Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Pattern-reconfigurable antenna-assisted secret key generation from multipath fading channels*

Zheng WAN†1, Mengyao YAN1, Kaizhi HUANG†‡1,2, Zhou ZHONG1, Xiaoming XU1, Yajun CHEN1, Fan WU2

[1]*PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China*

[2]*Purple Mountain Laboratories for Network and Communication Security, Nanjing 210096, China*

†E-mail: wanzheng18@alumni.hust.edu.cn; huangkaizhi@tsinghua.org.cn

Received Feb. 28, 2023; Revision accepted Sept. 3, 2023; Crosschecked Dec. 19, 2023

Abstract: Physical layer key generation (PKG) technology leverages reciprocal channel randomness to generate shared secret keys. However, multipath fading at the receiver may degrade the correlation between legitimate uplink and downlink channels, resulting in a low key generation rate (KGR). In this paper, we propose a PKG scheme based on the pattern-reconfigurable antenna (PRA) to boost the secret key capacity. First, we propose a reconfigurable intelligent surface (RIS) based PRA architecture with the capability of flexible and reconfigurable antenna patterns. Then, we present the PRA-based PKG protocol to improve the KGR via mitigation of the effects of multipath fading. Specifically, a novel algorithm for estimation of the multipath channel parameters is proposed based on atomic norm minimization. Thereafter, a novel optimization method for the matching reception of multipath signals is formulated based on the improved binary particle swarm optimization (BPSO) algorithm. Finally, simulation results show that the proposed scheme can resist multipath fading and achieve a high KGR compared to existing schemes. Moreover, our findings indicate that the increased degree of freedom of the antenna patterns can significantly increase the secret key capacity.

Key words: Physical layer security; Secret key generation; Reconfigurable intelligent surface; Multipath fading; Pattern-reconfigurable antenna

https://doi.org/10.1631/FITEE.2300126 **CLC number:** TN918

1 Introduction

The inherent broadcast nature of wireless media renders them vulnerable to diverse attacks from potential eavesdroppers (Ji XS et al., 2022). Compared with traditional cryptography techniques with high computational complexity and high delays, physical layer key generation (PKG) provides an alternative idea to establish symmetric keys between legitimate parties. By leveraging the inherent randomness and reciprocity of wireless channels, PKG can achieve theoretical information security (Jin et al., 2021). However, the key generation rate (KGR) can hardly be guaranteed in some harsh propagation scenarios, such as low mobility or low signal-to-noise ratio (SNR) propagation environments.

Recently, the emergence of reconfigurable intelligent surface (RIS) has provided a promising means to address the problems mentioned above. RIS has the ability to control electromagnetic wave characteristics such as phase, amplitude, and polarization, through changes in the state of each element, which can dynamically program and reconstruct wireless environments in real time (Cheng et al., 2022). Since the key generation performance relies on the received

‡ Corresponding author

* Project supported by the National Key Research and Development Program of China (Nos. 2022YFB2902202 and 2022YFB2902205) and the National Natural Science Foundation of China (No. U22A2001)

ORCID: Zheng WAN, https://orcid.org/0000-0003-4547-5918; Kaizhi HUANG, https://orcid.org/0000-0002-7084-3826

signal power, RIS could be the critical enabler for improving the KGR. Inspired by this, several studies on RIS-assisted PKG systems have been conducted. Ji ZJ et al. (2021) and Hu et al. (2022) designed passive and active beamforming in the RIS-assisted key generation system, which can enhance the correlation between legitimate uplink and downlink channels. Furthermore, a two-path propagation model for RIS-assisted wireless communications was considered in Zhou et al. (2022). The proposed experimental results revealed that the phase shifts of RISs can be optimized by appropriate configuration for multipath fading mitigation. Zhang HL et al. (2021) exploited the potential of the RIS as a spatial equalizer to address multipath fading. However, the main difficulty is that a RIS can neither send nor receive pilots, so channel estimation is challenging.

Fortunately, another more active application of RIS is the merging of RISs and radio frequency (RF) chains, so that they become the receiving RISs with baseband reception capability (Alexandropoulos and Vlachos, 2020; Jian et al., 2022; Lu et al., 2022). Meanwhile, the dynamic metasurface antenna (DMA) with beam-tailoring capabilities has been conceptualized in parallel works (Shlezinger et al., 2021; Lou et al., 2022; Wu GB et al., 2022). The receiving RISs and DMA with beam-tailoring capabilities are promising means of implementing the pattern-reconfigurable antenna (PRA). By effectively and rapidly changing the radiation pattern in a software-programmable manner (Wu W et al., 2019; Dai et al., 2020), PRA has the ability to combat fast fading and thus improves the receiving performance.

Motivated by the above works, we propose a novel RIS-based PRA architecture with flexible and reconfigurable antenna patterns. Different from the design of the RIS as a reflecting surface, we mitigate the effects brought about by multipath fading at the receivers. Based on this PRA architecture, we propose a key generation scheme to improve the secret key capacity by increasing the correlation between legitimate uplink and downlink channels. Our main technical contributions are as follows:

1. We propose a novel RIS-based PRA architecture. Different from conventional antennas with a fixed antenna pattern and concentrating energy in the directions of the target, to overcome the effect of multipath fading, PRA can optimize the antenna pattern in real time according to the multipath signal to change the way of the multipath superposition.

2. We propose a novel PRA-based PKG protocol. Specifically, a novel algorithm for the estimation of the multipath channel parameters is proposed based on atomic norm minimization (ANM). Then, a novel optimizing method for RIS configuration code is formulated based on the improved binary particle swarm optimization (BPSO) algorithm to match multipath signals. Finally, secret keys are generated at a high rate from the multipath fading channel.

3. Simulation results show that the proposed method can resist multipath fading and achieve a low key disagreement ratio (KDR). The secret key capacity of the proposed scheme is greatly improved compared with that of existing schemes. Moreover, our findings indicate that the higher the degree of freedom of the antenna patterns, the higher the secret key capacity.

Notations: In this paper, a bold lowercase $\boldsymbol{a}$ denotes a column vector, and a bold uppercase $\boldsymbol{A}$ denotes a matrix. We use $(\cdot)^{\mathrm{T}}$, $(\cdot)^{\mathrm{H}}$, $(\cdot)^{*}$, and $(\cdot)^{\dagger}$ to denote the matrix transpose, conjugate transpose, element-wise conjugate, and pseudoinverse operators, respectively. We use $|\cdot|$ to denote the absolute value, "$\odot$" to denote the product of elements, and $\mathrm{diag}\,(\cdot)$ to diagonalize a vector. $\angle(\cdot)$ denotes the phase of a complex vector. Here, $E(X)$ represents the expectation operator of the random variable X, and $I(X;Y)$ represents the mutual information between X and Y.

2 System and channel model

As shown in Fig. 1, we consider a narrowband time-division duplexing (TDD) communication system, wherein a base station (BS) Alice and a user Bob aim to extract consistent keys from the wireless channel. Alice is equipped with a PRA, and Bob is a single-antenna user. Meanwhile, a passive eavesdropper Eve is several wavelengths away from Bob. It is assumed that Eve has knowledge of the secret key generation process and intends to obtain the key information from signals she received. The wireless channel between Alice and Bob is modeled as the typical Saleh–Valenzuela channel model, in which the signal travels through L resolvable paths to reach the receiver. The multipath fading channel changes randomly with the propagation environment and the relative position of the transceiver. Since

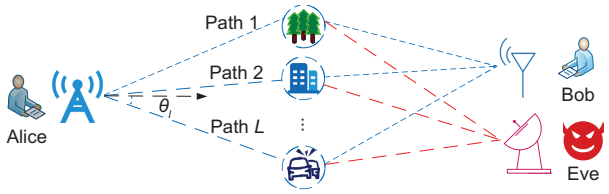

Fig. 1 System and channel model

Eve is located at a distance of more than half a wavelength from Bob, the channel of Eve is uncorrelated from that of Bob.

