. The channel coherence time can be long when the RIS is used to serve a low-mobility user [28]–[32]. Therefore, the channel estimation and the transmission of $\boldsymbol{U}$ do not have to be performed very often. However, the vector $\boldsymbol{a}$ can be randomly generated in each transmission, which renders the wiretap channel intractable and hence guarantees the security. Moreover, if there exists a secret link between the RIS and Alice, it is also possible to let Alice generate $\boldsymbol{a}$ and calculate the reflection coefficient vector $\boldsymbol{p}$. In this case, the transmission of $\boldsymbol{U}$ is removed and the backhaul information can be reduced.

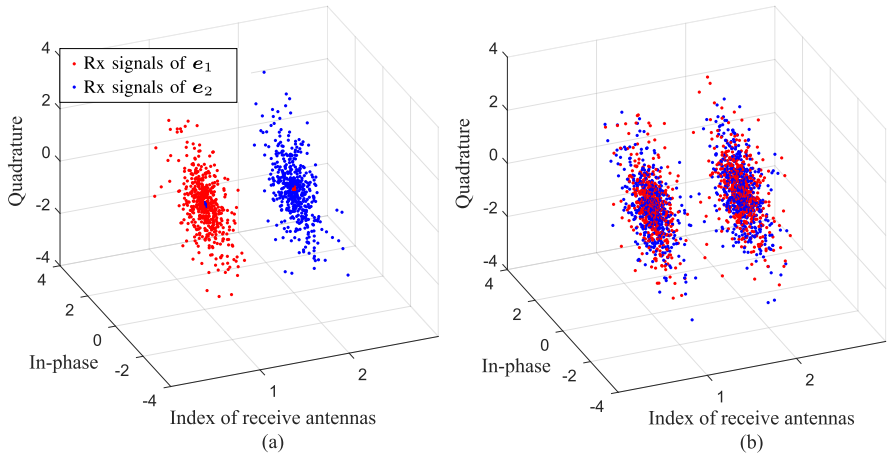


Fig. 2. Reflected signals received at (a) Bob and (b) Eve, with $L = 2$, $K = 2$, $M = 2$, and $N = 5$. The red dots and blue dots represent the received signals when Alice transmits the SSK symbols $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$, respectively. The comparison between (a) and (b) shows Bob is more likely to correctly estimate the index of the active transmit antenna than Eve.

transmission. Thus, the coherent detection is also unavailable for Eve.

B. RIS-Enabled Secure QSSK Transmission: Scheme II

1) Reflection Coefficients Design: The objective is to find a reflection coefficient matrix $\boldsymbol{P}_{\mathrm{II}}$ which guarantees that $\boldsymbol{G}\boldsymbol{P}_{\mathrm{II}}\boldsymbol{H}$ is a diagonal matrix with all diagonal elements being real numbers. This problem can then be formulated as

$$\boldsymbol{P}_{\mathrm{II}} = \arg\{\boldsymbol{P} \mid \|[\boldsymbol{G}\boldsymbol{P}\boldsymbol{H}]_{:,1:K} - [[\boldsymbol{G}\boldsymbol{P}\boldsymbol{H}]_{:,1:K}]_{\mathrm{diag}}\|^2 = 0 \cap \Im\{[\boldsymbol{G}\boldsymbol{P}\boldsymbol{H}]_{:,1:K}\} = \boldsymbol{0}\} \quad (19)$$

where the first condition guarantees that $[\boldsymbol{G}\boldsymbol{P}_{\mathrm{II}}\boldsymbol{H}]_{:,1:K}$ is a diagonal matrix, and the second constraint stems from that the imaginary components of the diagonal elements should be zero.

We solve the first condition in (19). Since the condition is the same to that in (6), the solutions can be obtained via (11), i.e.,

$$\boldsymbol{p}_{\mathrm{II}} = \frac{\eta \boldsymbol{U}\boldsymbol{a}_{\mathrm{II}}}{\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{II}}\|_\infty} \quad (20)$$

where $\boldsymbol{P}_{\mathrm{II}} = \mathrm{diag}\{\boldsymbol{p}_{\mathrm{II}}\}$ and $\boldsymbol{a}_{\mathrm{II}} \in \mathbb{C}^{N-K^2+K}$ is a linear combination vector. To avoid trivial cases, we assume $\boldsymbol{a}_{\mathrm{II}} \neq \boldsymbol{0}$. Next, we provide proposition 1 for determining the vector $\boldsymbol{a}_{\mathrm{II}}$ such that the second condition in (19) is meanwhile satisfied.

Proposition 1: The vector $\boldsymbol{a}_{\mathrm{II}}$ that satisfies the second condition in (19) can be obtained by

$$[\Re\{\boldsymbol{a}_{\mathrm{II}}\}^{\mathrm{T}}, \Im\{\boldsymbol{a}_{\mathrm{II}}\}^{\mathrm{T}}]^{\mathrm{T}} = \bar{\boldsymbol{V}}\boldsymbol{\omega} \quad (21)$$

where $\boldsymbol{\omega} \in \mathbb{R}^{2N-2K^2+K}$ is a random linear combination vector; $\bar{\boldsymbol{V}} \in \mathbb{R}^{2(N-K^2+K)\times(2N-2K^2+K)}$ denotes the orthonormal basis of the null space of $\boldsymbol{C} \in \mathbb{R}^{K\times 2(N-K^2+K)}$, and the matrix $\boldsymbol{C}$ is

$$\boldsymbol{C} = \begin{bmatrix} \Im\{\boldsymbol{c}_1\}, & \Im\{\boldsymbol{c}_2\}, & \cdots & \Im\{\boldsymbol{c}_K\} \\ \Re\{\boldsymbol{c}_1\}, & \Re\{\boldsymbol{c}_2\}, & \cdots & \Re\{\boldsymbol{c}_K\} \end{bmatrix}^{\mathrm{T}} \quad (22)$$

$$\boldsymbol{c}_i = \boldsymbol{U}^{\mathrm{T}}(\boldsymbol{g}_{i,:}^{\mathrm{T}} \odot \boldsymbol{h}_i). \quad (23)$$

Proof: The ith diagonal element of $\boldsymbol{G}\boldsymbol{P}_{\mathrm{II}}\boldsymbol{H}$, $i \in \mathcal{I}_K$, is written as

$$\alpha_{\mathrm{II},i} = \boldsymbol{p}_{\mathrm{II}}^{\mathrm{T}}(\boldsymbol{g}_{i,:}^{\mathrm{T}} \odot \boldsymbol{h}_i) \quad (24)$$

$$= \frac{\eta \boldsymbol{a}_{\mathrm{II}}^{\mathrm{T}}\boldsymbol{U}^{\mathrm{T}}(\boldsymbol{g}_{i,:}^{\mathrm{T}} \odot \boldsymbol{h}_i)}{\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{II}}\|_\infty} \quad (25)$$

$$= \frac{\boldsymbol{a}_{\mathrm{II}}^{\mathrm{T}}\boldsymbol{c}_i}{\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{II}}\|_\infty} \quad (26)$$

where (24) derives from (5) and $\boldsymbol{P}_{\mathrm{II}} = \mathrm{diag}\{\boldsymbol{p}_{\mathrm{II}}\}$; (25) is obtained by substituting (20) into (24); (26) follows from letting $\boldsymbol{c}_i \triangleq \eta \boldsymbol{U}^{\mathrm{T}}(\boldsymbol{g}_{i,:}^{\mathrm{T}} \odot \boldsymbol{h}_i)$. We aim to find a general solution for the vector $\boldsymbol{a}_{\mathrm{II}}$ such that the imaginary components of all the K diagonal elements are zero. We first check the imaginary component of the ith diagonal element $\alpha_{\mathrm{II},i}$. Specifically, the imaginary component of $\alpha_{\mathrm{II},i}$ can be expanded from (26) as

$$\Im\{\alpha_{\mathrm{II},i}\} = \frac{\Re\{\boldsymbol{a}_{\mathrm{II}}^{\mathrm{T}}\}\Im\{\boldsymbol{c}_i\} + \Im\{\boldsymbol{a}_{\mathrm{II}}^{\mathrm{T}}\}\Re\{\boldsymbol{c}_i\}}{\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{II}}\|_\infty} \quad (27)$$

where the infinite norm $\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{II}}\|_\infty > 0$. The equality (27) indicates that the imaginary component of $\alpha_{\mathrm{II},i}$ is zero if the vector $\boldsymbol{a}_{\mathrm{II}}$ satisfies

$$\Re\{\boldsymbol{a}_{\mathrm{II}}^{\mathrm{T}}\}\Im\{\boldsymbol{c}_i\} + \Im\{\boldsymbol{a}_{\mathrm{II}}^{\mathrm{T}}\}\Re\{\boldsymbol{c}_i\} = 0. \quad (28)$$

The equality (28) reveals the constraint for the ith diagonal element to be a real number. Since the matrix $\boldsymbol{G}\boldsymbol{P}_{\mathrm{II}}\boldsymbol{H}$ has K diagonal elements, we have K linear equations that are obtained by running i from 1 to K in (28). These K linear equations can be collectively expressed as

$$\boldsymbol{C}[\Re\{\boldsymbol{a}_{\mathrm{II}}\}^{\mathrm{T}}, \Im\{\boldsymbol{a}_{\mathrm{II}}\}^{\mathrm{T}}]^{\mathrm{T}} = \boldsymbol{0} \quad (29)$$

where $\boldsymbol{C} \in \mathbb{R}^{K\times 2(N-K^2+K)}$ is given in (22). Assume the matrix $\boldsymbol{C}$ has more columns than rows, i.e., $2(N-K^2+K) > K$. It is readily to find that the solutions to (29) are in the null space of $\boldsymbol{C}$. Specifically, let $\bar{\boldsymbol{V}} \in \mathbb{R}^{2(N-K^2+K)\times(2N-2K^2+K)}$ denote the orthonormal basis of the null space of $\boldsymbol{C}$. Thus the solution to (29) is

$$[\Re\{\boldsymbol{a}_{\mathrm{II}}\}^{\mathrm{T}}, \Im\{\boldsymbol{a}_{\mathrm{II}}\}^{\mathrm{T}}]^{\mathrm{T}} = \bar{\boldsymbol{V}}\boldsymbol{\omega} \quad (30)$$

where $\boldsymbol{\omega} \in \mathbb{R}^{2N-2K^2+K}$ is a random linear combination vector. ■

Remark 2: From the dimensions of the random vector $\boldsymbol{\omega}$, it can be found that the DoR is

$$\mathsf{DoR} = 2N - 2K^2 + K. \tag{31}$$

Although the DoR is reduced comparing with the first scheme, this reflection design is able to enhance the spectral efficiency.

