University of Baghdad
College of Engineering
JE
JOURNAL OF ENGINEERING

Journal of Engineering

journal homepage: www.jcoeng.edu.iq

Volume 31 Number 9 September 2025

Enhanced Physical Layer Secret Key Generation via Beyond-Diagonal Reconfigurable Intelligent Surfaces in Multi-User MIMO Systems

Mina Fadhil Hasan *, Aqiel Niama Almamori

Department of Electronics and Communications Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq

ABSTRACT

Physical Layer Key Generation (PLKG) provides a promising approach for establishing secure cryptographic keys between legitimate parties. However, in static and quasi-static environments, the key generation rate is significantly limited due to the low entropy of the wireless channel. To overcome this, Reconfigurable Intelligent Surfaces (RIS) have been proposed to enhance the channel entropy by altering the phase of incident electromagnetic waves. This paper addresses this challenge by proposing a security architecture that integrates a Multi-Input Multi-Output (MIMO) base station with a Beyond-Diagonal Reconfigurable Intelligent Surface (BD-RIS) in multi-user scenarios, in the presence of an eavesdropper. Unlike conventional RIS, BD-RIS not only modifies the phase but also the magnitude of the impinging signals, introducing an additional degree of freedom that further enhances channel randomness. The secret key capacity of the proposed system is compared with that of conventional RIS in two scenarios: firstly, when a direct link exists alongside the BD-RIS-assisted link. Secondly, when the direct link is completely obstructed by an obstacle. Simulation results demonstrate that the proposed BD-RIS architecture outperforms conventional diagonal RIS (D-RIS) in all scenarios. Furthermore, the generated keys undergo randomness tests, successfully passing all National Institute of Standards and Technology (NIST) randomness subtests as well as the Autocorrelation (AC) test, confirming their suitability for secure communications. These findings establish BD-RIS as a promising technology for enhancing physical layer security in static environments for 5G/6G networks and IoT applications.

Keywords: Autocorrelation test (AC), BD-RIS, NIST, RIS, Secret key generation.

1. INTRODUCTION

Reconfigurable Intelligent Surfaces (RIS) are a two-dimensional array composed of large number of low-cost, programmable elements. Each element consists of a passive antenna integrated with a tunable impedance component, commonly implemented using electronically controllable devices such as varactor diodes or RF switches, and is managed

*Corresponding author
Peer review under the responsibility of University of Baghdad.
https://doi.org/10.31026/j.eng.2025.09.09
This is an open access article under the CC BY 4 license (http://creativecommons.org/licenses/by/4.0/).
Article received: 30/03/2025
Article revised: 10/06/2025
Article accepted: 03/07/2025
Article published: 01/09/2025

by an external control circuit, often realized through a field-programmable gate array (FPGA). The programmable nature of RIS arises from the ability to dynamically alter the state of these components, thereby adjusting the impedance value in real time, which in turn modifies the scattering matrix. This configuration allows each element to independently control the phase shift of incident electromagnetic waves since the impedance networks are not interconnected and therefore adds control to the wireless environment **(Ji et al., 2021; Yang et al., 2023; Gao et al., 2024b)**. Building on the foundation of this conventional diagonal RIS, a more generalized form, Beyond Diagonal-RIS (BD-RIS), has emerged to further enhance reconfigurability and security in wireless communications. In BD-RIS, the impedance network is interconnected, unlike RIS, which enables joint control over both the phase and magnitude of the reflected signals because of its ability to redistribute the power among the elements, which significantly expanding the degrees of freedom for optimizing the wireless channel **(Fang and Mao, 2024; Nerini et al., 2024; Santamaria et al., 2024)**. As wireless networks become more congested, e.g., the Internet of Things (IoT) **(Shlezinger et al., 2021)**, with the transition toward 6G networks, security becomes a significant concern due to the inherent broadcast nature of the wireless communication **(Mohammed, 2020)**. Traditionally, symmetric encryption schemes such as Advanced Encryption Standard (AES) and public key cryptography have played a crucial role in providing data integrity, confidentiality, and authentication. However, these methods rely on key sequences to function properly, and these keys can be predicted or become vulnerable under certain conditions **(Gao et al., 2024a; Shahiri et al., 2024)**. In response to these challenges, physical layer key generation (PLKG) provides lightweight; low latency Cryptographic security for wireless communication systems, where legitimate parties generate their encryption keys from the shared properties of the reciprocal wireless channel between them, providing information-theoretic security to wireless systems **(Zhang et al., 2016; Liu et al., 2017; Zhang et al., 2019)**.

However, in quasi-static and static environments such as indoor environment where limited randomness arise, PLKG provides insufficient secret key generation rate **(Hu et al., 2021)**. Exploiting the aforementioned features of RIS, along with its ease of deployment and passive nature, has made it a key focus in the literature **(Al-Nahhas et al., 2021; Hamza et al., 2024; Singh et al., 2024; Samy et al., 2025)**. **(Gao et al., 2024a)** investigates RIS-aided PLKG, covering channel modeling, application scenarios, and key design challenges. It also examines RIS jamming attacks, defense strategies, and future research directions. An innovative ICAS design is proposed by **(Gao et al., 2024b)**, in which RIS hardware is shared for both data transmission and secret key generation to achieve "one-time pad" communication. They model the problem as a Stackelberg game and use a DRQN-based dynamic strategy to optimize the RIS phase shift, with simulations showing improved performance compared to benchmarks. In the work of **(Hu et al., 2021)**, the SKG process is designed for two different scenarios, with derivations for both the exact and asymptotic secret key rates. Their simulation results confirm that the proposed scheme outperforms existing methods based on artificial random signals, emphasizing that the optimal switching time should be adjusted according to pilot power .

Additionally, the authors in **(Shahiri et al., 2024)** introduce a novel contribution that takes into account the spatial correlation between RIS elements when randomly changing their phases to induce randomness in static environments, investigate two phase-shift scenarios, propose a new framework for handling temporal correlations in channel samples and present an optimization approach to maximize SKG rate. An IRS-assisted physical layer key generation (CRKG) method that achieves adjustable key generation rates while ensuring

random key material is discussed in **(Staat et al., 2021)**. The authors introduce a channel oversampling technique to reduce bit mismatch and demonstrate the feasibility of IRS-assisted CRKG through a proof-of-concept system using low-cost IRS prototypes and MIMO radio transceivers. The work by **(Yang et al., 2023)** models IRS-assisted secret key generation in mmWave scenarios, deriving key channel properties under a uniform rectangular array (URA) configuration and analyzing the impact of quantization on reflection channel randomness. The research conducted in **(Ji et al., 2021)** demonstrates that employing SDR and SCA techniques can efficiently resolve the non-convexity challenges in IRS optimization, leading to improved secret key capacity in wireless networks.