3 Proposed RIS-based PRA architecture

In the conventional phased array architecture illustrated in Fig. 2a, the number of required phase shifters is proportional to the number of RF chains and the number of antennas. However, in next-generation communication systems, the number of antennas at the BS is usually 128 or 256. Therefore, the traditional phased array architecture suffers high costs due to the presence of numerous RF chains. In addition, each element of the phased array has the same structure and the fixed antenna pattern. When the electromagnetic waves of multipath signals reaching the receiving antenna are out of phase, the signal strength at the receiver is reduced. The fixed antenna pattern cannot mitigate or eliminate the influence of multipath fading at the array elements. The information loss of the received signal at the analog front end also cannot be compensated by digital baseband processing.

The proposed RIS-based PRA architecture is shown in Fig. 2b. Unlike existing arrays that maintain a fixed structure, PRA is a single-channel antenna, in which the PRA elements control patterns in terms of shape, direction, or gain. The proposed PRA consists of N PRA elements, and each PRA element is uniformly linearly arranged with a spacing d_{A}. Specifically, each PRA element is implemented by a single receiving RF chain RIS (Alexandropoulos and Vlachos, 2020; Alexandropoulos et al., 2022) containing M low-cost sub-wavelength metamaterial elements. All RIS elements are arranged with spacing d_{B} and coupled with a waveguide. The waveguide output is connected to a phase shifter. All phase shifters are fed to one RF chain to form a single-channel PRA.

In the far-field signal propagation scenario, the

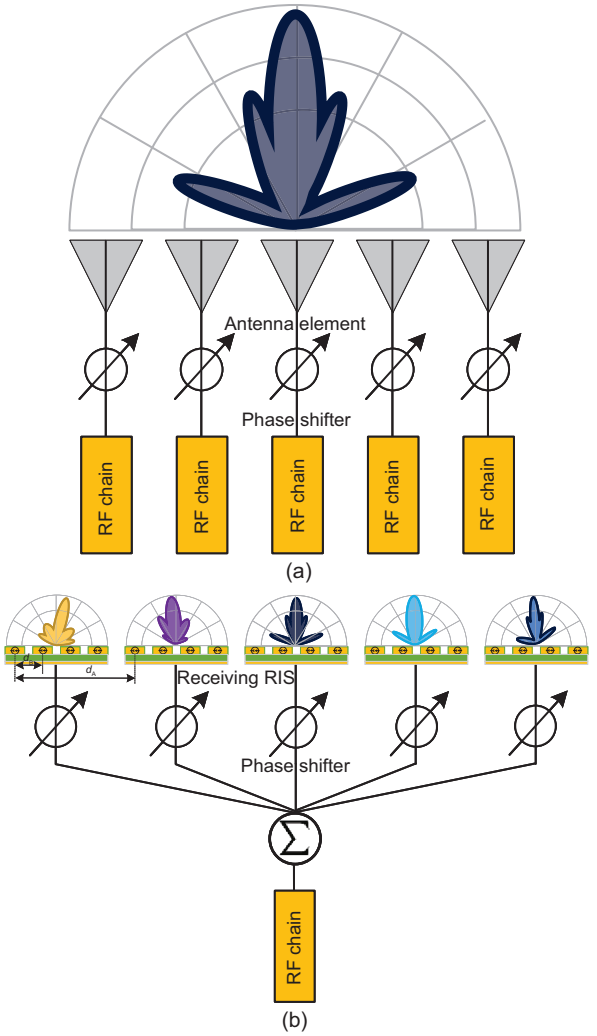

Fig. 2 Comparison of two array architectures: (a) a conventional phased array architecture; (b) the proposed pattern-reconfigurable antenna architecture

channel from Alice to Bob is presented as follows:

$$h_{\mathrm{AB}}=\sum_{n=1}^{N}\omega_n\sum_{l=1}^{L}\phi_n\left(\theta_l\right)g_{\mathrm{AB},l}\mathrm{e}^{\mathrm{j}\frac{2\pi(n-1)d_{\mathrm{A}}}{\lambda}\sin\theta_l},\quad(1)$$

where L is the number of distinct multipaths, and $g_{\mathrm{AB},l}$ and θ_l denote the complex path gain and direction-of-arrival (DOA) of the l^{th} path, respectively. Moreover, $\phi_n\left(\theta_l\right)$ represents the antenna pattern response of the n^{th} reconfigurable antenna with respect to θ_l, and ω_n is the phase shift of the n^{th} phase shifter. Similarly, considering channel reciprocity in TDD systems, the channel from Bob to Alice is expressed as follows:

$$h_{\mathrm{BA}}=\sum_{n=1}^{N}\omega_n\sum_{l=1}^{L}\phi_n\left(\theta_l\right)g_{\mathrm{BA},l}\mathrm{e}^{\mathrm{j}\frac{2\pi(n-1)d_{\mathrm{A}}}{\lambda}\sin\theta_l},\quad(2)$$

where $g_{\mathrm{BA},l}$ is the path gain of the uplink channel and $g_{\mathrm{AB},l}=g_{\mathrm{BA},l}$. Eqs. (1) and (2) can be represented in matrix form as follows:

$$h_{\mathrm{AB}}=h_{\mathrm{BA}}=\boldsymbol{\omega}^{\mathrm{T}}\left[\boldsymbol{A}\left(\boldsymbol{\theta}\right)\odot\boldsymbol{\Phi}\left(\boldsymbol{\theta}\right)\right]\boldsymbol{g}, \tag{3}$$

where $\boldsymbol{\omega}\triangleq[\omega_1,\omega_2,\cdots,\omega_N]^{\mathrm{T}}$, $\boldsymbol{g}\triangleq[g_1,g_2,\cdots,g_L]^{\mathrm{T}}$, $\boldsymbol{\theta}\triangleq[\theta_1,\theta_2,\cdots,\theta_L]^{\mathrm{T}}$, $\boldsymbol{\Phi}(\boldsymbol{\theta})\triangleq[\boldsymbol{\phi}_1(\boldsymbol{\theta}),\boldsymbol{\phi}_2(\boldsymbol{\theta}),\cdots,\boldsymbol{\phi}_N(\boldsymbol{\theta})]^{\mathrm{T}}\in\mathbb{C}^{N\times L}$, and $\boldsymbol{A}(\boldsymbol{\theta})\triangleq[\boldsymbol{a}(\theta_1),\boldsymbol{a}(\theta_2),\cdots,\boldsymbol{a}(\theta_L)]\in\mathbb{C}^{N\times L}$. The array response vector and antenna pattern response of the reconfigurable antenna are presented as $\boldsymbol{a}\left(\theta_l\right)=\left[1,\mathrm{e}^{\mathrm{j}\frac{2\pi d_{\mathrm{A}}}{\lambda}\sin\theta_l},\mathrm{e}^{\mathrm{j}\frac{2\pi 2d_{\mathrm{A}}}{\lambda}\sin\theta_l},\cdots,\mathrm{e}^{\mathrm{j}\frac{2\pi(N-1)d_{\mathrm{A}}}{\lambda}\sin\theta_l}\right]^{\mathrm{T}}$ and $\boldsymbol{\phi}\left(\boldsymbol{\theta}\right)\triangleq\left[\phi\left(\theta_1\right),\phi\left(\theta_2\right),\cdots,\phi\left(\theta_L\right)\right]^{\mathrm{T}}$, respectively.

4 Proposed PRA-based PKG scheme

In this section, a PRA-based PKG scheme is proposed, which includes three main steps: the BS estimates the multipath channel parameters; the BS configures the optimal pattern to maximize the receiving SNR; the BS and the user generate secret keys from channel measurements. The logic flow of the proposed scheme is shown in Fig. 3.

4.1 Estimation of multipath channel parameters

In this subsection, we propose a novel algorithm for the estimation of multipath channel parameters based on ANM for a single-channel PRA, which can approach the capability of a conventional multiantenna array. PRA generates a series of random antenna patterns to sense the incident signals within a single pilot symbol period, which are subsequently processed by the ANM algorithm to recover the DOA and path gain information based on the equivalent multi-dimensional received signals.