2) Transceiver Design: Since the equivalent channel matrix at Bob is diagonal with all diagonal elements being unknown real numbers, common signaling techniques such as the QAM and PSK cannot be used in this case. However, the channel gains being real values guarantee that the in-phase and quadrature components of the transmitted signals can independently carry information bits. Thus, the QSSK modulation can be employed to achieve the secure transmission and double the spectral efficiency [23].[5]

Specifically, two independent data streams are modulated into the QSSK symbols by selecting the transmit antennas to transmit the in-phase and quadrature components of an unmodulated carrier signal separately. Since only the paired receive antennas can receive the signals and the channel gains are real numbers, the legitimate receiver is able to identify the active transmit antennas by comparing the received signal powers of the in-phase and the quadrature components, respectively. As a result, the authorized receiver can recover the information without knowing the channel gains. However, the illegitimate receiver cannot identify the active transmit antennas since Alice-to-Eve channels are full and intractable. The transceiver design of the proposed RIS-enabled secure QSSK scheme is detailed as follows. At the transmitter, a group of $2\log K$ bits are transmitted. The first $\log K$ bits selects one of the K antennas to transmit the in-phase component of the unmodulated carrier signal, and the remaining $\log K$ bits determine another or the same antenna to transmit the quadrature component of the unmodulated carrier signal. Assume the first $\log K$ bits and the last $\log K$ bits are converted into decimal numbers i and j, respectively. The transmit signal of Alice is

$$\boldsymbol{x}_{\mathrm{II}} = [\boldsymbol{e}_i^{\mathrm{T}} + \jmath \boldsymbol{e}_j^{\mathrm{T}}, \quad \mathbf{0}^{\mathrm{T}}]^{\mathrm{T}}, \quad i \in \mathcal{I}_K, \ j \in \mathcal{I}_K. \tag{32}$$

Upon receiving the signals from Alice, the RIS reflects the signals using a randomly generated $\boldsymbol{P}_{\mathrm{II}}$ and then the reflected signals are forwarded to the receiver ends. In particular, the received signals at Bob are written as

$$\boldsymbol{y}_{\mathrm{II}} = \boldsymbol{D}_{\mathrm{II}}(\boldsymbol{e}_i + \jmath \boldsymbol{e}_j) + \boldsymbol{\mu} \tag{33}$$

$$= \alpha_{\mathrm{II},i}\boldsymbol{e}_i + \jmath \alpha_{\mathrm{II},j}\boldsymbol{e}_j + \boldsymbol{\mu} \tag{34}$$

where $\boldsymbol{D}_{\mathrm{II}} \triangleq \boldsymbol{G}\boldsymbol{P}_{\mathrm{II}}\boldsymbol{H}$ is the effective channel from Alice to Bob; (34) is derived from the fact that $\boldsymbol{D}_{\mathrm{II}}$ is a diagonal matrix with the ith diagonal element being a real number $\alpha_{\mathrm{II},i}$, $\boldsymbol{D}_{\mathrm{II}} = \mathrm{diag}\{\alpha_{\mathrm{II},1}, \ldots, \alpha_{\mathrm{II},K}\}$. From (34), Bob can identify the indices of the active transmit antenna to retrieve the secret messages by performing the non-coherent detection

$$\hat{i} = \arg\max_i |\Re\{y_{\mathrm{II},i}\}|^2 \tag{35}$$

$$\hat{j} = \arg\max_j |\Im\{y_{\mathrm{II},j}\}|^2 \tag{36}$$

where $y_{\mathrm{II},i}$ and $y_{\mathrm{II},j}$ are the ith and the jth element of $\boldsymbol{y}_{\mathrm{II}}$, respectively. This non-coherent detection has a complexity of $O(K)$, which scales linearly with the number of transmit antennas.

On the other hand, the reflection of the RIS prevents Eve from accurately estimating the indices of the active transmit antennas. Specifically, the reflected signals received at Bob and Eve are presented in Figure 3, where we consider a wiretap system with $L = 2$, $K = 2$, $M = 2$, $N = 5$, and the SNR is 30 dB. Each QSSK symbol delivers 2 bits. From Figure 3(a), we observe that the received constellations are clearly distinguishable at the two antennas of Bob. For example, the blue dots represent the received signals when transmit antennas $\#1$ and $\#2$ are activated to send the in-phase and quadrature components, respectively. As can be seen in Figure 3(a), the in-phase components at receive antenna $\#1$ and the quadrature components at receive antenna $\#2$ tend to be stronger. It indicates that the active transmit antennas can be identified by comparing the received signal powers. In contrast, Figure 3(b) shows Eve's reception is completely messed up. For example, the dots in red, blue, green and cyan form a disrupted constellation diagram. Thus, Eve is unable to perform the non-coherent detection.

C. RIS-Enabled Secure PSK Transmission: Scheme III

1) Reflection Coefficients Design: The objective is to find a reflection coefficient matrix $\boldsymbol{P}_{\mathrm{III}}$ which guarantees that $\boldsymbol{G}\boldsymbol{P}_{\mathrm{III}}\boldsymbol{H}$ is a diagonal matrix with all diagonal elements being positive real numbers. This problem can then be formulated as

$$\begin{aligned}\boldsymbol{P}_{\mathrm{III}} = \arg\{\boldsymbol{P} \mid \|[\boldsymbol{G}\boldsymbol{P}\boldsymbol{H}]_{:,1:K} - [[\boldsymbol{G}\boldsymbol{P}\boldsymbol{H}]_{:,1:K}]_{\mathrm{diag}}\|^2 = 0 \\ \cap \Im\{[\boldsymbol{G}\boldsymbol{P}\boldsymbol{H}]_{:,1:K}\} = \mathbf{0} \cap \Re\{[\boldsymbol{G}\boldsymbol{P}\boldsymbol{H}]_{:,1:K}\} \succeq \mathbf{0}\}\end{aligned} \tag{37}$$

where $\succeq$ denotes a component-wise greater; the first condition guarantees that $[\boldsymbol{G}\boldsymbol{P}_{\mathrm{III}}\boldsymbol{H}]_{:,1:K}$ is a diagonal matrix; the second and the third constraints stem from the requirement that the diagonal elements are positive real numbers.

We solve the first condition in (37). Since the condition is the same to that in (6), the solutions can be obtained via (11), i.e.,

$$\boldsymbol{p}_{\mathrm{III}} = \frac{\eta \boldsymbol{U}\boldsymbol{a}_{\mathrm{III}}}{\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{III}}\|_\infty} \tag{38}$$

where $\boldsymbol{P}_{\mathrm{III}} = \mathrm{diag}\{\boldsymbol{p}_{\mathrm{III}}\}$ and $\boldsymbol{a}_{\mathrm{III}} \in \mathbb{C}^{N-K^2+K}$ is a linear combination vector. To avoid trivial cases, we assume $\boldsymbol{a}_{\mathrm{III}} \neq \mathbf{0}$. The denominator $\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{III}}\|_\infty$ is incorporated to ensure that the maximum reflection gain is η. Next, we provide proposition 2 for determining the vector $\boldsymbol{a}_{\mathrm{III}}$ such that the second and the third conditions in (37) are meanwhile satisfied.

[5]The generalized QSSK signaling can be used to further enhance the spectral efficiency.

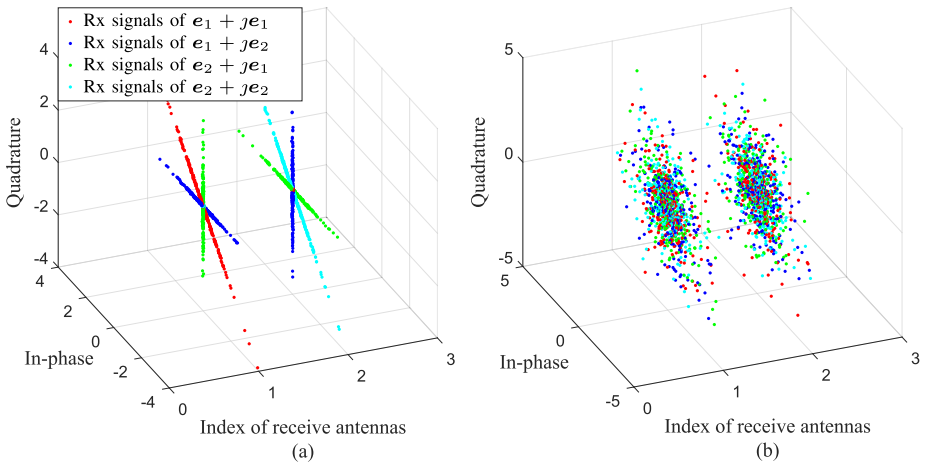


Fig. 3. Reflected signals received at (a) Bob and (b) Eve, with $L = 2$, $K = 2$, $M = 2$, and $N = 5$. The red dots, blue dots, green dots, and cyan dots denote the received signals when Alice transmits QSSK symbols $\boldsymbol{e}_1 + j\boldsymbol{e}_1$, $\boldsymbol{e}_1 + j\boldsymbol{e}_2$, $\boldsymbol{e}_2 + j\boldsymbol{e}_1$, and $\boldsymbol{e}_2 + j\boldsymbol{e}_2$, respectively. The comparison between (a) and (b) shows Bob is more likely to correctly estimate the indices of the active transmit antennas than Eve.