However, diagonal RIS (D-RIS) is limited to phase-only control due to its architecture, where each element operates independently and is not electrically interconnected with others. This limitation arises from the diagonal nature of the scattering matrix. As a result, the system's ability to introduce sufficient channel variability is reduced, which in turn limits the randomness required for secure key generation, especially in static and quasi-static environments. In contrast, beyond-diagonal RIS (BD-RIS) with its interconnected architecture, enables the formation of a full (non-diagonal) scattering matrix. This structure allows for joint influence on the amplitude and phase of the reflected signals, significantly increasing the degrees of freedom in channel manipulation. The added flexibility enhances channel randomness needed in physical-layer key generation.

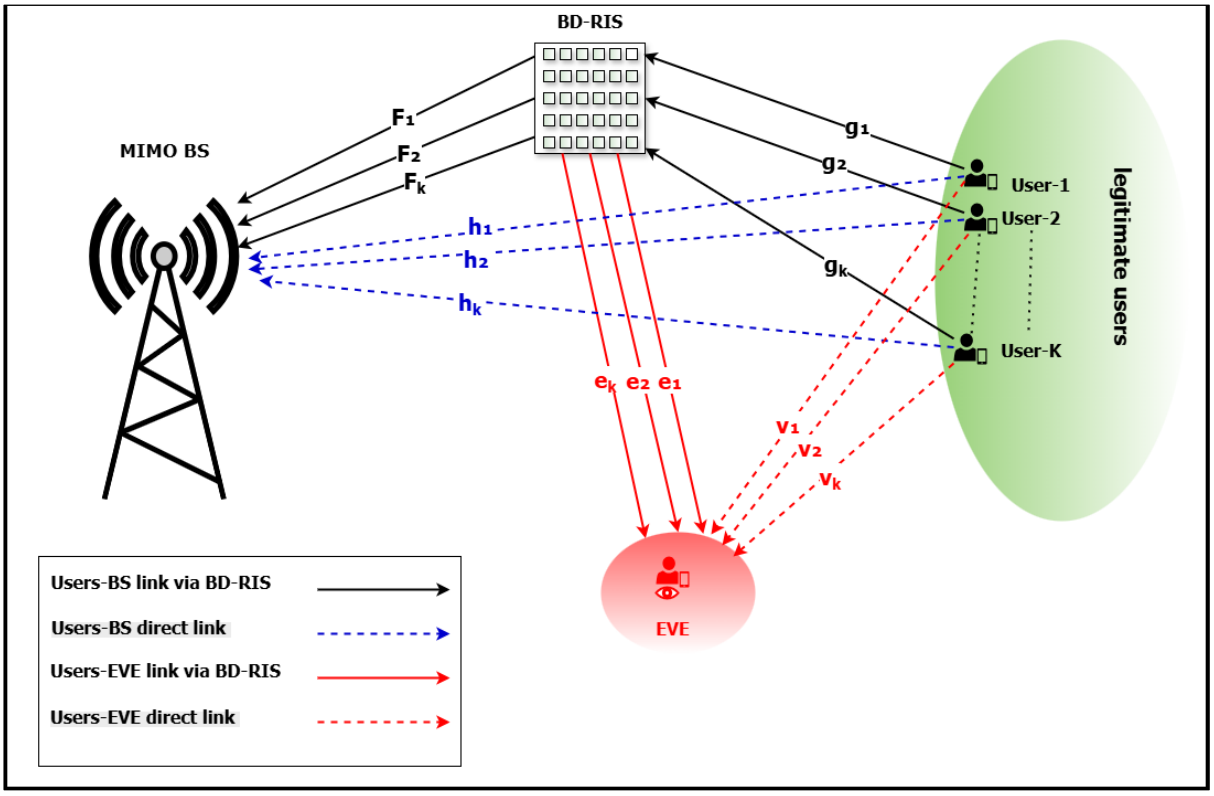
In this paper, we integrate (BD-RIS) with multi-user MIMO system and utilize this novel architecture to generate physical layer secret keys based on channel observation. The key generation process follows the steps: Channel probing, Quantization, Information reconciliation, and Privacy amplification, preceded by random initialization of the BD-RIS scattering matrix, which serves as the only source of randomness in the static environment. The secret key capacity is evaluated through simulations and compared with the diagonal-RIS (D-RIS) and the No-RIS in two scenarios: when the direct link is fully blocked by an obstacle, so the only path from the BS to the users is that via the BD-RIS, and when the direct link is present. Simulation results demonstrate a consistent enhancement in key capacity compared to both the D-RIS and No-RIS cases across all scenarios. Additionally, randomness tests are conducted to validate the quality of the generated keys. The results confirm that the generated keys successfully pass both the NIST randomness subtests and the autocorrelation test, affirming their statistical robustness.

2. SYSTEM MODEL

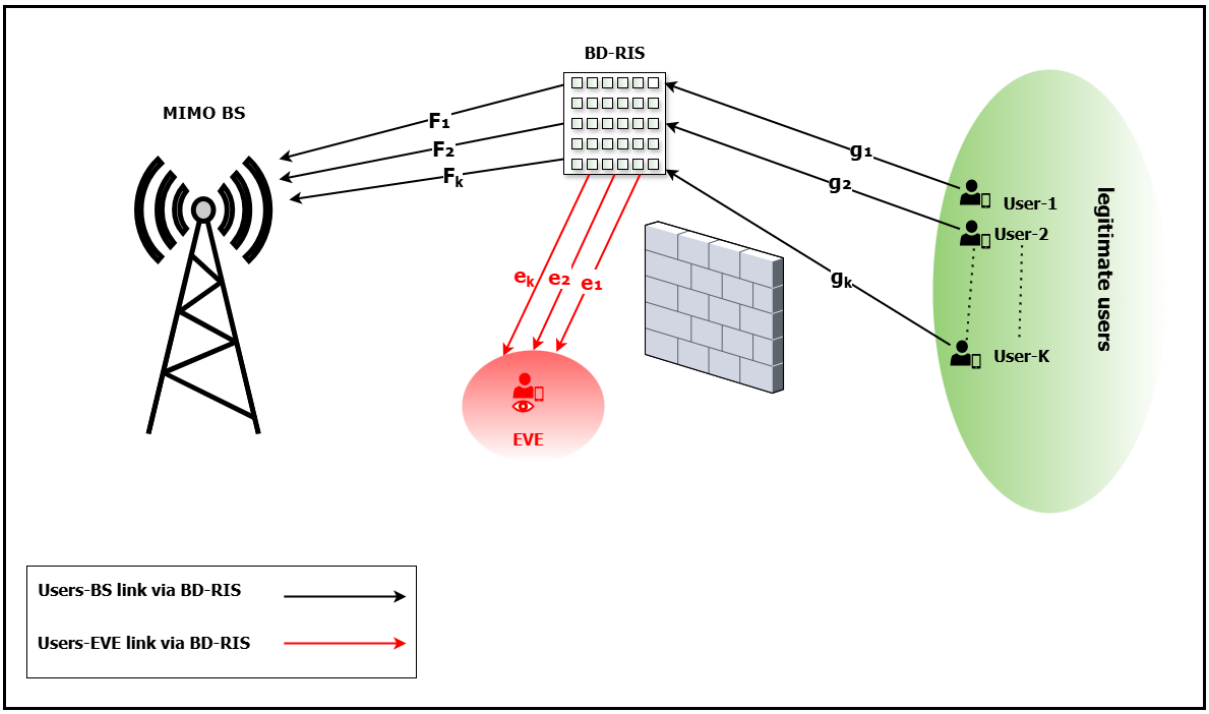
Consider the system illustrated in **Fig. 1**, which consists of a multiple-input multiple-output (MIMO) base station (BS) equipped with M active antennas. The BS aims to generate a physical-layer key (PLK) from the channel state information (CSI) of the channels between itself and K legitimate users under two scenarios: (a) when the direct link is fully blocked, and communication relies solely on the Beyond Diagonal Reconfigurable Intelligent Surface (BD-RIS); (b) when the direct channel is available, with additional assistance from the BD-RIS. The BD-RIS is composed of N passive antennas, which play a crucial role in enhancing channel randomness and assisting in secure key generation. It is assumed that the distance among antenna elements exceed half a wavelength to ensure that the mutual coupling between them is negligible **(Mishra et al., 2024)**.