Assume that the DOA and path gain are approximately constant during the short sensing time. Bob first sends the pilot symbol x to Alice, and then Alice samples K times within a single symbol with different receiving patterns by adjusting the phase shifters. The received multipath signal is expressed as follows:

$$\boldsymbol{y}_{\mathrm{A}}=\boldsymbol{\Omega}^{\mathrm{T}}\left[\boldsymbol{A}\left(\boldsymbol{\theta}\right)\odot\boldsymbol{\Phi}\left(\boldsymbol{\theta}\right)\right]\boldsymbol{g}x+\boldsymbol{n}_{\mathrm{A}}, \tag{4}$$

where $\boldsymbol{\Omega}\triangleq[\boldsymbol{\omega}_1,\boldsymbol{\omega}_2,\cdots,\boldsymbol{\omega}_K]\in\mathbb{C}^{N\times K}$ is the phase shift matrix, and $\boldsymbol{n}_{\mathrm{A}}\triangleq[n_{\mathrm{A},1},n_{\mathrm{A},2},\cdots,n_{\mathrm{A},K}]^{\mathrm{T}}\in\mathbb{C}^{K\times 1}$ is the additive white Gaussian noise (AWGN) following $n_{\mathrm{A},k}\sim\mathcal{CN}\left(0,\sigma_n^2\right)$, $k\in\{1,2,\cdots,K\}$. The least squares (LS) algorithm is used to estimate the channel as follows:

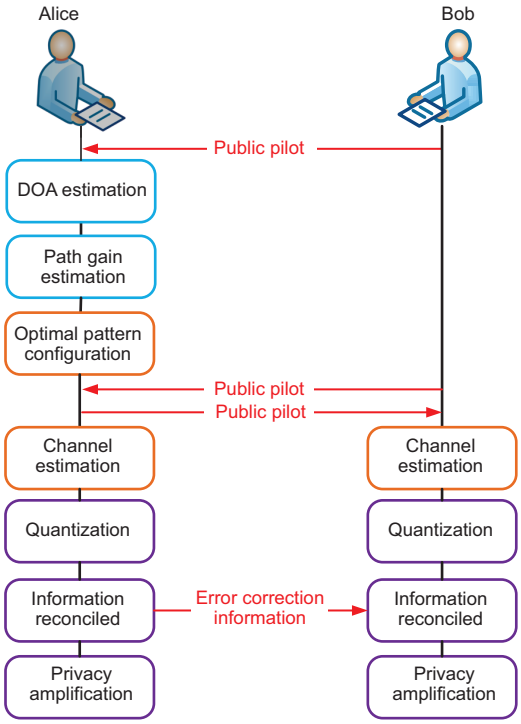

Fig. 3 Logic flow of the proposed PRA-based PKG scheme

$$\hat{\boldsymbol{h}}_{\mathrm{BA}}=\frac{\boldsymbol{y}_{\mathrm{A}}}{x}=\boldsymbol{\Omega}^{\mathrm{T}}\left[\boldsymbol{A}\left(\boldsymbol{\theta}\right)\odot\boldsymbol{\Phi}\left(\boldsymbol{\theta}\right)\right]\boldsymbol{g}+\boldsymbol{\varepsilon}, \tag{5}$$

where $\boldsymbol{\varepsilon}\triangleq[\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_K]^{\mathrm{T}}$ is the channel estimation error following $\varepsilon_k\sim\mathcal{CN}\left(0,\sigma_n^2/P_x\right)$, and P_x is the power of the pilot symbol. We set $\boldsymbol{\Omega}$ to a Hadamard matrix due to $\boldsymbol{\Omega}^{\dagger}=\boldsymbol{\Omega}^{-1}=\frac{1}{N}\boldsymbol{\Omega}^{\mathrm{H}}$. Thus, we can reconstruct the multi-channel received signal as follows:

$$\tilde{\boldsymbol{h}}_{\mathrm{BA}}=\left(\boldsymbol{\Omega}^{\mathrm{T}}\right)^{\dagger}\hat{\boldsymbol{h}}_{\mathrm{BA}}=\left[\boldsymbol{A}\left(\boldsymbol{\theta}\right)\odot\boldsymbol{\Phi}\left(\boldsymbol{\theta}\right)\right]\boldsymbol{g}+\tilde{\varepsilon}. \tag{6}$$

To efficiently recover DOA and path gain with only a single RF chain and a small sampling length, all reconfigurable antennas set the same receiving patterns $\phi\left(\boldsymbol{\theta}\right)$. Accordingly, Eq. (6) can be simplified to the following form:

$$\tilde{\boldsymbol{h}}_{\mathrm{BA}}=\boldsymbol{A}\left(\boldsymbol{\theta}\right)\mathrm{diag}\left(\phi\left(\boldsymbol{\theta}\right)\right)\boldsymbol{g}+\tilde{\boldsymbol{\varepsilon}}. \tag{7}$$

Eq. (7) can be solved by the ANM theory. Unlike the traditional compressed sensing (CS) method that selects codewords on a finite codebook, ANM is based

on an infinite set to perform a search in the range of infinite precision, which can solve the basis mismatch problem (He et al., 2021). According to the signal to be recovered, the atomic set is defined as follows:

$$\mathcal{A}=\left\{\boldsymbol{a}\left(\theta_l\right)\in\mathbb{C}^{N\times 1}:\theta_l\in\left[-\frac{\pi}{2},\frac{\pi}{2}\right]\right\},\tag{8}$$

where the cardinality of $\mathcal{A}$ is infinite, i.e., $|\mathcal{A}|=+\infty$. The atomic norm of $\tilde{\boldsymbol{h}}_{\mathrm{BA}}$ with respect to $\mathcal{A}$ is

$$\begin{aligned}&\left\|\tilde{\boldsymbol{h}}_{\mathrm{BA}}\right\|_{\mathcal{A}}=\inf\left\{q:\tilde{\boldsymbol{h}}_{\mathrm{AB}}\in q\mathrm{conv}\left(\mathcal{A}\right)\right\}\\&=\inf\nolimits_{\left\{\theta_l\in\left[-\frac{\pi}{2},\frac{\pi}{2}\right],g_l\in\mathbb{C}\right\}}\left\{\sum_l\left|g_l'\right|:\tilde{\boldsymbol{h}}_{\mathrm{AB}}=\sum_l g_l'\boldsymbol{a}\left(\theta_l\right)\right\},\end{aligned}\tag{9}$$

where $\mathrm{conv}\left(\mathcal{A}\right)$ is the convex hull of $\mathcal{A}$ and $g_l'=\phi\left(\theta_l\right)g_l$. The atomic norm can be obtained by an equivalent semidefinite program (SDP) problem, as follows:

$$\min_{\nu,\boldsymbol{u}}\left(\tfrac{1}{2}\nu+\tfrac{1}{2}u_1\right)\ \text{s.t.}\ \begin{bmatrix}\nu & \tilde{\boldsymbol{h}}_{\mathrm{AB}}^{\mathrm{H}}\tilde{\boldsymbol{h}}_{\mathrm{AB}}\\ \tilde{\boldsymbol{h}}_{\mathrm{AB}} & \boldsymbol{T}\left(\boldsymbol{u}\right)\end{bmatrix}\geq 0,\tag{10}$$

where u_1 is the diagonal element of $\boldsymbol{T}\left(\boldsymbol{u}\right)$, and $\boldsymbol{T}\left(\boldsymbol{u}\right)$ denotes a Toeplitz matrix, which is expressed as follows:

$$\boldsymbol{T}\left(\boldsymbol{u}\right)=\begin{bmatrix}u_1 & u_2 & \cdots & u_N\\ u_2^* & u_1 & \cdots & u_{N-1}\\ \vdots & \vdots & & \vdots\\ u_N^* & u_{N-1}^* & \cdots & u_1\end{bmatrix}.\tag{11}$$

Convex problem (10) can be solved using convex optimization tools. Next, the angle information is recovered from $\boldsymbol{T}\left(\boldsymbol{u}\right)$ by Vandermonde decomposition:

$$\boldsymbol{T}\left(\boldsymbol{u}\right)=\sum_{l=1}^{L}\lambda_l\boldsymbol{a}\left(\theta_l\right)\boldsymbol{a}^{\mathrm{H}}\left(\theta_l\right)=\boldsymbol{A}\left(\boldsymbol{\theta}\right)\boldsymbol{\Sigma}\boldsymbol{A}^{\mathrm{H}}\left(\boldsymbol{\theta}\right).\tag{12}$$

Note that the decomposition in Eq. (12) is unique when $L<N$, which means that the number of reconfigurable antennas should be larger than the number of paths. Then, substitute the DOA estimate $\hat{\boldsymbol{\theta}}$ into Eq. (7) to calculate the path gain estimate $\hat{\boldsymbol{g}}$ via the LS algorithm.