Proposition 2: The vector $\boldsymbol{a}_{\mathrm{III}}$ that satisfies the second and the third constraints in (37) are expressed as

$$\begin{bmatrix} \Re\{\boldsymbol{a}_{\mathrm{III}}\} \\ \Im\{\boldsymbol{a}_{\mathrm{III}}\} \end{bmatrix} = \begin{bmatrix} -\boldsymbol{A}_1^{-1}\boldsymbol{A}_2\boldsymbol{\varpi} + \boldsymbol{A}_1^{-1}\boldsymbol{\iota} \\ \boldsymbol{\varpi} \end{bmatrix} \tag{39}$$

where $\boldsymbol{\varpi} \in \mathbb{R}^{2N-2K^2}$ denotes a random real vector; $\boldsymbol{\iota} = [\iota_1, \ldots, \iota_K, 0, \ldots, 0]^{\mathrm{T}} \in \mathbb{R}^{2K}$ is a real vector with the first K elements being random positive numbers, i.e., $\iota_i > 0$, and the last K elements being zero; $\boldsymbol{A}_1 \in \mathbb{R}^{2K\times 2K}$ and $\boldsymbol{A}_2 \in \mathbb{R}^{2K\times(2N-2K^2)}$ are the first $2K$ columns and the last $2N-2K^2$ columns of $\boldsymbol{A}$, respectively, i.e., $\boldsymbol{A} = [\boldsymbol{A}_1\ \boldsymbol{A}_2] \in \mathbb{R}^{2K\times(2N-2K^2+2K)}$, and the matrix $\boldsymbol{A}$ is written as

$$\boldsymbol{A} = \begin{bmatrix} \Re\{\boldsymbol{c}_1\} & \cdots & \Re\{\boldsymbol{c}_K\} & \Im\{\boldsymbol{c}_1\} & \cdots & \Im\{\boldsymbol{c}_K\} \\ -\Im\{\boldsymbol{c}_1\} & \cdots & -\Im\{\boldsymbol{c}_K\} & \Re\{\boldsymbol{c}_1\} & \cdots & \Re\{\boldsymbol{c}_K\} \end{bmatrix}^{\mathrm{T}}. \tag{40}$$

Proof: We first provide explicit expressions for the diagonal elements of $\boldsymbol{G}\boldsymbol{P}_{\mathrm{III}}\boldsymbol{H}$. From (26) and replacing $\boldsymbol{a}_{\mathrm{II}}$ with $\boldsymbol{a}_{\mathrm{III}}$, the ith diagonal element of $\boldsymbol{G}\boldsymbol{P}_{\mathrm{III}}\boldsymbol{H}$ can be written as

$$\alpha_{\mathrm{III},i} = \frac{\boldsymbol{a}_{\mathrm{III}}^{\mathrm{T}}\boldsymbol{c}_i}{\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{III}}\|_\infty} \tag{41}$$

where $\boldsymbol{c}_i \triangleq \eta\boldsymbol{U}^{\mathrm{T}}(\boldsymbol{g}_{i,:}^{\mathrm{T}} \odot \boldsymbol{h}_i)$. We aim to find a general solution for the vector $\boldsymbol{a}_{\mathrm{III}}$ such that all the K diagonal elements are positive real numbers. Now, we check the real and imaginary components of the ith diagonal element $\alpha_{\mathrm{III},i}$. Specifically, the real and imaginary components of $\alpha_{\mathrm{III},i}$ can be respectively expanded from (41) as

$$\Re\{\alpha_{\mathrm{III},i}\} = \frac{\Re\{\boldsymbol{a}_{\mathrm{III}}^{\mathrm{T}}\}\Re\{\boldsymbol{c}_i\} - \Im\{\boldsymbol{a}_{\mathrm{III}}^{\mathrm{T}}\}\Im\{\boldsymbol{c}_i\}}{\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{III}}\|_\infty} \tag{42}$$

$$\Im\{\alpha_{\mathrm{III},i}\} = \frac{\Re\{\boldsymbol{a}_{\mathrm{III}}^{\mathrm{T}}\}\Im\{\boldsymbol{c}_i\} + \Im\{\boldsymbol{a}_{\mathrm{III}}^{\mathrm{T}}\}\Re\{\boldsymbol{c}_i\}}{\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{III}}\|_\infty} \tag{43}$$

where $\|\boldsymbol{U}\boldsymbol{a}_{\mathrm{III}}\|_\infty > 0$. (42) and (43) indicate that $\alpha_{\mathrm{III},i}$ is a positive real number if $\boldsymbol{a}_{\mathrm{III}}$ satisfies

$$\Re\{\boldsymbol{a}_{\mathrm{III}}^{\mathrm{T}}\}\Re\{\boldsymbol{c}_i\} - \Im\{\boldsymbol{a}_{\mathrm{III}}^{\mathrm{T}}\}\Im\{\boldsymbol{c}_i\} = \iota_i \tag{44}$$

$$\Re\{\boldsymbol{a}_{\mathrm{III}}^{\mathrm{T}}\}\Im\{\boldsymbol{c}_i\} + \Im\{\boldsymbol{a}_{\mathrm{III}}^{\mathrm{T}}\}\Re\{\boldsymbol{c}_i\} = 0 \tag{45}$$

where $\iota_i > 0$ denotes a positive number. (44) guarantees that the real component of $\alpha_{\mathrm{III},i}$ is positive, and (45) enforces the imaginary component of $\alpha_{\mathrm{III},i}$ to be zero. Since the matrix $\boldsymbol{G}\boldsymbol{P}_{\mathrm{III}}\boldsymbol{H}$ has K diagonal elements, we have $2K$ linear equations that are obtained from running i from 1 to K in (44) and (45), respectively. These $2K$ linear equations can be collectively expressed in a matrix form as

$$\boldsymbol{A}[\Re\{\boldsymbol{a}_{\mathrm{III}}\}^{\mathrm{T}}, \Im\{\boldsymbol{a}_{\mathrm{III}}\}^{\mathrm{T}}]^{\mathrm{T}} = \boldsymbol{\iota} \tag{46}$$

where $\boldsymbol{A} \in \mathbb{R}^{2K\times(2N-2K^2+2K)}$ is given in (40); $\boldsymbol{\iota} \in \mathbb{R}^{2K}$ is a vector with elements drawn from the right-hand sides of (44) and (45), i.e., $\boldsymbol{\iota} = [\iota_1, \ldots, \iota_K, 0, \ldots, 0]^{\mathrm{T}}$.

The existence of solutions to (46) is guaranteed by supposing the matrix $\boldsymbol{A}$ has more columns than rows, i.e., $N > K^2$. This condition also indicates (46) is a group of underdetermined linear equations, and has an infinite number of solutions for $\boldsymbol{a}_{\mathrm{III}}$ [24]. The general solution is

$$\begin{aligned} &[\Re\{\boldsymbol{a}_{\mathrm{III}}\}^{\mathrm{T}}, \Im\{\boldsymbol{a}_{\mathrm{III}}\}^{\mathrm{T}}]^{\mathrm{T}} \\ &\quad = \arg\{\boldsymbol{a} \mid \boldsymbol{A}\boldsymbol{a} = \boldsymbol{\iota}\} &(47)\\ &\quad = \arg\{\boldsymbol{\Psi}\boldsymbol{\varpi} + \boldsymbol{a}_* \mid \boldsymbol{\varpi} \in \mathbb{R}^{2N-2K^2}\} &(48)\end{aligned}$$

where $\boldsymbol{\Psi} \in \mathbb{R}^{(2N-2K^2+2K)\times(2N-2K^2)}$ is a basis of the null space of $\boldsymbol{A}$; $\boldsymbol{\varpi}$ denotes a linear combination vector and $\boldsymbol{\Psi}\boldsymbol{\varpi}$ is an element in the null space of $\boldsymbol{A}$; $\boldsymbol{a}_* \in \mathbb{R}^{2(N-K^2+K)}$ is a particular solution to $\boldsymbol{A}\boldsymbol{a} = \boldsymbol{\iota}$, i.e., $\boldsymbol{A}\boldsymbol{a}_* = \boldsymbol{\iota}$. (48) follows from laws of the linear algebra that the solution to $\boldsymbol{A}\boldsymbol{a} = \boldsymbol{\iota}$ can be expressed by the sum of one particular solution $\boldsymbol{a}_*$ and an arbitrary element in the null space of $\boldsymbol{A}$, i.e., $\boldsymbol{\Psi}\boldsymbol{\varpi}$. Next, we provide expressions for $\boldsymbol{a}_*$ and $\boldsymbol{\Psi}$.