The system also includes a passive eavesdropper attempting to intercept the generated keys. Following the widely adopted assumption in physical-layer key generation **(Hu et al., 2021; Shahiri et al., 2024; Ji et al., 2021; Gao et al., 2024b)**, both the legitimate users and the

eavesdropper are modeled as single-antenna nodes. This reflects the fact that PLKG focuses on the decorrelation of channel observations between legitimate users and EVE, rather than the decoding capability.



(a) The direct link is present.



(b) The direct channel is fully blocked

Figure 1. The proposed system model.

Also, assume that the entire system operates in time-division duplexing (TDD) mode. The environment is considered to be quasi-static, meaning that the primary source of randomness in the system originates from the BD-RIS phase shift matrix. Additionally, the eavesdropper is assumed to be positioned at least half a wavelength away from the legitimate users and possesses knowledge of the physical-layer key generation (PLKG) algorithm being employed **(Patwari et al., 2010; Staat et al., 2021)**.

3. SECRET KEY GENERATION SCHEME

The process of generating the physical-layer secret key follows well-established steps, as outlined in **(Gao et al., 2024a)**:
Initializing BD-RIS scattering matrix with complex entries whose magnitude and phase are independently and uniformly distributed. Each element can be represented as follows: $S_{ij} = a_{ij}\, e^{j\theta_{ij}}$, where $a_{ij} \sim \mathcal{U}(0,1)$ denotes the amplitude, and $\theta_{ij} \sim \mathcal{U}[0,2\pi)$ is the phase. This is followed by Channel probing, Quantization, Information reconciliation, and Privacy amplification, as illustrated in **Fig. 2**.

3.1 Random Phase Shift Generation

In a time-division duplexing (TDD) system, each coherence time frame τ is segmented into three distinct phases: the uplink (UL) training phase $\tau_{\text{up\_training}}$, the uplink (UL) data transmission phase $\tau_{\text{up-data}}$ and downlink (DL) data transmission phase $\tau_{\text{down-data}}$ **(Mishra et al., 2024).** Where the time frame τ should satisfy the condition below:

$$\tau \geq \tau_{up-training} + \tau_{up-data} + \tau_{down-data} \quad (1)$$

As depicted in **Fig. 3 (Demir and Björnson, 2022)**, the entire secret key generation process occurs exclusively during the training phase, starting with the random initialization of the BD-RIS scattering matrix. This initialization generates a random full scattering matrix, in contrast to the RIS, which produces only a diagonal matrix, thereby offering superior performance **(Shen et al., 2022)**. The full scattering matrix introduces greater randomness to the channel, which is crucial for overcoming the limitations imposed by the static environment.

3.2 Channel Probing

During the channel probing phase, the short-term channel reciprocity inherent in time-division duplex (TDD) systems is leveraged to estimate key channel parameters, such as received signal strength (RSS) and channel state information (CSI). Since RSS provides only amplitude information, CSI is used in our key generation scheme to achieve a higher key generation rate **(Wang et al., 2011; Zhang et al., 2016)**, offering a more detailed representation of the channel and enabling improved performance.

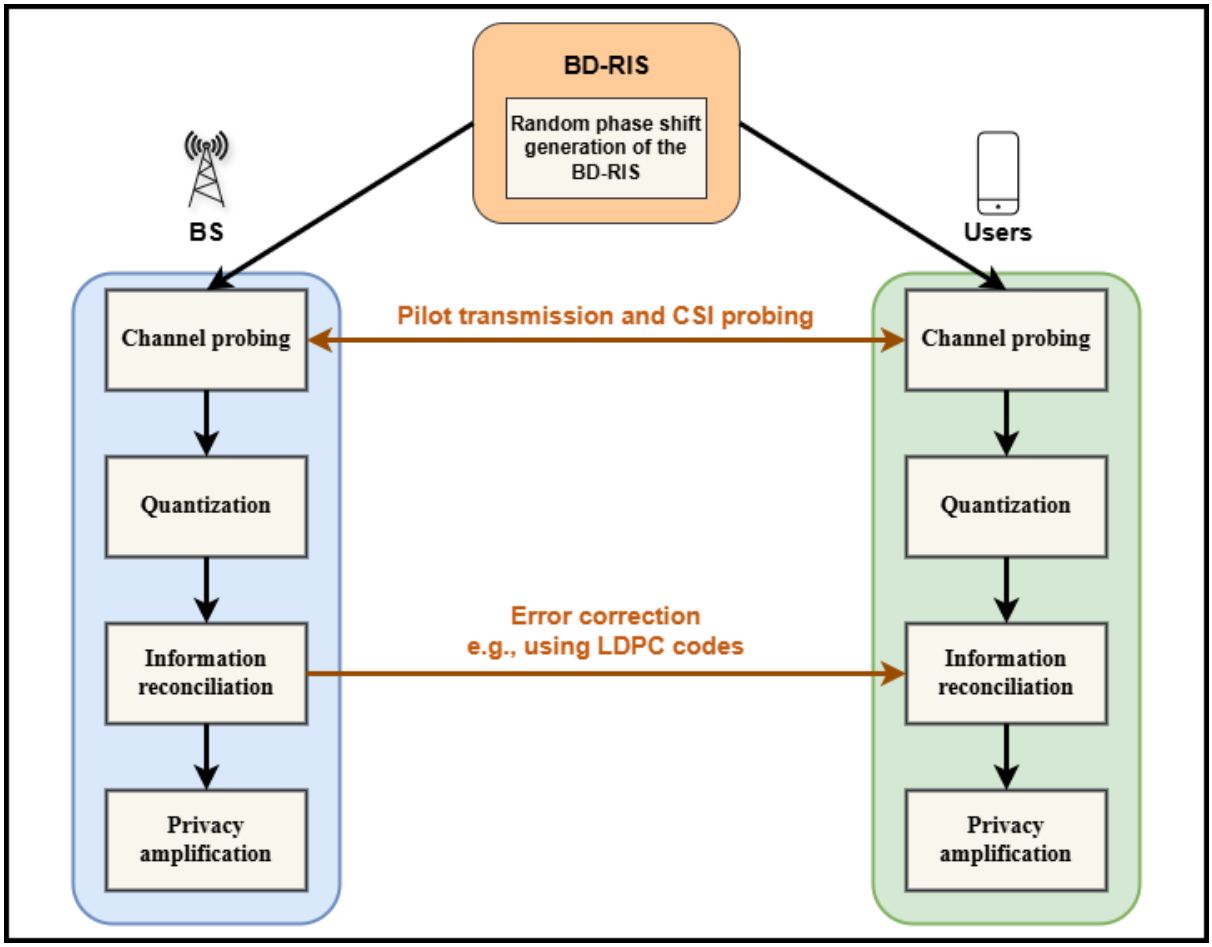


Figure 2. Key generation steps.