4.2 Optimal matching of multipath signals

4.2.1 Problem formulation

The higher the channel estimation accuracy, the greater the correlation between the channel estimates of Alice and Bob. To boost the secret key capacity, in the multipath signal matching stage, each reconfigurable antenna can adjust the antenna pattern according to the estimated multipath channel parameters to mitigate the multipath fading effect. Consequently, optimal matching aims to maximize the receiving SNR to increase the correlation between legitimate uplink and downlink channels. The optimization problem can be formulated as follows:

$$\max_{\boldsymbol{\omega},\boldsymbol{\Phi}\left(\hat{\boldsymbol{\theta}}\right)}\frac{\left|\boldsymbol{\omega}^{\mathrm{T}}\left[\boldsymbol{A}\left(\hat{\boldsymbol{\theta}}\right)\odot\boldsymbol{\Phi}\left(\hat{\boldsymbol{\theta}}\right)\right]\hat{\boldsymbol{g}}\right|^2}{\sigma_n^2}\ \text{s.t.}\ \left|\omega_n\right|=1,\phi_n(\hat{\boldsymbol{\theta}})\in\mathcal{P},\tag{13}$$

where $\mathcal{P}$ denotes the set comprising all possible antenna patterns.

Specifically, we consider that the phase shift at each receiving RIS element can take only a finite number of discrete values. We assume that b is the phase resolution in bits per RIS phase-tunable unit element. Thus, the set of feasible discrete phases at each RIS element is $\mathcal{F}=\left\{0,\Delta\varphi,\cdots,\Delta\varphi\left(2^b-1\right)\right\}$, where $\Delta\varphi=2\pi/2^b$. The antenna pattern of each receiving RIS is given as follows:

$$\phi_n\left(\theta_l\right)=\sum_{m=1}^{M}\vartheta_n\left(m\right)\mathrm{e}^{\mathrm{j}\frac{2\pi(m-1)d_{\mathrm{B}}}{\lambda}\sin\theta_l},\tag{14}$$

where $\vartheta_n\left(m\right)=\mathrm{e}^{\mathrm{j}\varphi_n(m)}$ is the phase excitation of each RIS unit element and $\varphi_n\left(m\right)\in\mathcal{F}$ is the corresponding phase shift coefficient. By applying a control voltage to a diode, $\mathcal{P}$ contains a total of 2^{bM} antenna patterns, each determined by the configuration phase shift matrix $\boldsymbol{\Psi}\triangleq\left[\boldsymbol{\varphi}_1,\boldsymbol{\varphi}_2,\cdots,\boldsymbol{\varphi}_N\right]^{\mathrm{T}}$. Therefore, the optimization problem (13) is rewritten as follows:

$$\max_{\boldsymbol{\omega},\boldsymbol{\Psi}}\frac{\left|\boldsymbol{\omega}^{\mathrm{T}}\left[\boldsymbol{A}\left(\hat{\boldsymbol{\theta}}\right)\odot\boldsymbol{\Phi}\left(\hat{\boldsymbol{\theta}}\right)\right]\hat{\boldsymbol{g}}\right|^2}{\sigma_n^2}\ \text{s.t.}\ \left|\omega_n\right|=1,\varphi_n\left(m\right)\in\mathcal{F}.\tag{15}$$

4.2.2 Problem decomposition

Problem (15) is a non-convex problem and contains the product of the elements; we first transform it into the matrix multiplication form and then decompose it into two sub-problems. Specifically, $\left[\boldsymbol{A}\left(\hat{\boldsymbol{\theta}}\right)\odot\boldsymbol{\Phi}\left(\hat{\boldsymbol{\theta}}\right)\right]\hat{\boldsymbol{g}}$ in the objective function is rewritten as

$$\left[\boldsymbol{A}\left(\hat{\boldsymbol{\theta}}\right)\odot\boldsymbol{\Phi}\left(\hat{\boldsymbol{\theta}}\right)\right]\hat{\boldsymbol{g}}=\begin{bmatrix}\vartheta_1 & & \\ & \ddots & \\ & & \vartheta_N\end{bmatrix}\begin{bmatrix}\boldsymbol{C}_1(\hat{\boldsymbol{\theta}})\hat{\boldsymbol{g}}\\ \vdots\\ \boldsymbol{C}_N(\hat{\boldsymbol{\theta}})\hat{\boldsymbol{g}}\end{bmatrix},\tag{16}$$

where $\boldsymbol{\vartheta}_n \triangleq [\vartheta_n(1), \vartheta_n(2), \cdots, \vartheta_n(M)]$, $\boldsymbol{C}_n(\hat{\boldsymbol{\theta}}) \triangleq [\boldsymbol{c}_n(\theta_1), \boldsymbol{c}_n(\theta_2), \cdots, \boldsymbol{c}_n(\theta_L)]$, and $\boldsymbol{c}_n(\theta_l) = \mathrm{e}^{\mathrm{j}\frac{2\pi d_{\mathrm{A}}(n-1)}{\lambda}\sin\theta_l}\boldsymbol{b}(\theta_l)$. Here, $\boldsymbol{b}(\theta_l) = \left[1, \mathrm{e}^{\mathrm{j}\frac{2\pi d_{\mathrm{B}}}{\lambda}\sin\theta_l}, \cdots, \mathrm{e}^{\mathrm{j}\frac{2\pi(M-1)d_{\mathrm{B}}}{\lambda}\sin\theta_l}\right]^{\mathrm{T}}$ is the array response vector of RIS. Then, problem (15) is converted to the following form:

$$\max_{\boldsymbol{\omega},\boldsymbol{\Psi}} \frac{\left|[\omega_1,\cdots,\omega_N]\begin{bmatrix}\boldsymbol{\vartheta}_1 & & \\ & \ddots & \\ & & \boldsymbol{\vartheta}_N\end{bmatrix}\begin{bmatrix}\boldsymbol{C}_1(\hat{\boldsymbol{\theta}})\hat{\boldsymbol{g}} \\ \vdots \\ \boldsymbol{C}_N(\hat{\boldsymbol{\theta}})\hat{\boldsymbol{g}}\end{bmatrix}\right|^2}{\sigma_n^2}$$
$$\text{s.t. } |\omega_n| = 1,\ \varphi_n(m) \in \mathcal{F}. \tag{17}$$

Since the optimization variables $\boldsymbol{\omega}$ and $\boldsymbol{\Psi}$ are uncoupled with each other, we decompose the problem into two sub-problems and optimize them to obtain the optimal solution. Since the phase shifter adjusts only the phase, according to the Cauchy–Schwarz inequality, when the received signals of each reconfigurable antenna are superimposed in the same phase on the RF chain, the received power is the maximum (Tse and Viswanath, 2005). Accordingly, the optimal phase shift of the phase shifter is represented as follows:

$$\boldsymbol{\omega}_{\mathrm{opt}} = \left[\mathrm{e}^{-\mathrm{j}\angle\left(\boldsymbol{\vartheta}_1\boldsymbol{C}_1(\hat{\boldsymbol{\theta}})\hat{\boldsymbol{g}}\right)}, \mathrm{e}^{-\mathrm{j}\angle\left(\boldsymbol{\vartheta}_2\boldsymbol{C}_2(\hat{\boldsymbol{\theta}})\hat{\boldsymbol{g}}\right)}, \cdots, \mathrm{e}^{-\mathrm{j}\angle\left(\boldsymbol{\vartheta}_N\boldsymbol{C}_N(\hat{\boldsymbol{\theta}})\hat{\boldsymbol{g}}\right)}\right]. \tag{18}$$

Then, solving sub-problem $\boldsymbol{\Psi}$ is equivalent to maximizing this term for $n \in \{1, 2, \cdots, N\}$:

$$\max_{\boldsymbol{\vartheta}_n} \left|\boldsymbol{\vartheta}_n\boldsymbol{C}_n(\hat{\boldsymbol{\theta}})\hat{\boldsymbol{g}}\right| \quad \text{s.t.} \quad \varphi_n(m) \in \mathcal{F}. \tag{19}$$

4.2.3 Improved BPSO algorithm

Since each reconfigurable antenna is controlled independently, optimization of the RIS configuration code can be conducted in parallel to improve efficiency. To address the discrete non-convex constraint effectively, in the following text, we propose an improved BPSO algorithm to optimize $\boldsymbol{\Psi}$.