Let $\boldsymbol{A} = [\boldsymbol{A}_1\ \boldsymbol{A}_2]$, where $\boldsymbol{A}_1 \in \mathbb{R}^{2K\times 2K}$ is constructed from the first $2K$ columns of $\boldsymbol{A}$ and $\boldsymbol{A}_2 \in \mathbb{R}^{2K\times(2N-2K^2)}$ consists of the last $2N-2K^2$ columns of $\boldsymbol{A}$. Then (46) is rewritten as

$$\boldsymbol{\iota} = \boldsymbol{A}_1\boldsymbol{\eta}_1 + \boldsymbol{A}_2\boldsymbol{\eta}_2 \tag{49}$$

where $\boldsymbol{\eta}_1 \in \mathbb{R}^{2K}$ and $\boldsymbol{\eta}_2 \in \mathbb{R}^{2N-2K^2}$; (49) derives from letting $[\Re\{\boldsymbol{a}_{\mathrm{III}}\}^{\mathrm{T}}, \Im\{\boldsymbol{a}_{\mathrm{III}}\}^{\mathrm{T}}]^{\mathrm{T}} = [\boldsymbol{\eta}_1^{\mathrm{T}}\ \boldsymbol{\eta}_2^{\mathrm{T}}]^{\mathrm{T}}$. Moreover,

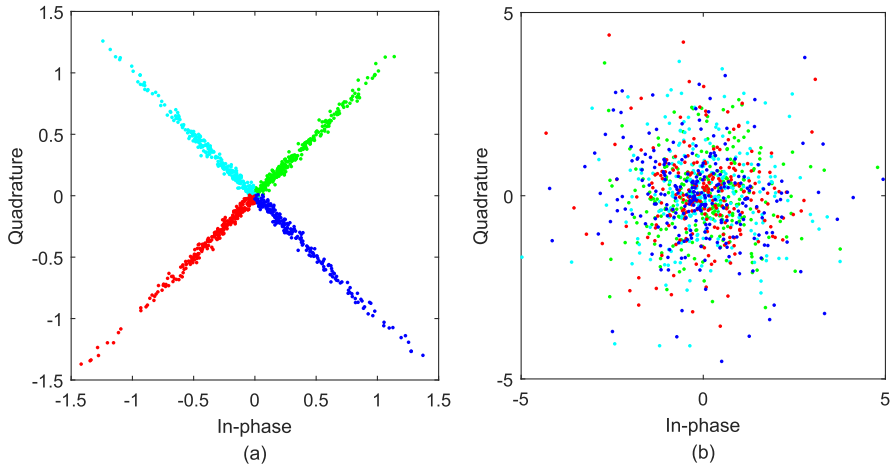


Fig. 4. Reflected QPSK symbols at receive antenna #1 of (a) Bob and at receive antenna #1 of (b) Eve, with $L = 2$, $K = 2$, $M = 2$, $N = 5$. The red dots, blue dots, green dots, and cyan dots denote the QPSK symbols in four quadrants respectively. The results show that the received signal samples at Eve are completely distorted, while the phases of the received signal samples at Bob are clearly distinguishable. Therefore, Bob is more likely to reliably recover the QPSK symbols than Eve.

we observe from (49) that $\boldsymbol{\eta}_1$ can be represented by $\boldsymbol{\eta}_2$

$$\boldsymbol{\eta}_1 = \boldsymbol{A}_1^{-1}(\boldsymbol{\iota} - \boldsymbol{A}_2\boldsymbol{\eta}_2) \tag{50}$$

where the square matrix $\boldsymbol{A}_1$ is invertible since $\boldsymbol{A}$ is column full-rank. Let $\boldsymbol{\eta}_2 = \mathbf{0}$, and thus we have $\boldsymbol{\eta}_1 = \boldsymbol{A}_1^{-1}\boldsymbol{\iota}$. These particular realizations of $\boldsymbol{\eta}_1$ and $\boldsymbol{\eta}_2$ are grouped to form the particular solution $\boldsymbol{a}_*$ in (48), which is

$$\boldsymbol{a}_* = \begin{bmatrix} \boldsymbol{A}_1^{-1}\boldsymbol{\iota} \\ \mathbf{0} \end{bmatrix} \tag{51}$$

and (51) can readily validate the equality

$$\boldsymbol{A}\boldsymbol{a}_* = \boldsymbol{\iota}. \tag{52}$$

In addition, the base for the null space of $\boldsymbol{A}$ can also be represented by $\boldsymbol{A}_1$ and $\boldsymbol{A}_2$, which is

$$\boldsymbol{\Psi} = \begin{bmatrix} -\boldsymbol{A}_1^{-1}\boldsymbol{A}_2 \\ \boldsymbol{I} \end{bmatrix} \tag{53}$$

and the full-rank matrix $\boldsymbol{\Psi}$ satisfies the equality

$$\boldsymbol{A}\boldsymbol{\Psi} = \mathbf{0}. \tag{54}$$

Finally, the general solution $[\Re\{\boldsymbol{a}_{\rm III}\}^{\rm T}, \Im\{\boldsymbol{a}_{\rm III}\}^{\rm T}]^{\rm T} = \arg\{\boldsymbol{\Psi}\boldsymbol{\varpi} + \boldsymbol{a}_*\}$ can be expressed as

$$\begin{bmatrix} \Re\{\boldsymbol{a}_{\rm III}\} \\ \Im\{\boldsymbol{a}_{\rm III}\} \end{bmatrix} = \begin{bmatrix} -\boldsymbol{A}_1^{-1}\boldsymbol{A}_2\boldsymbol{\varpi} + \boldsymbol{A}_1^{-1}\boldsymbol{\iota} \\ \boldsymbol{\varpi} \end{bmatrix} \tag{55}$$

which completes the proof. ■

Remark 3: From the dimensions of the real vector $\boldsymbol{\varpi}$ and $\boldsymbol{\iota}$, it can be found that the DoR is

$$\text{DoR} = 2N - 2K^2 + 0.5K \tag{56}$$

where the term $0.5K$ is due to the K random positive numbers in vector $\boldsymbol{\iota}$.

2) Transceiver Design: We note that the equivalent channel matrix at Bob is diagonal with all diagonal elements being positive real numbers. Thus, the transmit antennas of Alice and the receive antennas of Bob are one-to-one paired. In addition, since the effective channel gains are real numbers, no phase changes will be incurred on the transmitted signals. Therefore, a phase-based constellation diagram, i.e., the PSK modulation, can be used for the transmission between Alice and Bob. Moreover, by sending multiple PSK symbols, the spectral efficiency scales linearly with the number of transmit antennas. Specifically, the transmit signal of Alice is given by

$$\boldsymbol{x}_{\rm III} = [q_1, q_2, \ldots, q_K, 0, \ldots, 0]^{\rm T} \tag{57}$$

where $q_i \in \mathcal{Q}$ is a PSK symbol, and $\mathcal{Q}$ is a PSK constellation diagram. Upon receiving the signals from Alice, the RIS reflects the signals and then the reflected signals reach the receiver ends. In particular, the received signals at Bob are

$$\boldsymbol{y}_{\rm III} = \boldsymbol{D}_{\rm III}\boldsymbol{x}_{\rm III} + \boldsymbol{\mu} \tag{58}$$

$$= \sum_{i=1}^{K} \alpha_{{\rm III},i} q_i \boldsymbol{e}_i + \boldsymbol{\mu} \tag{59}$$

where $\boldsymbol{D}_{\rm III} \triangleq \boldsymbol{G}\boldsymbol{P}_{\rm III}\boldsymbol{H}$ is the effective channel from Alice to Bob; (59) follows that $\boldsymbol{D}_{\rm III}$ is a diagonal matrix, and $\boldsymbol{D}_{\rm III} = \text{diag}\{\alpha_{{\rm III},1}, \ldots, \alpha_{{\rm III},K}\}$. In addition, (59) reveals that the PSK symbols can be independently detected without knowing the channel gains. For example, the PSK symbol received at the ith antenna of Bob can be estimated by

$$\hat{q}_i = \arg\min_{q_i \in \mathcal{Q}} |y_{{\rm III},i} - \alpha_{{\rm III},i} q_i|^2 \tag{60}$$

$$= \arg\max_{q_i \in \mathcal{Q}} \Re\{y_{{\rm III},i}^* q_i\} \tag{61}$$

where $y_{{\rm III},i}$ is the ith element of $\boldsymbol{y}_{\rm III}$; (61) follows from a direct expansion of $|y_{{\rm III},i} - \alpha_{{\rm III},i} q_i|^2$, $|q_i| = 1$, and $\alpha_{{\rm III},i} > 0$. This non-coherent detection has a complexity of $O(L)$, and decoding a total number of K PSK symbols results in a complexity of $O(KL)$.

We present the reflected signals received at Bob and Eve in Figure 4. From Figure 4(a), we observe that the phases of

TABLE I
PERFORMANCE METRICS OF DIFFERENT SCHEMES

Proposed scheme	DoR	Spectral efficiency	Receiver complexity of Bob
RIS-enabled secure SSK	$2(N-K^2+K)$	$\log K$	$O(K)$
RIS-enabled secure QSSK	$2N-2K^2+K$	$2\log K$	$O(K)$
RIS-enabled secure PSK	$2N-2K^2+0.5K$	$K\log\lvert\mathcal{Q}\rvert$	$O(K\lvert\mathcal{Q}\rvert)$

the received signal samples are clearly distinguishable at Bob, which means Bob can decode the QPSK symbols by simply identifying the phases. In contrast, however, Figure 4(b) shows Eve's reception is completely messed up. For example, the dots in red, blue, green and cyan form a uniformly distributed constellation diagram. No obvious statistical difference can be employed to recover the transmitted information.

Remark 4: Table I explicitly provides a performance comparison of the proposed three secure transmission schemes in terms of DoR, spectral efficiency, and receiver complexity. For identical K and N, the RIS-enabled secure SSK scheme has the highest DoR and the lowest spectral efficiency, while the RIS-enabled secure PSK scheme has the highest spectral efficiency and the lowest DoR. Furthermore, the RIS-enabled secure QSSK scheme achieves a balance between the DoR and the spectral efficiency.