Figure 3. Coherence block structure with training, uplink, and downlink phases.

After initializing the BD-RIS phases, the K legitimate users transmit pilot signals to the base station (BS). Let the pilot sequence length is τ_{pilot}, where $\tau_{pilot} < \tau_{up\text{-}training}$ and assume the pilot sequence of the j[th] user is represented as $\mathbf{x_j} \in \mathbb{R}^{\tau_{pilot} \times 1}$, and assume orthogonality among pilots **(Akbarpour-Kasgari and Ardebilipour, 2018)**:

$$\boldsymbol{X}^{\boldsymbol{T}} * \boldsymbol{X} = \boldsymbol{I_K} \quad (2)$$

Where $\mathbf{X} = [\mathbf{x_1}, \mathbf{x_2}, \ldots\ldots, \mathbf{x_k}] \in \mathbb{R}^{\tau_{pilot} \times K}$ is the pilot matrix.

Accordingly, the base station (BS) and the passive eavesdropper (EVE) receive the following signals, respectively:

$$\boldsymbol{Y_{BS}} = \sum_{j=1}^{k} \sqrt{P}\left(\boldsymbol{h_j} + \boldsymbol{F}\,\boldsymbol{\Phi}\;\boldsymbol{g_j}\right)\boldsymbol{x_j'} + \boldsymbol{N_{BS}} \quad (3)$$

And,

$$\boldsymbol{y_{EVE}} = \sum_{j=1}^{k} \sqrt{P}\left(v_j + \boldsymbol{e'}\,\boldsymbol{\Phi}\;\boldsymbol{g_j}\right)\boldsymbol{x_j}' + \boldsymbol{n_{EVE}} \quad (4)$$

At the Base Station (BS):

The received signal during the uplink pilot phase is denoted by $\boldsymbol{Y_{BS}} \in \mathbb{C}^{M\,x\,\tau_{pilot}}$, Each legitimate user $j \in \{1, 2, \ldots, K\}$ transmits an orthogonal pilot sequence $\mathbf{x_j} \in \mathbb{R}^{\tau_{pilot}\,x\,1}$ with normalized energy. The total received signal is a superposition of the direct channels $\mathbf{h_j} \in \mathbb{C}^{M\,x\,1}$,representing the channel between the BS and the jth user, and the reflected components through the BD-RIS. The channel matrix between the BS and the BD-RIS is $\mathbf{F} \in \mathbb{C}^{M\,x\,N}$, and the channel vector from the BD-RIS to the jth user is $\mathbf{g_j} \in \mathbb{C}^{N\,x\,1}$. The BD-RIS scattering behavior is captured by the scattering matrix $\boldsymbol{\Phi} \in \mathbb{C}^{N\,x\,N}$. P denotes the uplink transmit power of each user, and the additive white Gaussian noise at the BS is $\boldsymbol{N_{BS}} \in \mathbb{C}^{M\,x\,\tau_{pilot}}$, modeled as circularly symmetric complex Gaussian noise $\boldsymbol{\mathcal{CN}}\,(0, \sigma^2\mathbf{I})$.

At the passive eavesdropper (EVE):

The received pilot signal is represented by $\boldsymbol{y_{EVE}} \in \mathbb{C}^{1\,x\,\tau_{pilot}}$ includes the direct channel components $v_j \in \mathbb{C}^{1\,x\,1}$between the eavesdropper and the jth user, and the reflected components from the BD-RIS, where $\mathbf{e} \in \mathbb{C}^{Nx1}$ models the channel from the BD-RIS to the eavesdropper. The noise at the eavesdropper is denoted by $\boldsymbol{n_{EVE}} \in \mathbb{C}^{1\,x\,\tau_{pilot}}$, also modeled as circularly symmetric complex Gaussian noise $\boldsymbol{\mathcal{CN}}\,(0, \sigma^2\mathbf{I})$.

The BD-RIS scattering matrix $\boldsymbol{\Phi} \in \mathbb{C}^{N\,x\,N}$ is fully connected **(Li et al., 2024)**, implying non-diagonal structure as can be seen in Eq. (5) unlike RIS which is single connected and hence its scattering matrix is diagonal as seen in Eq. (6). Both RIS and BD-RIS structures are illustrated in **Fig. 4.**

$$\boldsymbol{\Phi}_{BD-RIS} = \begin{bmatrix} S_{1,1} & S_{1,2} \\ S_{2,1} & S_{2,2} \end{bmatrix} \quad (5)$$

$$\boldsymbol{\Phi}_{RIS} = \begin{bmatrix} S_{1,1} & 0 \\ 0 & S_{2,2} \end{bmatrix} \quad (6)$$

For all channels, the propagation model consists of both large-scale and small-scale fading effects. The large-scale fading follows a distance-dependent path loss model given by:

$$L\,(d_z) = d_z^{-\alpha} \quad (7)$$

where d_z represents the distance between the transmitter and receiver, and α is the path loss exponent. The small-scale fading component follows a Nakagami-m distribution, with the probability density function (PDF) expressed as **(Gómez-Déniz and Gómez-Déniz, 2024)**:

$$q(y; m) = \frac{m^m\, y^{m-1}}{\Gamma(m)}\, e^{-my}, \forall y > 0 \quad (8)$$

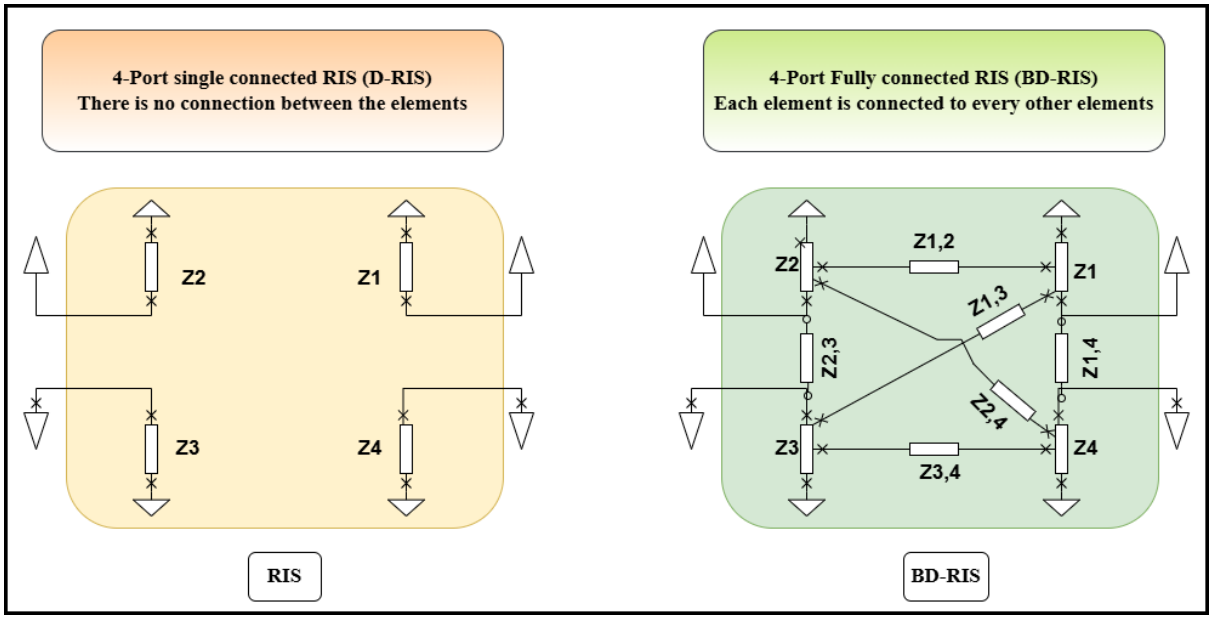


Figure 4. RIS versus BDRIS architecture **(Shen et al., 2022)**

Where m is the Nakagami fading parameter. The gamma function Γ(m) is defined as **(Hamza et al., 2024)**:

$$\Gamma\ (m) = \int_0^\infty z^{m-1} e^{-z} dz \tag{9}$$

Then, the required channel state information (CSI) is estimated using the least squares (LS) estimator by leveraging the received signals (Eq. (3) and Eq. (4)) along with the transmitted pilot matrix $\boldsymbol{X}$ (Eq. (2)). Specifically, the combined uplink channels between the base station (BS) and the users, and between the eavesdropper (EVE) and the users, are estimated as follows:

$$\widehat{\boldsymbol{H}}_{\boldsymbol{combined-BS}} = \boldsymbol{Y_{BS}} * \boldsymbol{X} \tag{10}$$

$$\widehat{\boldsymbol{h}}_{\boldsymbol{combined-EVE}} = \boldsymbol{y_{EVE}} * \boldsymbol{X} \tag{11}$$

The resulting $\widehat{\boldsymbol{H}}_{\boldsymbol{combined-BS}} \in \mathbb{C}^{M\ x\ K}$ and $\widehat{\boldsymbol{h}}_{\boldsymbol{combined-EVE}} \in \mathbb{C}^{1\ x\ K}$ provide the BS and EVE with the estimated cascaded channels from all users.

3.3 Quantization

The classification of quantization methods can be determined by various criteria. For instance, quantizers can be categorized based on their processing approach, such as absolute-value-based and differential-value-based quantizers. Another classification is based on bit representation, e.g., single-bit and multi-bit quantizers **(Zhang et al., 2016)**. In this study, we adopt a quantization method based on the cumulative distribution function (CDF), primarily due to its simplicity and ability to produce an equiprobable output **(Staat et al., 2021; Gao et al., 2024a; Patwari et al., 2010)**.

In this phase, to simplify the explanation, we assume that the same quantization process is performed independently at both the base station (BS) and the passive eavesdropper (EVE), using their respective channel observations. However, for ease of presentation and without

loss of generality, the following description focuses on the procedure carried out at the BS. After obtaining the estimated channel state information (CSI) between the BS and each legitimate user via the least squares (LS) estimator, as defined in Equation (10). Let $\widehat{\boldsymbol{h}}_{\boldsymbol{BS-j}} \in \mathbb{C}^{M\ x\ 1}$ denote the estimated CSI vector between the BS and the jth user. The ith element of this vector, $\hat{h}_{BS-j}{}^{(i)}$, corresponds to the channel coefficient observed at the ith antenna. Each antenna's observation is processed by computing the magnitude:

$$y_j(i) = \left|\hat{h}_{BS-j}{}^{(i)}\right| \tag{12}$$

The real-valued features $y_j(i)$ are then quantized using a Multi-bit Adaptive Quantization (MAQ) scheme into Q=4. 2^b quantization levels, with b=1 in this model. The empirical cumulative distribution function (CDF) is represented as:

$$F_i(y) = p[y_j(i) \leq y] \tag{13}$$

Then, the thresholds for these levels are computed using the inverse of this CDF as follows:

$$\eta_q = F^{-1}\left(\frac{q}{Q}\right), \mathrm{q} = \{1, \ldots, \mathrm{Q}-1\} \tag{14}$$

Each sample $y_j(i)$ is then assigned to a quantization level as:

$$r(i) = max\{q:\ y_j(i) > \eta_{q-1}\} \tag{15}$$

Each quantization level $r(i)$ is then mapped to a binary codeword $d\big(r(i)\big)$ using a predefined gray codebook, which is also consider a parity bit to enhance robustness.
Finally, the secret key for the jth user is constructed by concatenating these codewords across all M antennas:

$$z_j = \left[\, d\big(r(1)\big), d\big(r(2)\big), \ldots, d\big(r(M)\big)\,\right] \in \{0,1\}^{M.b} \tag{16}$$

3.4 Information Reconciliation

To fix mismatches in the independently quantized channel state information (CSI) caused by the presence of noise (as shown in Eq. (3) and Eq. (4)), this step is needed to ensure both the base station (BS) and the users generate the same key. A common method is to use Low-Density Parity-Check (LDPC) codes **(Gao et al., 2024a; Almaamory, 2011; Gao et al., 2024b).** In this method, the BS creates a short summary of its key, called a syndrome, and sends it over a public channel. The user then uses belief propagation decoding, an algorithm that gradually corrects the errors in their key by comparing it with the syndrome, until it matches the BS's key.
Another approach is to use Principal Component Analysis (PCA) **(Gao et al., 2024a)**. PCA reduces the noise in CSI by projecting it onto a lower-dimensional space that captures the most important patterns. Both the BS and the user apply the same projection and then quantize the result to generate matching key bits.

3.5 Privacy Amplification

To avoid any vulnerability to leakage of information due to the use of a public channel, the key sequences generated are then further processed through the use of a hash function to enhance the security of the physical layer key generation (PLKG) process **(Li et al., 2019)**.