In the classical BPSO algorithm, the particle position is regarded as the solution to the problem to be solved (Khanesar et al., 2007). Every particle is represented as an M-dimensional vector, and every element of the vector is described by the digit "0" or "1," corresponding to the element of the RIS coding matrix (Zhang L et al., 2018). Considering that each metamaterial element in the proposed scheme contains b-bit discrete phases, we set each particle as an $(M \cdot b)$-dimensional vector, where each b particles represent a phase value. The moving velocity of the particle indicates the probability of position change and is given by the following expression:

$$\begin{aligned}\boldsymbol{v}_i^{k+1} =& w\boldsymbol{v}_i^k + c_1 \cdot \mathrm{rand}_1^k \cdot \left(\mathbf{pBest}_i^k - \boldsymbol{x}_i^k\right) \\ &+ c_2 \cdot \mathrm{rand}_2^k \cdot \left(\mathbf{gBest}_i^k - \boldsymbol{x}_i^k\right),\end{aligned} \tag{20}$$

where rand_1^k and rand_2^k are random numbers between 0 and 1, c_1 and c_2 are the acceleration constants, w is the inertia weight, $\mathbf{pBest}_i^k$ is the individual optimal position, and $\mathbf{gBest}_i^k$ is the global optimal position. Consistent with the probabilistic interpretation, velocity $v_i(j)$ is constrained within the interval $[0, 1]$, by means of a sigmoid-function mapping:

$$\mathrm{Sigmoid}\left(v_i(j)\right) = \frac{1}{1+\mathrm{e}^{-v_i(j)}}. \tag{21}$$

Accordingly, the position $\boldsymbol{x}_i^{k+1}$ is updated via using the following expression:

$$x_i^{k+1}(j) = \begin{cases} 1, & \mathrm{rand} < \mathrm{Sigmoid}\left(v_i^{k+1}(j)\right), \\ 0, & \mathrm{rand} \geq \mathrm{Sigmoid}\left(v_i^{k+1}(j)\right), \end{cases} \tag{22}$$

where $v_i(j)$ and $x_i^{k+1}(j)$ are the j^{th} elements of $\boldsymbol{v}_i$ and $\boldsymbol{x}_i^{k+1}$, respectively.

To calculate the fitness function to evaluate the targets, we first convert the $(M \cdot b)$-dimensional binary vector into an M-dimensional phase vector via the following expression:

$$\bar{\boldsymbol{x}}_i^{k+1}(m) = \boldsymbol{x}_i^{k+1}(m : b \cdot m) \cdot \left[\pi/2^0, \pi/2, \cdots, \pi/2^{b-1}\right]^{\mathrm{T}}, \tag{23}$$

where $\boldsymbol{x}_i^{k+1}(m : b \cdot m)$ represents the m^{th} column to the $(m \cdot b)^{\mathrm{th}}$ column of the vector $\boldsymbol{x}_i^{k+1}$ for $m \in \{1, 2, \cdots, M\}$. Then, the fitness function is given as

$$\mathrm{fitness}\left(\bar{\boldsymbol{x}}_i^{k+1}\right) = \left|\mathrm{e}^{\mathrm{j}\bar{\boldsymbol{x}}_i^{k+1}}\boldsymbol{C}_n(\hat{\boldsymbol{\theta}})\hat{\boldsymbol{g}}\right|. \tag{24}$$

The flowchart of the improved BPSO algorithm is given in Fig. 4. The termination condition is that the difference in the values of the objectives for two successive iterations is smaller than a predefined threshold τ. Finally, through multiple iterations and evaluation of the fitness, the optimal patterns with the desired receiving performance can be conveniently and quickly obtained for b-bit coding elements.

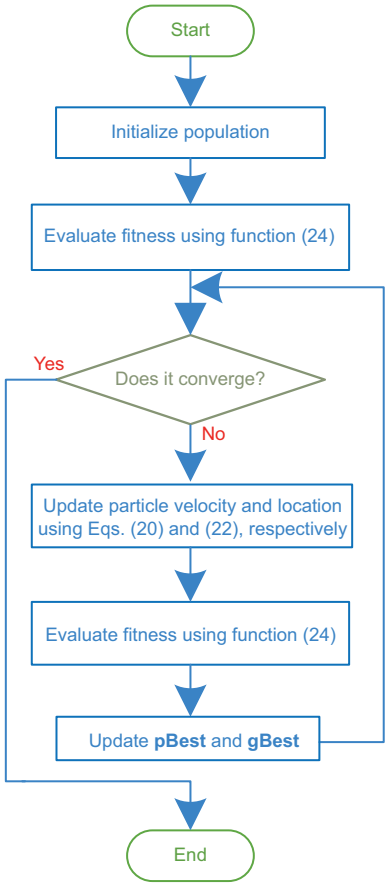

Fig. 4 Flowchart of the proposed improved binary particle swarm optimization algorithm

4.3 Secret key generation from the wireless channel

In the PKG stage, PRA uses the optimized antenna patterns to change the way of multipath superposition to overcome the effect of multipath fading. Specifically, Alice transmits and receives the pilot using the optimal shift $\boldsymbol{\omega}_{\text{opt}}$ and the configuration RIS phase shift coefficient $\boldsymbol{\Psi}_{\text{opt}}$. The received signals from Alice and Bob are given by the following expressions:

$$r_{\text{A}} = \boldsymbol{\omega}_{\text{opt}}^{\text{T}} \left[\boldsymbol{A}\left(\boldsymbol{\theta}\right) \odot \boldsymbol{\Phi}_{\text{opt}}\left(\boldsymbol{\theta}\right)\right] \boldsymbol{g} x_{\text{B}} + n_{\text{A}}, \tag{25}$$

$$r_{\text{B}} = \boldsymbol{\omega}_{\text{opt}}^{\text{T}} \left[\boldsymbol{A}\left(\boldsymbol{\theta}\right) \odot \boldsymbol{\Phi}_{\text{opt}}\left(\boldsymbol{\theta}\right)\right] \boldsymbol{g} x_{\text{B}} + n_{\text{B}}. \tag{26}$$

After the LS estimation, Alice and Bob obtain the channel estimates as

$$\hat{h}_{\text{A}} = \boldsymbol{\omega}_{\text{opt}}^{\text{T}} \left[\boldsymbol{A}\left(\boldsymbol{\theta}\right) \odot \boldsymbol{\Phi}_{\text{opt}}\left(\boldsymbol{\theta}\right)\right] \boldsymbol{g} + \frac{x_{\text{B}}^{\text{H}} n_{\text{A}}}{\left|x_{\text{B}}\right|^2}, \tag{27}$$

$$\hat{h}_{\text{B}} = \boldsymbol{\omega}_{\text{opt}}^{\text{T}} \left[\boldsymbol{A}\left(\boldsymbol{\theta}\right) \odot \boldsymbol{\Phi}_{\text{opt}}\left(\boldsymbol{\theta}\right)\right] \boldsymbol{g} + \frac{x_{\text{A}}^{\text{H}} n_{\text{B}}}{\left|x_{\text{A}}\right|^2}. \tag{28}$$

Consequently, Alice and Bob can acquire highly correlated channel estimates by combating multipath fading. After the following steps of the PKG, i.e., quantization, information reconciliation, and privacy amplification, the estimated channel values are finally converted into secret keys (Wan et al., 2021).