IV. PERFORMANCE ANALYSIS

A. Secrecy Rate Analysis

We first analyze the secrecy rates of the proposed transmission schemes. The SSK, QSSK, and PSK symbols are with finite input of the wireless channel since they are constituted by either the active antenna index or the modulated symbols in a finite alphabet. Regarding the output of the channel, the received signals are continuous due to the fading and the additive Gaussian noise. Consequently, the channel is with discrete-input and continuous-output. In this case, the achievable rate has been characterized in [27]. Recall the signal model in (2) and (3). We can calculate the achievable rates of Bob and Eve in analogy with [27] as

$$R_{\mathrm{Bob}} = \log|\mathcal{M}| - \frac{1}{|\mathcal{M}|}\sum_{\imath=1}^{|\mathcal{M}|} \mathbb{E}_{\boldsymbol{\mu}}\left\{\log\sum_{l=1}^{|\mathcal{M}|}\exp\left(\frac{-\|\boldsymbol{GPH}(\boldsymbol{x}_\imath-\boldsymbol{x}_l)+\boldsymbol{\mu}\|^2+\|\boldsymbol{\mu}\|^2}{\sigma^2}\right)\right\} \tag{62}$$

$$R_{\mathrm{Eve}} = \log|\mathcal{M}| - \frac{1}{|\mathcal{M}|}\sum_{\imath=1}^{|\mathcal{M}|} \mathbb{E}_{\boldsymbol{\nu}'}\left\{\log\sum_{l=1}^{|\mathcal{M}|}\exp\left(-\|\boldsymbol{\Sigma}^{-\frac{1}{2}}\boldsymbol{B}(\boldsymbol{x}_\imath-\boldsymbol{x}_l)+\boldsymbol{\nu}'\|^2+\|\boldsymbol{\nu}'\|^2\right)\right\} \tag{63}$$

where $\mathcal{M}$ denotes the alphabet of the baseband symbols, i.e., the indices of the active antennas or the PSK symbols; $\boldsymbol{x}_\imath$ and $\boldsymbol{x}_l$ are the $\imath$th and lth symbols in $\mathcal{M}$; $\boldsymbol{\nu}'$ is the whitened effective noise with zero mean and unit variance observed at Eve, where $\boldsymbol{\nu}' = \boldsymbol{\Sigma}^{-\frac{1}{2}}(\boldsymbol{FPH}(\boldsymbol{x}_\imath - \boldsymbol{x}_l) + \boldsymbol{\nu})$; $\boldsymbol{\Sigma} = \mathbb{E}\{\boldsymbol{FPH}(\boldsymbol{x}_\imath - \boldsymbol{x}_l)(\boldsymbol{x}_\imath - \boldsymbol{x}_l)^\dagger\boldsymbol{H}^\dagger\boldsymbol{P}^\dagger\boldsymbol{F}^\dagger\} + \gamma^2\boldsymbol{I}$ is the covariance matrix of the effective noise. We consider the term $\boldsymbol{FPH}(\boldsymbol{x}_\imath - \boldsymbol{x}_l)$ as an interference to Eve since $\boldsymbol{P}$ contains certain degrees of randomness and renders the proposed scheme a one-time pad system. That is, Eve can only retrieve the information in the direct link from Alice to Eve. The secrecy rate R is the difference between the achievable rates of Bob and Eve

$$R = [R_{\mathrm{Bob}} - R_{\mathrm{Eve}}]^+ \tag{64}$$

where $[x]^+ = \max\{0, x\}$. Equations (62)-(64) can be numerically evaluated by randomly generating a large number of noise realizations and taking the expectation.

B. BER Analysis

1) RIS-Enabled Secure SSK Scheme:

Lemma 1: Bob's BER of the RIS-enabled secure SSK transmission scheme is given by

$$\epsilon_1 = \delta_\kappa - \delta_\kappa\int_0^\infty\int_0^\infty \mathcal{F}_{\chi_2^2}^{K-1}(t) f_{\chi_2^2}(t;\lambda) f_\lambda(\lambda) dt d\lambda \tag{65}$$

where $\kappa = \log K$ and δ_κ is a scaling factor; $\mathcal{F}_{\chi_2^2}(t)$ represents the cumulative distribution function (CDF) of a chi-square distribution with two degrees of freedom; $f_{\chi_2^2}(t;\lambda)$ represents the probability distribution function (PDF) of a non-central chi-square distribution with two degrees of freedom and the non-centrality is $\lambda = \mathbb{E}\{\lambda_i\}$, where $\lambda_i = \frac{2|\alpha_{\mathrm{I},i}|^2}{\sigma^2}$; $f_\lambda(\lambda)$ is the PDF of λ.

Proof: The proof follows from the following derivation

$$\epsilon_1 = \delta_\kappa(1 - \mathbb{E}_\lambda\{\Delta\}) \tag{66}$$

$$= \delta_\kappa\left(1 - \mathbb{E}_\lambda\left\{\int_0^\infty \prod_{j=1, j\neq i}^{K} p(|y_{\mathrm{I},j}|^2 < t) p(|y_{\mathrm{I},i}|^2 = t) dt\right\}\right) \tag{67}$$

$$= \delta_\kappa - \delta_\kappa\int_0^\infty\int_0^\infty \mathcal{F}_{\chi_2^2}^{K-1}(t) f_{\chi_2^2}(t;\lambda) f_\lambda(\lambda) dt d\lambda \tag{68}$$

where Δ is the probability of correct active antenna detection for a given non-centrality λ.

We first illustrate the derivation of (66). Using the definition of Δ, the symbol error rate can be expressed as $1 - \mathbb{E}_\lambda\{\Delta\}$, i.e., the probability of erroneously identifying an active antenna. A scaling factor δ_κ is included here to transform the symbol error rate into the BER, which is based on the assumption that the active antenna may be falsely determined as any of the other antennas with equal probability. Given the initial value $\delta_0 = 0$, δ_κ can be written as

$$\delta_\kappa = \delta_{\kappa-1} + \frac{2^{\kappa-1} - \delta_{\kappa-1}}{2^\kappa - 1} \tag{69}$$

where the proof can be found in [26]. Next, we introduce the derivations of (67), which is to calculate the probability of the correct antenna detection. Recall that in the RIS-enabled secure SSK scheme, a single transmit antenna is activated and the corresponding antenna index conveys secret messages. Assume the ith transmit antenna is activated. The received signals at Bob are

$$y_{\mathrm{I},i} = \alpha_{\mathrm{I},i} + \mu_i, \quad y_{\mathrm{I},j} = u_j, \quad j \neq i \tag{70}$$

where for a given $\alpha_{\mathrm{I},i}$, $\Re\{y_{\mathrm{I},i}\}$ and $\Im\{y_{\mathrm{I},i}\}$ follow the Gaussian distributions, denoted by $\Re\{y_{\mathrm{I},i}\} \sim \mathcal{N}(\Re\{\alpha_{\mathrm{I},i}\}, \frac{\sigma^2}{2})$ and $\Im\{y_{\mathrm{I},i}\} \sim \mathcal{N}(\Im\{\alpha_{\mathrm{I},i}\}, \frac{\sigma^2}{2})$, respectively. Similarly, we have $\Re\{y_{\mathrm{I},j}\} \sim \mathcal{N}(0, \frac{\sigma^2}{2})$ and $\Im\{y_{\mathrm{I},j}\} \sim \mathcal{N}(0, \frac{\sigma^2}{2})$. Therefore, the squared terms with a normalization factor $\frac{2}{\sigma^2}$ follow the chi-square distributions, i.e.,

$$\frac{2}{\sigma^2}|y_{\mathrm{I},i}|^2 \sim \chi_2^2(t;\lambda_i), \quad \frac{2}{\sigma^2}|y_{\mathrm{I},j}|^2 \sim \chi_2^2(t) \tag{71}$$

where the non-centrality is $\lambda_i = \frac{2|\alpha_i|^2}{\sigma^2}$. Since $\{\alpha_i\}$ are i.i.d. random variables, we have $\mathbb{E}\{\lambda_i\} = \lambda$. From the non-coherent detection in (18), the antenna is correctly detected if $|y_{\mathrm{I},i}|^2$ is the maximum. Thus, the correct antenna detection probability Δ for a given λ is

$$\begin{aligned}\Delta &= \int_0^\infty p(|y_{\mathrm{I},1}|^2 < t, \ldots, |y_{\mathrm{I},i-1}|^2 < t, \\ &\quad |y_{\mathrm{I},i+1}|^2 < t, \ldots, |y_{\mathrm{I},K}|^2 < t) p(|y_{\mathrm{I},i}|^2 = t) dt \quad (72)\\ &= \int_0^\infty \prod_{j=1, j\neq i}^{K} p(|y_{\mathrm{I},j}|^2 < t) p(|y_{\mathrm{I},i}|^2 = t) dt \quad (73)\\ &= \int_0^\infty \mathcal{F}_{\chi_2^2}^{K-1}(t) f_{\chi_2^2}(t;\lambda) dt \quad (74)\end{aligned}$$

where (72) denotes that the received power $|y_{\mathrm{I},j}|^2$ of the inactive antenna is lower than $|y_{\mathrm{I},i}|^2$ of the active antenna; equations (73) and (74) follow from the fact that the arguments in $\{|y_{\mathrm{I},j}|^2\}$ are i.i.d. random variables. Finally, equation (68) is derived by averaging over the distribution of $f_\lambda(\lambda)$, which can be obtained using the empirical histogram based method. ∎

2) RIS-Enabled Secure QSSK Scheme:

Lemma 2: Bob's BER of the RIS-enabled secure QSSK transmission scheme is given by

$$\epsilon_2 = \delta_{2\kappa} - \delta_{2\kappa} \int_0^\infty \left(\int_0^\infty \mathcal{F}_{\chi_1^2}^{K-1}(t) f_{\chi_1^2}(t;\varrho) dt \right)^2 f_\varrho(\varrho) d\varrho \tag{75}$$

where $\mathcal{F}_{\chi_1^2}(t)$ represents the CDF of a chi-square distribution having one degree of freedom; $f_{\chi_1^2}(t;\varrho)$ represents the PDF of a non-central chi-square distribution having one degree of freedom and the non-centrality is $\varrho = \mathbb{E}\{\varrho_i\}$, where $\varrho_i = \frac{2\alpha_{\mathrm{II},i}^2}{\sigma^2}$; $f_\varrho(\varrho)$ is the PDF of ϱ.