4. SIMULATION RESULTS AND PERFORMANCE EVALUATION

4.1 Performance Analysis

4.1.1 Secret Key Capacity

Here, the secret key capacity of the proposed scheme is analyzed and compared to that of the diagonal RIS and no RIS. Taking into account the two following scenarios, when the direct link is present and when the direct link is fully blocked by an obstacle.
The secret key capacity can be calculated as follows:

$$\boldsymbol{C_{sk} = I\left(\widehat{H}_{Users-BS}, \widehat{H}_{BS-Users}\right) - I\left(\widehat{H}_{Users-BS}, \widehat{H}_{Users-EVE}\right)} \quad (17)$$

Since EVE is more than half wavelength apart from all users, the channels between the users and the BS ($\widehat{\mathbf{H}}_{\mathbf{Users-BS}}$) and between the users and EVE ($\widehat{\mathbf{H}}_{\mathbf{Users-EVE}}$) are independent. Means that there is no mutual information between them **(Wan et al., 2023)**. This is leading to the fact that EVE cannot extract any useful information, and that Eq. (12) is simplified to:

$$\boldsymbol{C_{sk} = I\left(\widehat{H}_{Users-BS}, \widehat{H}_{BS-Users}\right)} \quad (18)$$

Nonetheless, the inclusion of EVE in the system model remains important. It allows for evaluating the security strength of the key generation process under passive eavesdropping conditions. Even when EVE is assumed to monitor the pilot transmissions and access all public reconciliation messages, the independence between the BS-users and EVE-users channels ensures that the secret key generated at EVE differs from that at the legitimate parties which demonstrates that the proposed scheme achieves information-theoretic security grounded in the physical properties of the wireless medium.
Additionally, since time-division duplex TDD mode is assumed in our work, the uplink and downlink channels between users and BS are reciprocal **(Laas et al., 2020)** and hence the secret key capacity depends only on the total channel between users and the BS as seen in Eq. (14):

$$\boldsymbol{\widehat{H}_{Users-BS} = H + F\,\Phi\,G} \quad (19)$$

4.1.2 Autocorrelation (AC) Test

The autocorrelation test is performed to determine the randomness of the cryptographic key streams based on the predictability of key sequences. It checks the similarity between the sequence and its shifted versions. To this end, a key is regarded as valid if it is able to sustain this test, i.e., it has a maximum value at zero lag and minimal values at all other lags **(Ridha and Jawad, 2022; Abdel-Ghaffar and Daoudi, 2023)**.

4.1.3 NIST Test

To further assess the randomness of the generated secret keys, we conduct the National Institute of Standards and Technology (NIST) randomness test on the resulting bit sequences test **(Zhang et al., 2016; Staat et al., 2021)**. According to the test criteria, a sequence is considered to have passed a sub-test if the p-value is not less than 0.01 and perfectly passed it if the p-value is equal to 1. A widely used subset of 8 tests is applied, as adopted in prior PLKG works, to balance completeness and computational feasibility **(Sabir and Abdulhussain, 2011; Wan et al., 2023; Linh et al., 2024).**

4.2 Simulation Setup and Result Discussion

MATLAB is used to simulate the wireless network depicted in **Fig. 1**, where the base station (BS) and the BD-RIS are positioned at coordinates (0, 0, 20) and (50, 5, 1.5), respectively. The distances between the K users and the BD-RIS follow a sequential pattern of (5, 15, 25…) meters, while the eavesdropper is positioned 10 meters from the BD-RIS. The BS is equipped with (M = 64) active antennas, whereas the BD-RIS consists of (N = 128) passive reflecting elements. The total transmission power varies from -5 dBm to 45 dBm. Regarding large-scale fading parameters, the path loss at a reference distance of (d = 1) meter is set to -28 dB, with path loss exponents of 3.75 for direct links and 2.0 for links through the BD-RIS. This choice reflects the fact that direct links are more likely to experience obstruction and severe scattering, leading to higher path loss exponents, while links via the BD-RIS are typically assumed to have line-of-sight (LoS) or near-LoS propagation, allowing them to approximate the free-space conditions with a lower exponent. To ensure accuracy, Monte Carlo simulations with 1000 realizations are conducted. All the parameters used in the simulation are mentioned in **Table 1**.

Fig. 5 shows that BD-RIS outperforms RIS in all scenarios, thereby enhancing the resulting secret key capacity. The reason behind that is the utilization of a full matrix phase shift design in BD-RIS, rather than the diagonal matrix used in RIS, as shown in Eqs. (5, 6). This additional degree of freedom in BD-RIS allows for more efficient signal manipulation, leading to better channel reciprocity and improved key generation performance.

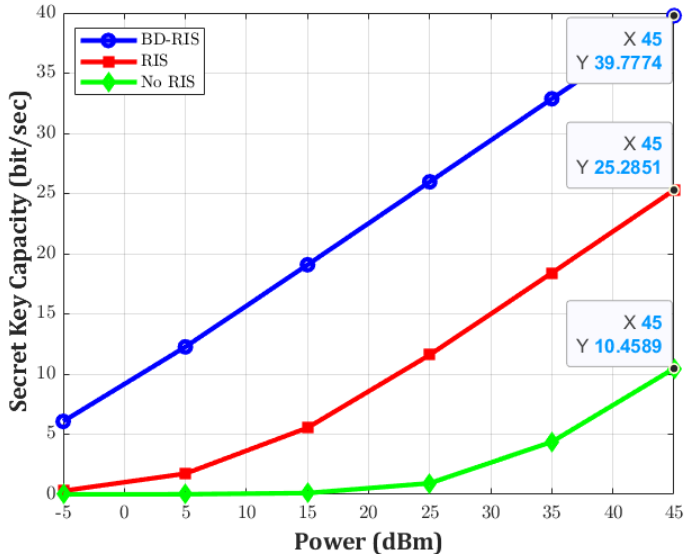
The percentage improvement in secret key capacity is calculated as:

$$Improvement\ percentage\ (\%) = \frac{C_{BD-RIS} - C_{RIS}}{C_{RIS}}\ 100\% \quad (20)$$

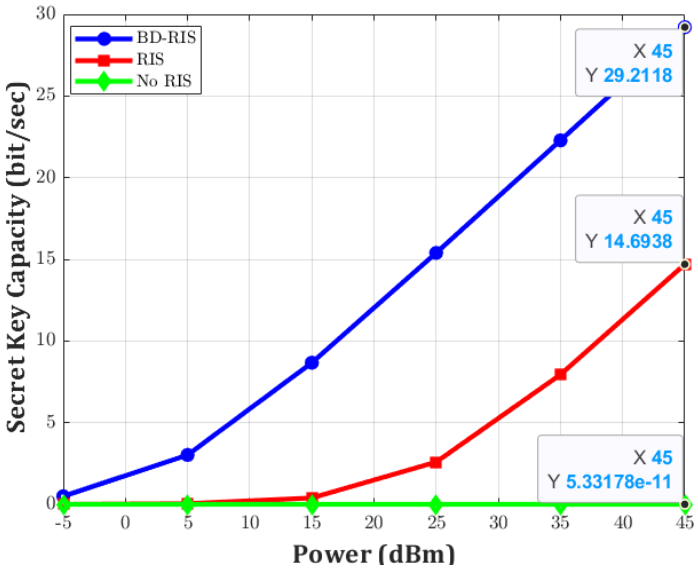
Table 1. Simulation Parameters

Parameter	Value
BS coordinates (X, Y, Z)	(0, 0, 20)
BD-RIS coordinates (X, Y, Z)	(50, 5, 1.5)
The distance between 1st user and BD-RIS	5 m
The step increment between 1st user and kth user with respect to BD-RIS (e.g., 2st user is 15 m from the BS)	10 m
Number of BS antennas, M	64
Number of BD-RIS passive antennas, N	128
Power range, P	(-5: 45) dBm
Reference distance, do	1 m
Reference path loss, L(do)	-28 dB
Path loss exponents of direct links, α	3.75
Path loss exponents of links through the BD-RIS, α	2
Number of Monte Carlo realizations	1000 realization