Remark 1 The eavesdropper Eve is located several wavelengths away from the legitimate user. Therefore, Eve experiences uncorrelated multipath fading from the legitimate channel. Although Eve can use the proposed scheme to improve the receiving SNR, as long as the eavesdropping channel is different from the legitimate channel, Eve cannot steal any information about the secret keys.

Remark 2 The computational complexity of the proposed scheme focuses mainly on DOA estimation and RIS code optimization. The computational complexity of SDP is about $\mathcal{O}\left((N+1)^{3.5}\right)$ (He et al., 2021). The computational complexity of the improved BPSO algorithm is about $\mathcal{O}\left(N\sqrt{Mb}\log\left(1/\tau\right)\right)$ (Khanesar et al., 2007). The proposed scheme exhibits superior KGR performance when compared to the conventional phased array while using fewer hardware resources. Although there is a slight increase in computational overhead, the benefits of this approach are clear.

Remark 3 Note that when radiating elements are in close proximity, mutual coupling effects may arise due to hardware non-idealities. Mutual coupling among the radiating elements results in lower antenna efficiency, which further increases the KDR and degrades secret key capacity. However, a significant amount of work has been done on reducing coupling, and numerous techniques have been proposed (Saenz et al., 2009). Moreover, metasurface and metamaterial-based antenna designs have demonstrated outstanding performance in eliminating the mutual coupling effects among antenna elements (Yang et al., 2012). On the other hand, mutual coupling among the radiating elements reduces the end-to-end received power (Qian and Di Renzo, 2021). Therefore, the proposed scheme can be considered the upper limit of secret key capacity performance in ideal conditions.

5 Simulation and numerical results

In this section, we evaluate the performance of the proposed scheme with the aid of numerical

simulations. Alice and Bob adopt the TDD mode at the frequency of 2.4 GHz. Alice is equipped with a single-channel PRA, and Bob is equipped with a single antenna. As illustrated in Fig. 5, PRA is uniformly arranged linearly with eight receiving RISs, and the spacing between adjacent RISs is $\lambda/2$. Each RIS consists of four metasurface radiating elements with spacing of $\lambda/8$. The unit radiating elements having 2-bit states can realize discrete configuration with 0°, 90°, 180°, and 270° phase shifts. The number of multipaths is set to 3 and the DOA is uniformly distributed in $[-60°, 60°]$. The complex gain of each multipath is independent of each other and follows the Gaussian distribution with $\mathcal{CN}(0, 1/L)$. The PRA controls the phase shifter to sample the received signals with eight different receiving patterns within a single symbol, and the DOA and path gain are constant during this short time. The SNR is defined as P_x/σ_n^2. Considering the complexity and accuracy of the proposed improved BPSO algorithm, the convergence threshold is set to $\tau = 0.01$. The simulation parameters are given in Table 1.

5.1 Performance of multipath channel parameter estimation

First, we provide the normalized mean square error (NMSE) as a performance metric of the estimated parameters, defined as follows:

$$\mathrm{NMSE}(\boldsymbol{\theta}) = \frac{E\left[|\boldsymbol{\theta} - \hat{\boldsymbol{\theta}}|^2\right]}{E\left[|\boldsymbol{\theta}|^2\right]}, \tag{29}$$

$$\mathrm{NMSE}(\boldsymbol{g}) = \frac{E\left[|\boldsymbol{g} - \hat{\boldsymbol{g}}|^2\right]}{E\left[|\boldsymbol{g}|^2\right]}. \tag{30}$$

Table 1 Simulation parameters

Parameter	Value
Carrier frequency	2.4 GHz
Number of PRA RF chains	1
Number of receiving RISs	8
Number of RIS elements	4
Number of multipaths	3
Spacing between adjacent RISs	$\lambda/2$
Spacing between adjacent elements	$\lambda/8$
Angular spread	$[-60°, 60°]$
Complex gain	$\mathcal{CN}(0, 1/L)$
Number of snapshots	8
Convergence threshold τ	0.01

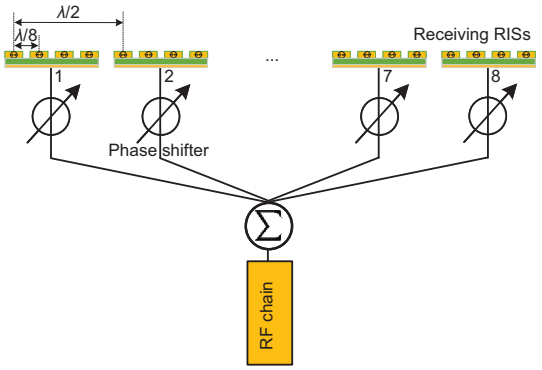

Fig. 5 Simulation parameter setting of the pattern-reconfigurable antenna architecture

We compare the DOA estimation performance with those of different estimation algorithms. As shown in Fig. 6, the proposed method outperforms the PRA architecture using the orthogonal matching pursuit (OMP) method (Lin et al., 2021). The OMP method is a grid-based method for sparse reconstruction, and the spatial domain is discretized into grids with grid size of 1° in the simulations. Thus, the grid mismatch leads to a performance penalty. However, the proposed scheme adopts the ANM estimation method without grids and thus has higher estimation accuracy. Moreover, we compare the weighted subspace fitting (WSF) algorithm based on the phased array with the same aperture. The proposed scheme has the same number of samples as the WSF algorithm but performs better. This observation means that over-sampling a single-channel PRA in the time domain can substitute spatial sampling of the conventional phased array.

Next, we show the DOA and path gain estimation performance with different numbers of receiving RISs in Fig. 7. We find that better estimation performance is achieved as the number of receiving RISs increases. Increasing the number of receiving RISs implies increasing the sampling number of electromagnetic waves in the spatial dimension, thus improving the ability of the PRA to resolve multipath angles. However, increasing the number of receiving RISs also means increasing the aperture of the PRA, so we need to choose a suitable number of receiving RISs to reconcile the performance and physical size.

5.2 Performance of optimal matching of multipath signals

Next, we present the correlation coefficient ρ and the KDR as the performance metrics of optimal

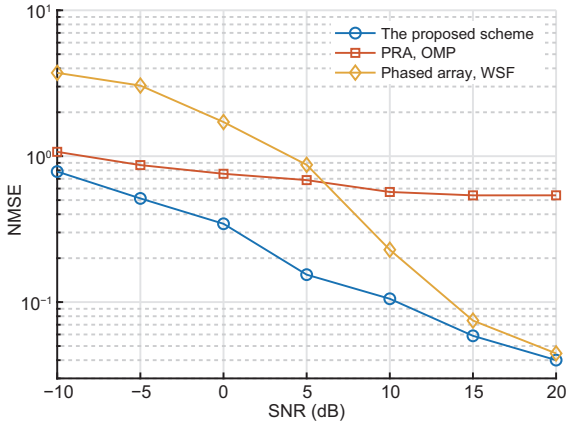

Fig. 6 DOA estimation performance with different algorithms versus the SNR

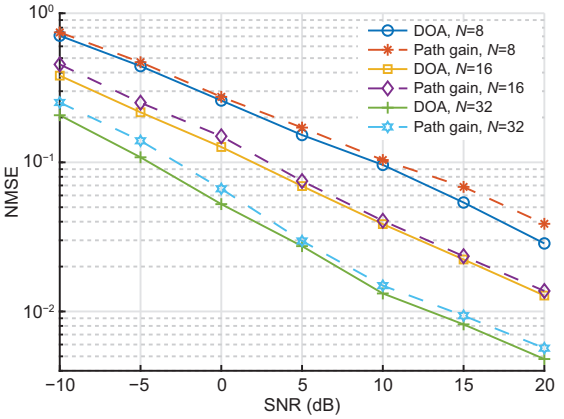

Fig. 7 DOA and path gain estimation performance with different numbers of receiving RISs