Proof: The proof follows from the following derivation

$$\begin{aligned}\epsilon_2 &= \delta_{2\kappa}\big(1 - \mathbb{E}_\varrho\{\Omega^2\}\big) \quad (76)\\ &= \delta_{2\kappa}\left(1 - \mathbb{E}_\varrho\left\{\left(\int_0^\infty \mathcal{F}_{\chi_1^2}^{K-1}(t) f_{\chi_1^2}(t;\varrho) dt\right)^2\right\}\right) \quad (77)\\ &= \delta_{2\kappa} - \delta_{2\kappa} \int_0^\infty \left(\int_0^\infty \mathcal{F}_{\chi_1^2}^{K-1}(t) f_{\chi_1^2}(t;\varrho) dt \right)^2 f_\varrho(\varrho) d\varrho \quad (78)\end{aligned}$$

where Ω is the probability of correctly detecting the antenna that sends the in-phase component of the carrier signal, given the non-centrality ϱ.

The equation (76) follows from the fact that the real and imaginary components of the received signals in (34) are i.i.d. Therefore, the probability of correctly detecting both the antennas transmitting the in-phase and quadrature components is Ω^2, and the symbol error rate is $1 - \mathbb{E}_\gamma \Omega^2$. The scaling factor $\delta_{2\kappa}$ is due to 2κ binary bits are delivered in each transmission. The probability Ω is evaluated as follows. Assume the ith transmit antenna is activated to send the in-phase component of the carrier. From (34), taking real part of the received signals at Bob yields

$$\Re\{y_{\mathrm{II},i}\} = \alpha_{\mathrm{II},i} + \Re\{\mu_i\}, \;\; \Re\{y_{\mathrm{II},j}\} = \Re\{u_j\}, \; j \neq i \tag{79}$$

where for a given $\alpha_{\mathrm{II},i}$, we have $\Re\{y_{\mathrm{II},i}\} \sim \mathcal{N}(\alpha_{\mathrm{II},i}, \frac{\sigma^2}{2})$ and $\Re\{y_{\mathrm{II},j}\} \sim \mathcal{N}(0, \frac{\sigma^2}{2})$. Therefore, the squared terms with an normalization factor $\frac{2}{\sigma^2}$ follow the chi-square distributions, i.e.,

$$\frac{2}{\sigma^2}|\Re\{y_{\mathrm{II},i}\}|^2 \sim \chi_1^2(t;\varrho_i), \quad \frac{2}{\sigma^2}|\Re\{y_{\mathrm{II},j}\}|^2 \sim \chi_1^2(t) \tag{80}$$

with non-centrality $\gamma_i = \frac{2\alpha_{\mathrm{II},i}^2}{\sigma^2}$. Since the arguments in $\{\alpha_{\mathrm{II},i}\}$ are i.i.d. random variables, we have $\mathbb{E}\{\gamma_i\} = \gamma$. From the non-coherent detection in (35), the antenna is correctly detected when $|\Re\{y_{\mathrm{II},i}\}|^2$ is the maximum. Thus, the correct antenna detection probability Ω for a given γ is

$$\begin{aligned}\Omega &= \int_0^\infty \prod_{j=1, j\neq i}^{K} p(|\Re\{y_{\mathrm{II},j}\}|^2 < t) p(|\Re\{y_{\mathrm{II},i}\}|^2 = t) dt \quad (81)\\ &= \int_0^\infty \mathcal{F}_{\chi_1^2}^{K-1}(t) f_{\chi_1^2}(t;\lambda) dt \quad (82)\end{aligned}$$

where (81) and (82) follow from that the arguments in $\{|\Re\{y_{\mathrm{II},i}\}|^2\}$ are i.i.d. random variables. Finally, the equations (77) and (78) follow from (67) and (68), which completes the proof. ∎

3) RIS-Enabled Secure PSK Scheme:

Lemma 3: Bob's BER of the RIS-enabled secure PSK scheme is upper bounded by

$$\begin{aligned}\epsilon_3 \leq \frac{1}{\pi |\mathcal{M}| \log |\mathcal{M}|} \sum_{\imath=1}^{|\mathcal{M}|} \sum_{l=1}^{|\mathcal{M}|} d(\boldsymbol{x}_{\mathrm{III},\imath}, \boldsymbol{x}_{\mathrm{III},l}) \\ \times \mathbb{E}_{\boldsymbol{D}_{\mathrm{III}}} \left\{ \int_0^{\frac{\pi}{2}} \exp\left(- \frac{\|\boldsymbol{D}_{\mathrm{III}}(\boldsymbol{x}_{\mathrm{III},\imath} - \boldsymbol{x}_{\mathrm{III},l})\|^2}{2\sigma^2 \sin^2\theta} \right) d\theta \right\}\end{aligned} \tag{83}$$

where $\mathcal{M}$ is the alphabet of $\boldsymbol{x}_{\mathrm{III}}$ and $|\mathcal{M}| = K \log L$; $\boldsymbol{x}_{\mathrm{III},\imath}$ and $\boldsymbol{x}_{\mathrm{III},l}$ are the $\imath$th and the lth symbol in $\mathcal{M}$; $d(\boldsymbol{x}_{\mathrm{III},\imath}, \boldsymbol{x}_{\mathrm{III},l})$ is the Hamming distance of codewords $\boldsymbol{x}_{\mathrm{III},\imath}$ and $\boldsymbol{x}_{\mathrm{III},l}$. The expectation term in (83) can be further approximated by $(1 + \frac{\zeta_2}{2\sigma^2})^{-\zeta_1}$, where ζ_1 is the shape parameter and ζ_2 denotes the scale parameter of the approximated Gamma variable $\|\boldsymbol{D}_{\mathrm{III}}(\boldsymbol{x}_{\mathrm{III},\imath} - \boldsymbol{x}_{\mathrm{III},l})\|^2$.

Proof: The proof follows from the following derivation

$$\epsilon_3 \leq \frac{1}{|\mathcal{M}|\log|\mathcal{M}|}\sum_{\imath=1}^{|\mathcal{M}|}\sum_{l=1}^{|\mathcal{M}|} d(\boldsymbol{x}_{\mathrm{III},\imath},\boldsymbol{x}_{\mathrm{III},l}) \times\mathbb{E}_{\boldsymbol{D}_{\mathrm{III}}}\{p(\boldsymbol{x}_{\mathrm{III},\imath}\rightarrow\boldsymbol{x}_{\mathrm{III},l}|\boldsymbol{D}_{\mathrm{III}})\} \quad (84)$$

$$= \frac{1}{|\mathcal{M}|\log|\mathcal{M}|}\sum_{\imath=1}^{|\mathcal{M}|}\sum_{l=1}^{|\mathcal{M}|} d(\boldsymbol{x}_{\mathrm{III},\imath},\boldsymbol{x}_{\mathrm{III},l}) \times\mathbb{E}_{\boldsymbol{D}_{\mathrm{III}}}\left\{Q\left(\sqrt{\frac{\|\boldsymbol{D}_{\mathrm{III}}(\boldsymbol{x}_{\mathrm{III},\imath}-\boldsymbol{x}_{\mathrm{III},l})\|^2}{2\sigma^2}}\right)\right\} \quad (85)$$

where $p(\boldsymbol{x}_{\mathrm{III},\imath}\rightarrow\boldsymbol{x}_{\mathrm{III},l}|\boldsymbol{D}_{\mathrm{III}})$ represents the conditional pairwise error probability with respect to the channel $\boldsymbol{D}_{\mathrm{III}}$; $Q(\cdot)$ denotes the Gaussian Q function. The inequality (84) follows from the union bound technique and (85) derives from

$$p(\boldsymbol{x}_{\mathrm{III},\imath}\rightarrow\boldsymbol{x}_{\mathrm{III},l}|\boldsymbol{D}_{\mathrm{III}}) = p(\|\boldsymbol{y}_{\mathrm{III}}-\boldsymbol{D}_{\mathrm{III}}\boldsymbol{x}_{\mathrm{III},\imath}\|^2 > \|\boldsymbol{y}_{\mathrm{III}}-\boldsymbol{D}_{\mathrm{III}}\boldsymbol{x}_{\mathrm{III},l}\|^2|\boldsymbol{D}_{\mathrm{III}}) \quad (86)$$

$$= Q\left(\sqrt{\frac{\|\boldsymbol{D}_{\mathrm{III}}(\boldsymbol{x}_{\mathrm{III},\imath}-\boldsymbol{x}_{\mathrm{III},l})\|^2}{2\sigma^2}}\right). \quad (87)$$

Let $\tau = \|\boldsymbol{D}_{\mathrm{III}}(\boldsymbol{x}_{\mathrm{III},\imath}-\boldsymbol{x}_{\mathrm{III},l})\|^2$, which is the summation of multiple positive variables. Thus the probability density of τ can be approximated by a Gamma distribution. With the moment generating function of the Gamma variate, the expectation term can be further written as $\mathbb{E}_\tau\{Q(\sqrt{\frac{\tau}{2\sigma^2}})\} = \frac{2}{\pi}\int_0^{\pi/2}\left(1+\frac{\zeta_2}{2\sigma^2\sin^2\theta}\right)^{-\zeta_1}d\theta \leq (1+\frac{\zeta_2}{2\sigma^2})^{-\zeta_1}$. ∎

Remark 5: Since the effective channel is diagonalized, the transceive antennas are one-to-one paired. For the proposed RIS-enabled secure SSK and PSK schemes, the diversity order is one. As for the proposed RIS-enabled secure QSSK scheme, the diversity order is 0.5 since the received signals are independently and non-coherently detected by the in-phase and quadrature components. The insights of our BER analysis are two-fold. First, the derived BER expressions match well with the numerical results. Thus it provides a benchmark for conducting further research to enhance the reliability of the proposed transmission schemes. For example, antenna selection techniques can be employed for minimizing the BER. Otherwise, time-consuming Monte-Carlo simulations would be demanded. Second, the BER expression of the proposed scheme III reveals that the diversity gain can be approximated by ζ_1.