Notably, at 45 dBm, BD-RIS enhances the secret key capacity by approximately 57.32% compared to RIS when the direct link is present **Fig. (5-a)** and by 57.54% when the direct link is blocked **Fig. (5-b)**, demonstrating its robust performance in different channel conditions. To further validate the effectiveness of the proposed scheme, **Fig. 6** shows that all users' keys meet the conditions for passing the AC test. This confirms that the physical layer key is unpredictable, making it suitable to use as a cryptographic key between any two legitimate parties. Additionally, as shown in **Table 2**, the results of eight sub-tests for all users indicate that all p-values exceed the 0.01 threshold, with some having a value of 1 indicating perfect randomness. These findings confirm that the secret keys generated by the proposed scheme exhibit randomness and satisfy the security requirements necessary for practical communication systems.



(a) The direct link is present.



(b) The direct link is blocked by an obstacle.

Figure 5. Secret Key Capacity (Cs) in bps.

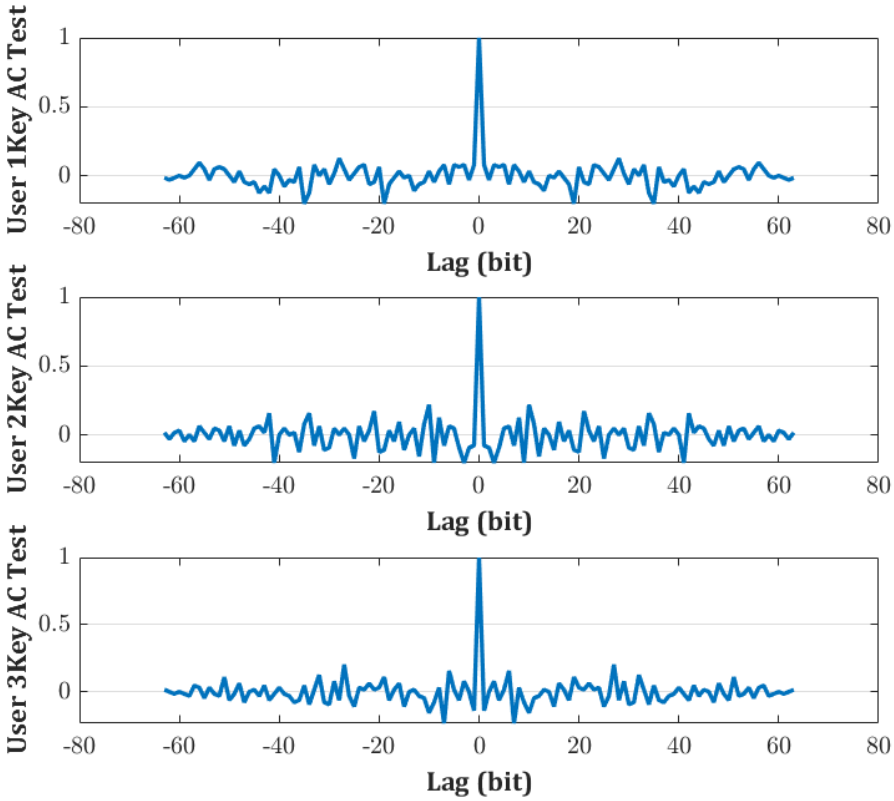


Figure 6. Autocorrelation (AC) test for the generated keys.

Table 2. NIST statistical test.

Test Name	User1	User2	User3
Frequency	1.00000	1.00000	1.00000
Block Frequency	1.00000	0.42350	0.94024
Cumulative Sums	0.28884	0.47950	0.28884
Runs	0.80259	0.31731	0.80259
Longest Run of Ones	0.16261	0.16261	0.16261
Approximate Entropy	1.00000	1.00000	1.00000
Serial	0.94722	0.96210	0.93459
DFT	0.25614	0.62650	0.62650

5. CONCLUSIONS

This paper proposes a Physical Layer Key Generation (PLKG) scheme that leverages the enhanced reconfigurability of Beyond-Diagonal Reconfigurable Intelligent Surfaces (BD-RIS) integrated with multi-user MIMO systems. Our work addresses the fundamental challenge of insufficient entropy in static and quasi-static wireless environments, which has limited the practical deployment of PLKG techniques. Our approach lies in exploiting BD-RIS's ability to manipulate both phase and magnitude of incident signals, in contrast to conventional diagonal RIS (D-RIS) which only controls phase. This additional degree of freedom significantly increases channel randomness and enhances security. The security and randomness of the generated keys are validated through multiple tests. All generated keys successfully passed the Autocorrelation (AC) test, demonstrating they satisfied all eight NIST statistical tests with p-values exceeding the 0.01 threshold, confirming their cryptographic quality

and suitability for secure communications. The tests were in scenarios with a blocked direct link, BD-RIS achieved a remarkable 57.32% improvement over D-RIS and where the direct link is present, BD-RIS still provided a 57.54% improvement at 45 dBm. These results demonstrate that BD-RIS technology offers a promising solution for enhancing entropy for secure key generation, making it particularly valuable for implementation in next-generation wireless applications such as 5G, 6G, and IoT where security is paramount.

NOMENCLATURE

Symbol	Description	Symbol	Description
a	Amplitude of BD-RIS element, dimensionless	n	Additive white Gaussian noise, complex, dimensionless
b	Number of quantization bits, dimensionless	P	Uplink transmission power, dBm
C_s	Secret key capacity, bits per second (bps)	Q	Number of quantization levels, dimensionless
d	Distance between two nodes, m	v	Channel vector from users to EVE
d_0	Reference distance, m	t	Time, s
e	Channel matrix from users to eavesdropper (EVE)	τ	Channel coherence time, s
F	Channel matrix from BS to BD-RIS, size M × N	τ_pilot	Pilot sequence length, s
G	Channel matrix from BD-RIS to users, size K × N	X	Pilot matrix of orthogonal sequences
H	Channel matrix from BS to users, size M × K	α	Path loss exponent, dimensionless
K	Number of legitimate users, dimensionless	β	Factor of variation (randomness), dimensionless
L	Number of antennas at EVE, dimensionless	φ	Phase of BD-RIS element, radians
M	Number of BS antennas, dimensionless	θ	Phase shift angle of RIS/BD-RIS element, radians
m	Nakagami fading parameter, dimensionless	Θ	Scattering matrix of BD-RIS, size N × N
N	Number of BD-RIS elements, dimensionless	Γ(·)	Gamma function

Acknowledgements

This work was supported by the Department of Electronics and Communications Engineering, College of Engineering, University of Baghdad. The authors would also like to thank the Ministry of Higher Education and Scientific Research for its continued academic support under the research project.