matching of multipath signals, defined as follows:

$$\rho = \frac{E\left[\left(\hat{h}_{\mathrm{A}} - \mu_{\hat{h}_{\mathrm{A}}}\right)\left(\hat{h}_{\mathrm{B}} - \mu_{\hat{h}_{\mathrm{B}}}\right)\right]}{\sigma_{\hat{h}_{\mathrm{A}}}\sigma_{\hat{h}_{\mathrm{B}}}}, \tag{31}$$

$$\mathrm{KDR} = \frac{\sum_{i=1}^{Q}\left|\mathrm{Key}_{\mathrm{A}}(i) - \mathrm{Key}_{\mathrm{B}}(i)\right|}{Q}, \tag{32}$$

where $\mu_{\hat{h}_{\mathrm{A}}}$, $\mu_{\hat{h}_{\mathrm{B}}}$ and $\sigma_{\hat{h}_{\mathrm{A}}}$, $\sigma_{\hat{h}_{\mathrm{B}}}$ represent the mean and standard deviation of channel estimates, respectively. The 1-bit quantization algorithm maps the analog channel measurements into binary values, and Q is the length of keys. Figs. 8 and 9 show the correlation coefficient and the KDR with different schemes, respectively. First, we find that the correlation coefficients of all schemes increase with the increasing SNR since the negative impacts of noises are reduced. For comparison, the benchmarks are random RIS codes that randomly shift the phase of the incoming signal and the phased array using coherent combining. It is noted that the proposed optimal design outperforms these benchmarks. For phased arrays, since each array element has the same structure and the fixed antenna pattern, multipath signals may be destructively superimposed at the array element, resulting in a loss of received power. In contrast, each RIS can optimize the pattern according to the estimated multipath parameters for matching reception to overcome multipath fading and improve the receiving SNR. Similarly, the proposed scheme can achieve a lower KDR, as shown in Fig. 9. Specifically, when the KDR is 0.1, the optimal setting achieves about 3 dB and 12 dB SNR gain compared to the PRA with random RIS code and the phased array, respectively.

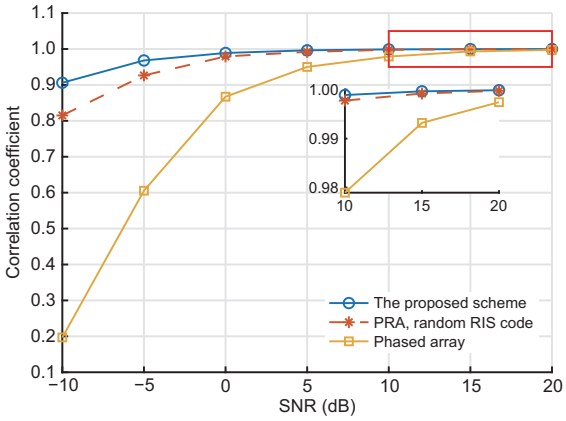

Fig. 8 Correlation coefficient with different schemes versus the SNR

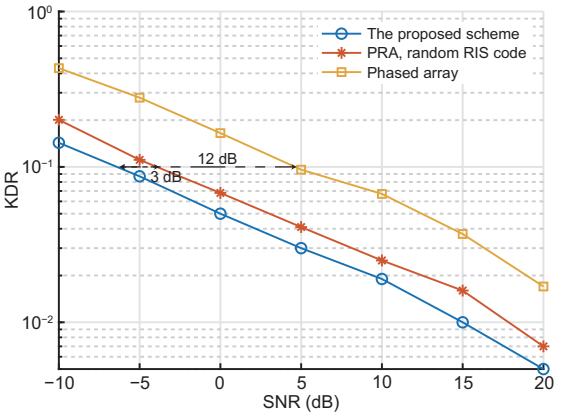

Fig. 9 KDR with different schemes versus the SNR

5.3 Secret key capacity

We present the secret key capacity as the performance metric of key generation, defined as follows:

$$C_{\mathrm{Key}} = I\left(\hat{h}_{\mathrm{A}}; \hat{h}_{\mathrm{B}} | \hat{h}_{\mathrm{E}}\right). \tag{33}$$

Fig. 10 shows the secret key capacity with

different schemes versus the SNR. It is observed that the proposed scheme can achieve a higher KGR than benchmark schemes. Specifically, when SNR=0 dB, the optimal setting achieves about 1.3 and 7.6 dB secret key capacity gain compared to the random RIS code and the phased array, respectively. This is because the antenna pattern of the PRA can be designed to mitigate the effects brought by multipath fading due to its flexibly configurable unit cell, thus enhancing the power of the received signal.

Fig. 11 shows the impact of the configurable degrees of freedom of the metamaterial unit on the secret key capacity. It can be observed that as the number of phase states of the metamaterial elements increases, the secret key capacity increases accordingly. This is expected because the higher the configurable degrees of freedom, the higher the degree of freedom in the antenna patterns. Therefore, the continuous phase shift can effectively increase the correlation between the legitimate uplink and downlink channels, thus increasing the secret key capacity. Moreover, we notice that compared with the 3-bit phase shift, the continuous phase shift has limited improvement in the key capacity, but the hardware complexity is significantly increased. Therefore, we recommend considering a 3-bit phase shift in the actual system implementation.

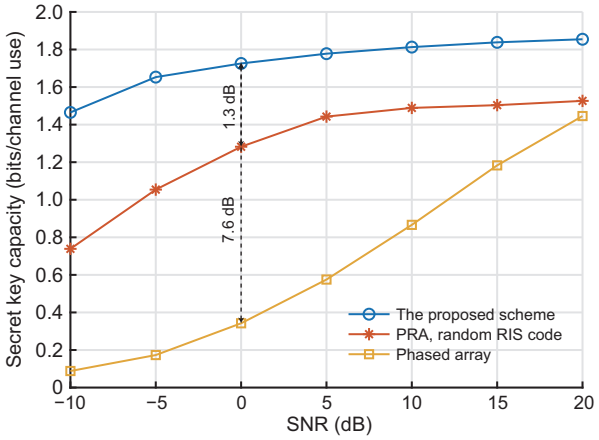

Fig. 10 Secret key capacity with different schemes versus the SNR

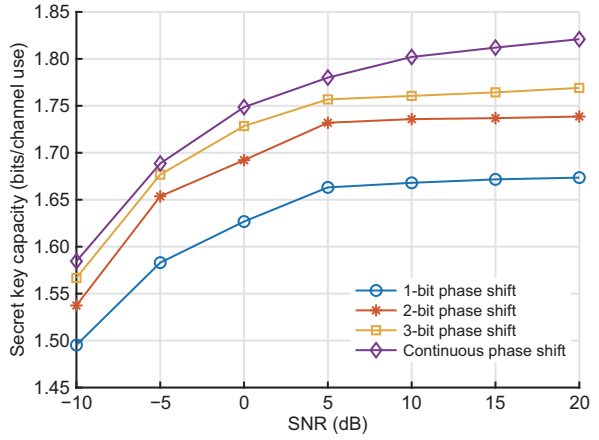

Fig. 11 Secret key capacity with different configurable degrees of freedom of the metamaterial unit

Fig. 12 shows the impact of the number of metamaterial elements on the secret key capacity. In the simulations, we keep the aperture of each receiving RIS at $\lambda/2$, and increasing the number of metamaterial elements means reducing the element spacing. We find that the secret key capacity increases with the increasing number of metamaterial elements. As more metamaterial elements are placed, the higher the degree of freedom of the antenna pattern for matching reception, the easier it is to eliminate or mitigate the multipath fading effect. However, it should be noted that the number of elements should not be too large. Otherwise, the mutual coupling among the radiating elements significantly reduces the end-to-end received power if the elements are spaced less than half of the wavelength apart, resulting in a corresponding decrease in the secret key capacity.