V. Numerical Results

In this section, we evaluate the performances of the three proposed schemes with respect to different parameter settings. We assume that the noise levels at Bob and Eve are the same, i.e., $\sigma^2 = \gamma^2$. The SNR in the simulations is defined by the transmit power of Alice divided by the noise power. In each transmission block, the elements of $\boldsymbol{H}$ are independently drawn from $\mathcal{CN}(0,1)$. The direct link between Alice and Eve are modeled as a Rician fading channel with a Rician factor 10 and a channel gain ξ. We assume that the channels from RIS to Bob and from RIS to Eve are spatially correlated and use the exponential correlation model with a correlation factor ρ to characterize the correlation. For the proposed RIS-enabled secure PSK transmission, the RIS is divided into two equal sub-arrays to perform the reflection independently. The free variables updated at the RIS are independently drawn from a uniform distribution $\mathcal{U}(0,1)$. The key findings are as follows.

Observation 1*: For all the proposed three secure transmission schemes, the information transmitted from Alice can be reliably recovered at Bob, while being undecodable at Eve. Eve's BER does not improve as the SNR increases even with a strong direct link and a correlated channel. Moreover, the analytical BER of Bob matches well with the numerical results (cf. Figure 5).*

The BER performances of Bob and Eve are evaluated for the three proposed schemes, and the results are presented in Figure 5. Four conclusions are as follows. First, in all the three proposed schemes, Bob can reliably retrieve the confidential messages and the diversity orders are approximately 1, 0.5, and 1. This is due to the diagonal effective channels observed at Bob, which enables Bob to recover the secret information by identifying the power profiles or the phases of the received signals. Second, the BER of Eve remains at a high level and does not improve as the SNR increases, even with a strong direct link and a highly correlated channel. Although the BER of Eve decreases as the channel gain of the direct link increases, she is still unable to recover the useful information. This is due to the reflection at the RIS, which is intractable to Eve and results in severe channel uncertainty. Moreover, since the reflection at the RIS operates as a random matrix multiplied with the transmitted signals, Eve cannot cancel out the multiplicative randomness even at high SNR. Third, as expected, the reliability of the proposed transmission schemes improves as the reflection efficiency increases since less power is dissipated. Fourth, the analytical BER of Bob matches well with the numerical results.

Observation 2*: The proposed random reflection methods significantly outperform the conventional beamforming and artificial noise techniques in secrecy rate at high SNR (cf. Figure 6).*

We compare the secrecy rates of the proposed random reflection schemes, the conventional beamforming techniques, and the artificial noise based schemes in Figure 6. The workflow of the beamforming schemes with finite-alphabet input and Gaussian input could be found in algorithm 1 of [27] and Section III-B of [13], respectively. In the beamforming techniques, we assume that Alice has perfect knowledge of the wiretap channel. For the beamforming techniques with finite-alphabet input, the secrecy rates first increase up to the corresponding maximum values, and then reduce gradually to zero as the SNR increases. On the other hand, the secrecy rates of the proposed reflection schemes keep growing before saturation at high SNR. Therefore, the secrecy performances of the proposed schemes significantly outperform that of the beamforming schemes in the high SNR region. The reasons are as follows. Using RIS for beamforming, we aim to degrade the quality of Eve's reception by adding the direct signals and the reflected signals destructively. However, as the signal power increases, the achievable rate of Eve saturates at the upper bound $\log|\mathcal{M}|$ when assuming finite-alphabet input, leading to

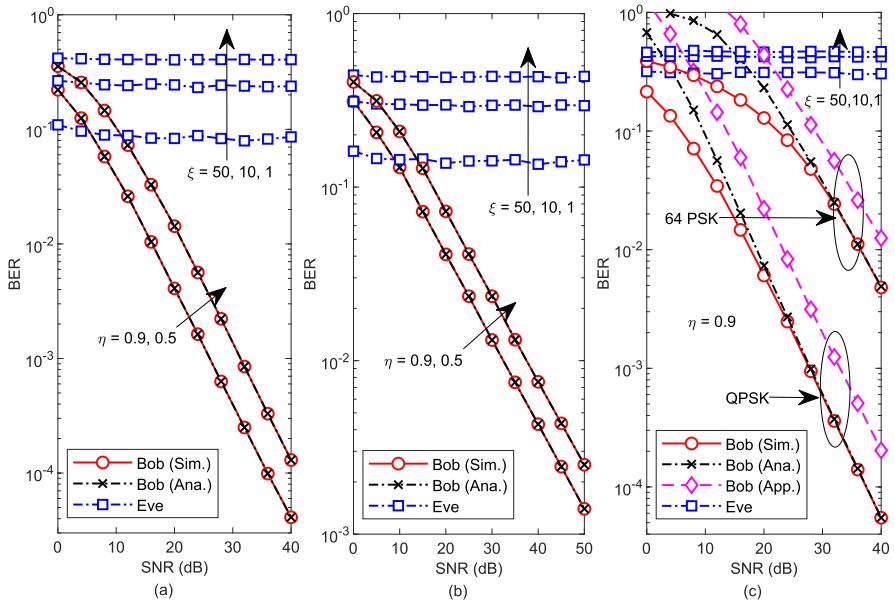


Fig. 5. BER performances of Bob and Eve are evaluated for (a) the RIS-enabled secure SSK scheme, (b) the RIS-enabled secure QSSK scheme, and (c) the RIS-enabled secure PSK scheme, where $L = 4$, $K = M = 2$. The channel correlation factor is $\rho = 0.5$. The number of reflecting elements of the RIS is $N = 16$. The Rician factor is 10. The results show that for all the proposed three secure transmission schemes, the information transmitted from Alice can be reliably recovered at Bob, while being undecodable at Eve. The abbreviations Ana., Sim., and App. represent analytical, simulation, and approximate, respectively. The analytical results are obtained via numerically evaluating the integrals in (65), (75), and (83). The approximate results are obtained by the Gamma approximation.

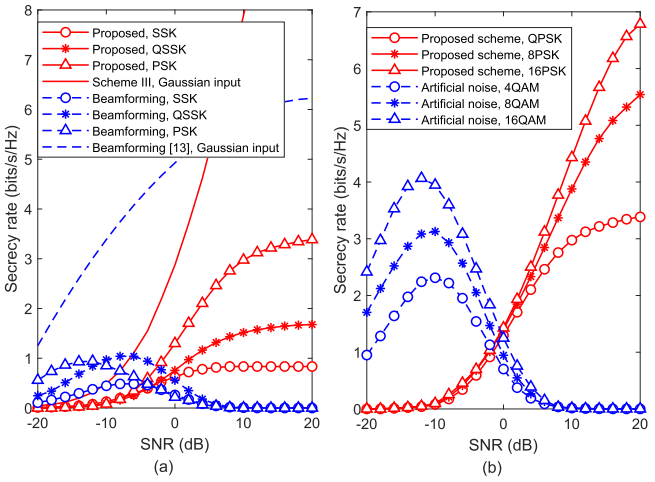


Fig. 6. The secrecy rates of the proposed schemes are compared with (a) the beamforming based scheme and (b) the artificial noise based scheme, where $L = 4$, $K = M = 2$. The number of reflecting elements is $N = 16$. The reflection efficiency is $\eta = 0.9$. The channel correlation factor is $\rho = 0.5$. The "Scheme III, Gaussian input" refers to the scheme in which the input is Gaussian and the reflection coefficients are obtained from the proposed scheme III. The scheme "Beamforming [13], Gaussian input" refers to the scheme of [13]. The numerical results show the secrecy rates of the proposed random reflection schemes significantly outperform that of the beamforming and the artificial noise schemes in the high SNR region.

a zero secrecy rate. For the proposed scheme III with Gaussian input, since the reflection matrix contains a certain degree of randomness and is kept secret at the RIS, Eve lacks necessary side information and the reflected signals received at Eve are treated as random interferences. As the transmitted power increases, the power of the random interferences will also be enhanced. In contrast, for the conventional beamforming scheme, the reflected signals received at Eve are regarded as useful signals. Therefore, the proposed scheme achieves a higher secrecy rate at high SNR. For the artificial noise based schemes, we assume the artificial noise follows from the CSCG distribution $\mathcal{CN}(\mathbf{0}, \boldsymbol{I})$. The results show that as the power of the useful signals grows, the secrecy rates first rise and then reach their peak values, and finally drop to zero. The reason is that as the SNR grows, the power of the useful signal overwhelms that of the artificial noise and thus the achievable rate of Eve can reach its upper bound at a sufficiently high SNR, i.e., $\log|\mathcal{M}|$. Since the achievable rate of Bob is also upper-bounded by $\log|\mathcal{M}|$, the secrecy rate will drop to zero at high SNR. In contrast, in the proposed schemes, the reflected signals received by Eve actually act as an intractable interference, which cannot be canceled even at high SNR. As the SNR increases, Bob's achievable rate keeps growing and a high secrecy rate can be achieved.

***Observation 3**: For a given number of reflecting elements, the proposed RIS-enabled secure PSK scheme outperforms the other two counterparts in both spectral efficiency and* DoR*, especially when using a higher modulation order (cf. Figure 7).*

In Figure 7, we evaluate the DoR with respect to the spectral efficiency for different schemes. We can see that for a given number of reflecting elements, the DoR decreases as the spectral efficiency increases. In addition, the proposed RIS-enabled secure PSK scheme outperforms the other two counterparts in both spectral efficiency and DoR, especially when using a higher modulation order. For example, when BPSK modulation is employed, the RIS-enabled secure PSK scheme can achieve a spectral efficiency of 7 bits/s/Hz and a

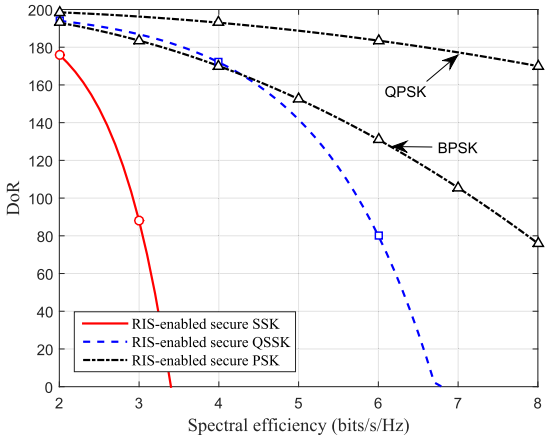


Fig. 7. The DoR is evaluated with respect to the spectral efficiency for different schemes. The number of reflecting elements is $N = 100$. The RIS-enabled PSK scheme uses the BPSK and QPSK modulations, respectively. It shows that for a given number of reflecting elements, the proposed RIS-enabled secure PSK scheme outperforms the other two counterparts in both spectral efficiency and DoR, especially when using a higher modulation order.

DoR of 105.5, which shows a clear advantage over the other two schemes. The performance gains are enlarged when QPSK modulation is employed. The RIS-enabled secure PSK scheme can further realize a spectral efficiency of 8 bits/s/Hz and a DoR of 170. However, we also note that the RIS-enabled secure QSSK scheme can achieve higher DoR at low spectral efficiencies. For example, at a spectral efficiency of 4 bits/s/Hz, a DoR of 172 is available for the RIS-enabled secure QSSK scheme, while the DoR is 170 for the RIS-enabled secure PSK scheme. From Figures 6 and 7, the proposed three schemes achieve a different balance amongst the spectral efficiency, DoR, and reliability, which can meet diverse requirements in practical scenarios. If Eve uses a brute-force attack, its search space is determined by the DoR and the number of possible values of each free parameter. For example, assume $N = 32$, $K = 4$. Each free parameter has 256 realizations. The search space reaches 40^{256}, which imposes a prohibitively high computational burden. It is possible to deploy an even larger number of reflecting elements with sufficiently precise reflecting coefficients. The complexity of the brute-force search attack could be even more unaffordable.

VI. Conclusion

In this article, we have investigated the reflection of RIS as a multiplicative randomness against a passive eavesdropper. The security is achieved without knowing the wiretap channel. The idea is to update the reflection coefficients while guaranteeing the legitimate channel matrix diagonalized. Since the reflection coefficients are updated in each transmission and kept private at the RIS, we have a one-time pad system. We provided three reflection designs and three secure transmission schemes, and the performance metrics including DoR, spectral efficiency, and BER are analyzed. The multiplicative randomness outperforms the conventional additive randomness methods in power-efficiency since no artificial interference is sent. The ramification of this article reveals that using RIS as a multiplicative randomness is a new perspective to improve the secrecy of wireless networks.

References

[1] M. L. Aho and K. Leppanen, "Key drivers and research challenges for 6G ubiquitous wireless intelligence," 6G Flagship, Univ. Oulu, Oulu, Finland, White Paper, Sep. 2019. [Online]. Available: http://urn.fi/urn:isbn:9789526223544

[2] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 162–169, Sep. 2018.

[3] S. Gong *et al.*, "Towards smart radio environment for wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2283–2314, 4th Quart., 2020.

[4] 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.

[5] W. Yan, X. Yuan, Z.-Q. He, and X. Kuai, "Passive beamforming and information transfer design for reconfigurable intelligent surfaces aided multiuser MIMO systems," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1793–1808, Aug. 2020.

[6] G. Yang, Y.-C. Liang, R. Zhang, and Y. Pei, "Modulation in the air: Backscatter communication over ambient OFDM carrier," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 1219–1233, Mar. 2018.

[7] S. Guo, S. Lv, H. Zhang, J. Ye, and P. Zhang, "Reflecting modulation," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2548–2561, Nov. 2020.

[8] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *Proc. IEEE Global Commun. Conf.*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.

[9] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, Oct. 2019.

[10] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1488–1492, Sep. 2019.

[11] K. Feng, X. Li, Y. Han, S. Jin, and Y. Chen, "Physical layer security enhancement exploiting intelligent reflecting surface," 2019, *arXiv:1911.02766*. [Online]. Available: http://arxiv.org/abs/1911.02766

[12] Z. Chu, W. Hao, P. Xiao, and J. Shi, "Intelligent reflecting surface aided multi-antenna secure transmission," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, Jan. 2020.

[13] W. Jiang, Y. Zhang, J. Wu, W. Feng, and Y. Jin, "Intelligent reflecting surface assisted secure wireless communications with multiple-transmit and multiple-receive antennas," *IEEE Access*, vol. 8, pp. 86659–86673, 2020.

[14] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jun. 2020.

[15] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599–82612, Jul. 2019.

[16] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2637–2652, Nov. 2020.

[17] Q. Li, H. Song, and K. Huang, "Achieving secure transmission with equivalent multiplicative noise in MISO wiretap channels," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 892–895, May 2013.

[18] S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst, "Secret channel training to enhance physical layer security with a full-duplex receiver," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2788–2800, Nov. 2018.

[19] Z.-Q. He and X. Yuan, "Cascaded channel estimation for large intelligent metasurface assisted massive MIMO," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 210–214, Feb. 2020.

[20] J. W. Wal 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.

[21] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying systems," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 650–660, Sep. 2011.

[22] J. Jeganathan, A. Ghrayeb, L. Szczecinski, and A. Ceron, "Space shift keying modulation for MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3692–3703, Jul. 2009.

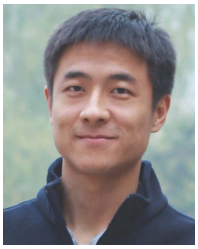
[23] R. Mesleh and A. Alhassi, *Space Modulation Techniques*. Hoboken, NJ, USA: Wiley, 2018.
[24] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge Univ. Press, 2004.
[25] M. S. John Proakis, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2008.
[26] R. Zhang, L.-L. Yang, and L. Hanzo, "Error probability and capacity analysis of generalised pre-coding aided spatial modulation," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 364–375, Jan. 2015.
[27] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2599–2612, Jul. 2012.
[28] Q. Wu and R. Zhang, "Beamforming optimization for wireless network aided by intelligent reflecting surface with discrete phase shifts," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1838–1851, Mar. 2020.
[29] H. Liu, X. Yuan, and Y.-J.-A. Zhang, "Matrix-calibration-based cascaded channel estimation for reconfigurable intelligent surface assisted multiuser MIMO," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2621–2636, Nov. 2020.
[30] B. Zheng and R. Zhang, "Intelligent reflecting surface-enhanced OFDM: Channel estimation and reflection optimization," *IEEE Wireless Commun. Lett.*, vol. 9, no. 4, pp. 518–522, Apr. 2020.
[31] M. Nemati, J. Ding, and J. Choi, "Short-range ambient backscatter communication using reconfigurable intelligent surfaces," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Seoul, South Korea, May 2020, pp. 1–6.
[32] C. You, B. Zheng, and R. Zhang, "Intelligent reflecting surface with discrete phase shifts: Channel estimation and passive beamforming," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dublin, Ireland, Jun. 2020, pp. 1–6.
[33] H. Wan, W. Chen, and X. Wang, "Joint source and relay design for MIMO relaying broadcast channels," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 345–348, Feb. 2013.
[34] L. Chen, S. Han, W. Meng, C. Li, and M. Berhane, "Power allocation for single-stream dual-hop full-duplex decode-and-forward MIMO relay," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 740–743, Apr. 2016.
[35] S. Gong, C. Xing, N. Yang, Y.-C. Wu, and Z. Fei, "Energy efficient transmission in multi-user MIMO relay channels with perfect and imperfect channel state information," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3885–3898, Jun. 2017.
[36] D. Wang and F. Wang, "Wireless MIMO switching with imperfect CSI in frequency and time division duplex," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2579–2590, May 2019.

Junshan Luo received the B.S. and M.S. degrees in information and communications engineering from the National University of Defense Technology (NUDT), Changsha, China, in 2014 and 2016, respectively, where he is currently pursuing the Ph.D. degree with the College of Electronic Science and Technology. His current research interests include reconfigurable intelligent surface, spatial modulation, massive MIMO, and physical layer security.

Fanggang Wang (Senior Member, IEEE) received the B.S. and Ph.D. degrees from the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China, in 2005 and 2010, respectively. He was a Post-Doctoral Fellow with the Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong, from 2010 to 2012. He was a Visiting Scholar with the Massachusetts Institute of Technology from 2015 to 2016 and the Singapore University of Technology and Design in 2014. He is currently a Professor with the State Key Laboratory of Rail Traffic Control and Safety, School of Electronic and Information Engineering, Beijing Jiaotong University. His research interests include wireless communications, signal processing, and information theory. He served as a technical program committee member for several conferences and as an Editor for the IEEE COMMUNICATIONS LETTERS.

Shilian Wang (Member, IEEE) received the B.S. and Ph.D. degrees in information and communication engineering from the National University of Defense Technology, in 1998 and 2004, respectively. Since 2004, he has been with the School of Electronic Science, National University of Defense Technology, as a Lecturer, an Associate Professor, and a Professor. From 2008 to 2009, he was a Visiting Scholar with the Department of Electronic and Electrical Engineering, Columbia University (CU), New York. His research interests include wireless communications and signal processing, specifically in the spread spectrum and the low-probability of interception communications.

Hao Wang received the B.S., M.E., and Ph.D. degrees in information and communication engineering from the National University of Defense Technology, in 2012, 2014, and 2018, respectively. Since 2018, he has been a Lecturer with the College of Electronic Science and Technology, National University of Defense Technology. His research interests include network coding, cooperative communications, and channel estimation.



Dong Wang received the B.S. degree from the School of Electronic and Information Engineering, Hebei University, Baoding, China, in 2016. He is currently pursuing the Ph.D. degree with the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China. His current research interests include multiway relaying communications and MIMO communications.