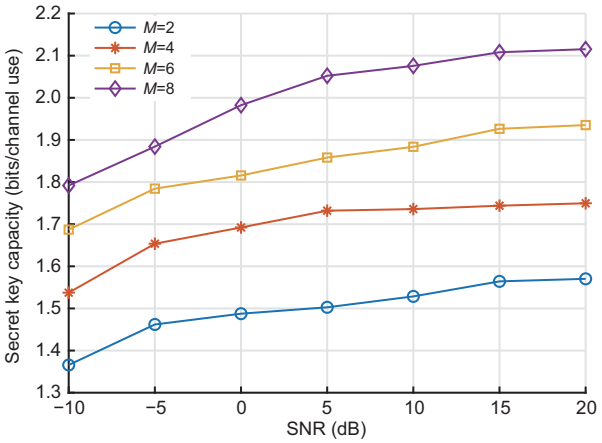

Fig. 12 Secret key capacity with different numbers of RIS metamaterial units

6 Conclusions

In this paper, we proposed a PRA-based PKG protocol to boost the secret key capacity. We first presented the RIS-based PRA architecture, in which each antenna had reconfigurable antenna patterns

to change the way of multipath superposition to reduce multipath fading. Then, we proposed the PRA-based PKG scheme, in which the flexibly reconfigurable antenna pattern of the PRA was designed to mitigate the multipath fading effects to improve the KGR. Simulation results showed that the proposed method can resist multipath fading and achieve a lower KDR. The secret key capacity of the proposed scheme was greatly improved compared with those of existing schemes.

Contributors

Zheng WAN and Mengyao YAN designed the research and initiated the work. Kaizhi HUANG drafted the paper. Zhou ZHONG and Xiaoming XU helped organize the paper. Zheng WAN, Yajun CHEN, and Fan WU revised and finalized the paper.

Compliance with ethics guidelines

Zheng WAN, Mengyao YAN, Kaizhi HUANG, Zhou ZHONG, Xiaoming XU, Yajun CHEN, and Fan WU declare that they have no conflict of interest.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Alexandropoulos GC, Vlachos E, 2020. A hardware architecture for reconfigurable intelligent surfaces with minimal active elements for explicit channel estimation. Proc IEEE Int Conf on Acoustics, Speech and Signal Processing, p.9175-9179. https://doi.org/10.1109/ICASSP40776.2020.9053976

Alexandropoulos GC, Vinieratou I, Wymeersch H, 2022. Localization via multiple reconfigurable intelligent surfaces equipped with single receive RF chains. *IEEE Wirel Commun Lett*, 11(5):1072-1076. https://doi.org/10.1109/LWC.2022.3156427

Cheng Q, Zhang L, Dai JY, et al., 2022. Reconfigurable intelligent surfaces: simplified-architecture transmitters—from theory to implementations. *Proc IEEE*, 110(9):1266-1289. https://doi.org/10.1109/JPROC.2022.3170498

Dai LL, Wang BC, Wang M, et al., 2020. Reconfigurable intelligent surface-based wireless communications: antenna design, prototyping, and experimental results. *IEEE Access*, 8:45913-45923. https://doi.org/10.1109/ACCESS.2020.2977772

He JG, Wymeersch H, Juntti M, 2021. Channel estimation for RIS-aided mmWave MIMO systems via atomic norm minimization. *IEEE Trans Wirel Commun*, 20(9):5786-5797. https://doi.org/10.1109/TWC.2021.3070064

Hu L, Li GY, Qian XW, et al., 2022. Joint transmit and reflective beamforming for RIS-assisted secret key generation. Proc IEEE Global Communications Conf, p.2352-2357.

Ji XS, Wu JX, Jin L, et al., 2022. Discussion on a new paradigm of endogenous security towards 6G networks. *Front Inform Technol Electron Eng*, 23(10):1421-1450. https://doi.org/10.1631/FITEE.2200060

Ji ZJ, Yeoh PL, Zhang DY, et al., 2021. Secret key generation for intelligent reflecting surface assisted wireless communication networks. *IEEE Trans Veh Technol*, 70(1):1030-1034. https://doi.org/10.1109/TVT.2020.3045728

Jian MN, Alexandropoulos GC, Basar E, et al., 2022. Reconfigurable intelligent surfaces for wireless communications: overview of hardware designs, channel models, and estimation techniques. *Intell Converg Netw*, 3(1):1-32. https://doi.org/10.23919/ICN.2022.0005

Jin L, Hu XY, Lou YM, et al., 2021. Introduction to wireless endogenous security and safety: problems, attributes, structures and functions. *China Commun*, 18(9):88-99. https://doi.org/10.23919/JCC.2021.09.008

Khanesar MA, Teshnehlab M, Shoorehdeli MA, 2007. A novel binary particle swarm optimization. Proc Mediterranean Conf on Control & Automation, p.1-6. https://doi.org/10.1109/MED.2007.4433821

Lin MT, Xu M, Wan X, et al., 2021. Single sensor to estimate DOA with programmable metasurface. *IEEE Int Things J*, 8(12):10187-10197. https://doi.org/10.1109/JIOT.2021.3051014

Lou YM, Jin L, Sun XL, et al., 2022. Multi-path separation and parameter estimation by single DMA in fading channel. *IET Commun*, 16(13):1475-1485. https://doi.org/10.1049/cmu2.12341

Lu Y, Hao M, Mackenzie R, 2022. Reconfigurable intelligent surface based hybrid precoding for THz communications. *Intell Converg Netw*, 3(1):103-118. https://doi.org/10.23919/ICN.2022.0003

Qian XW, Di Renzo M, 2021. Mutual coupling and unit cell aware optimization for reconfigurable intelligent surfaces. *IEEE Wirel Commun Lett*, 10(6):1183-1187. https://doi.org/10.1109/LWC.2021.3061449

Saenz E, Ederra I, Gonzalo R, et al., 2009. Coupling reduction between dipole antenna elements by using a planar meta-surface. *IEEE Trans Antenn Propag*, 57(2):383-394. https://doi.org/10.1109/TAP.2008.2011249

Shlezinger N, Alexandropoulos GC, Imani MF, et al., 2021. Dynamic metasurface antennas for 6G extreme massive MIMO communications. *IEEE Wirel Commun*, 28(2):106-113. https://doi.org/10.1109/MWC.001.2000267

Tse D, Viswanath P, 2005. Fundamentals of Wireless Communication. Cambridge University Press, Cambridge, UK.

Wan Z, Huang KZ, Lou YM, et al., 2021. Channel covariance matrix based secret key generation for low-power terminals in frequency division duplex systems. *Electron Lett*, 57(8):324-327. https://doi.org/10.1049/ell2.12123

Wu GB, Dai JY, Cheng Q, et al., 2022. Sideband-free space-time-coding metasurface antennas. *Nat Electron*, 5(11):808-819. https://doi.org/10.1038/s41928-022-00857-0

Wu W, Wu Z, Liang WL, 2019. Metasurface inspired pattern reconfigurable antenna. Proc IEEE MTT-S Int Wireless Symp, p.1-3. https://doi.org/10.1109/IEEE-IWS.2019.8804018

Yang XM, Liu XG, Zhou XY, et al., 2012. Reduction of mutual coupling between closely packed patch antennas using waveguided metamaterials. *IEEE Antenn Wirel Propag Lett*, 11:389-391. https://doi.org/10.1109/LAWP.2012.2193111

Zhang HL, Song LY, Han Z, et al., 2021. Spatial equalization before reception: reconfigurable intelligent surfaces for multi-path mitigation. Proc IEEE Int Conf on Acoustics, Speech and Signal Processing, p.8062-8066. https://doi.org/10.1109/ICASSP39728.2021.9414612

Zhang L, Chen XQ, Liu S, et al., 2018. Space-time-coding digital metasurfaces. *Nat Commun*, 9(1):4334. https://doi.org/10.1038/s41467-018-06802-0

Zhou RY, Chen XY, Tang WK, et al., 2022. Modeling and measurements for multi-path mitigation with reconfigurable intelligent surfaces. Proc 16th European Conf on Antennas and Propagation, p.1-5. https://doi.org/10.23919/EuCAP53622.2022.9769365