Credit Authorship Contribution Statement

Mina Fadhil Hasan: Writing (original draft), Software, Methodology, Validation, Investigation. Aqiel Niama Almamori: Supervision, Conceptualization, Writing (review & editing), Validation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

Abdel-Ghaffar, E.A. and Daoudi, M., 2023. Personal authentication and cryptographic key generation based on electroencephalographic signals. *Journal of King Saud University - Computer and Information Sciences*, 35(5), P. 101541. https://doi.org/10.1016/j.jksuci.2023.03.019.

Akbarpour-Kasgari, A. and Ardebilipour, M., 2018. Probability-based pilot allocation for MIMO relay distributed compressed sensing channel estimation. *EURASIP Journal on Advances in Signal Processing*, 2018(1), P. 18. https://doi.org/10.1186/s13634-018-0539-7.

Almaamory, A., 2011. LDPC coded multiuser MC-CDMA performance over multipath Rayleigh fading channel. *Journal of Engineering*, 17(04), pp. 1039–1046. https://doi.org/10.31026/j.eng.2011.04.28.

Al-Nahhas, B., Obeed, M., Chaaban, A. and Hossain, M.J., 2021. RIS-aided cell-free massive MIMO: Performance analysis and competitiveness. In: *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. pp. 1–6. https://doi.org/10.1109/ICCWorkshops50388.2021.9473521.

Demir, Ö.T. and Björnson, E., 2022. Is channel estimation necessary to select phase-shifts for RIS-assisted massive MIMO? *IEEE Transactions on Wireless Communications*, 21(11), pp. 9537–9552. https://doi.org/10.1109/TWC.2022.3177700.

Fang, T. and Mao, Y., 2024. A low-complexity beamforming design for beyond-diagonal RIS aided multi-user networks. *IEEE Communications Letters*, 28(1), pp. 203–207. https://doi.org/10.1109/LCOMM.2023.3333411.

Gao, N., Han, Y., Li, N., Jin, S. and Matthaiou, M., 2024a. When physical layer key generation meets RIS: opportunities, challenges, and road ahead. *IEEE Wireless Communications*, 31(3), pp. 355–361. https://doi.org/10.1109/MWC.013.2200538.

Gao, N., Yao, Y., Jin, S., Li, C. and Matthaiou, M., 2024b. RIS-assisted simultaneous transmission and secret key generation: An ICAS paradigm. In: *IEEE INFOCOM 2024 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. pp. 1–6. https://doi.org/10.1109/INFOCOMWKSHPS61880.2024.10620776.

Gómez-Déniz, E. and Gómez-Déniz, L., 2024. A new derivation of the Nakagami-m distribution as a composite of the Rayleigh distribution. *Wireless Networks*, 30(5), pp. 3051–3060. https://doi.org/10.1007/s11276-024-03713-5.

Hamza, K.M., Basharat, S., Jung, H., Gidlund, M. and Hassan, S.A., 2024. Secrecy analysis of RIS-assisted uplink NOMA systems under Nakagami-m fading. In: *2024 IEEE International Conference on Communications Workshops (ICC Workshops)*. pp. 1511–1516. https://doi.org/10.1109/ICCWorkshops59551.2024.10615519.

Hu, X., Jin, L., Huang, K., Sun, X., Zhou, Y. and Qu, J., 2021. Intelligent reflecting surface-assisted secret key generation with discrete phase shifts in static environment. *IEEE Wireless Communications Letters*, 10(9), pp. 1867–1870. https://doi.org/10.1109/LWC.2021.3084347.

Ji, Z., Yeoh, P.L., Zhang, D., Chen, G., Zhang, Y., He, Z., Yin, H. and li, Y., 2021. Secret key generation for intelligent reflecting surface assisted wireless communication networks. *IEEE Transactions on Vehicular Technology*, 70(1), pp. 1030–1034. https://doi.org/10.1109/TVT.2020.3045728.

Laas, T., Nossek, J.A., Bazzi, S. and Xu, W., 2020. On reciprocity in physically consistent TDD systems with coupled antennas. *IEEE Transactions on Wireless Communications*, 19(10), pp. 6440–6453. https://doi.org/10.1109/TWC.2020.3003414.

Li, G., Sun, C., Zhang, J., Jorswieck, E., Xiao, B. and Hu, A., 2019. Physical layer key generation in 5G and beyond wireless communications: challenges and opportunities. *Entropy*, https://doi.org/10.3390/e21050497.

Li, H., Shen, S., Zhang, Y. and Clerckx, B., 2024. Channel estimation and beamforming for beyond diagonal reconfigurable intelligent surfaces. *IEEE Transactions on Signal Processing*, 72, pp. 3318–3332. https://doi.org/10.1109/TSP.2024.3424229.

Linh, D. v., Yem, V. v., Kien, T. V and Thao, H.T.P., 2024. Key generation algorithms based on complex components of channel impulse response for massive MIMO wireless communication systems. *IEEE Access*, 12, pp. 89947–89956. https://doi.org/10.1109/ACCESS.2024.3419052.

Liu, Y., Chen, H.-H. and Wang, L., 2017. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Communications Surveys & Tutorials*, 19(1), pp. 347–376. https://doi.org/10.1109/COMST.2016.2598968.

Mishra, A., Mao, Y., D'Andrea, C., Buzzi, S. and Clerckx, B., 2024. Transmitter side beyond-diagonal reconfigurable intelligent surface for massive MIMO networks. *IEEE Wireless Communications Letters*, 13(2), pp. 352–356. https://doi.org/10.1109/LWC.2023.3329065.

Mohammed, S.A., 2020. Securing physical layer for FHSS communication system using code and phase hopping techniques in CDMA, system design and implementation. *Journal of Engineering*, 26(7), pp. 190–205. https://doi.org/10.31026/j.eng.2020.07.13.

Nerini, M., Shen, S. and Clerckx, B., 2024. Closed-form global optimization of beyond diagonal reconfigurable intelligent surfaces. *IEEE Transactions on Wireless Communications*, 23(2), pp. 1037–1051. https://doi.org/10.1109/TWC.2023.3285262.

Patwari, N., Croft, J., Jana, S. and Kasera, S.K., 2010. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Transactions on Mobile Computing*, 9(1), pp. 17–30. https://doi.org/10.1109/TMC.2009.88.

Ridha, O. and Jawad, G., 2022. Scheme for generating true random numbers using electro-mechanical switches. *Journal of Engineering*, 28(3), pp. 73–85. https://doi.org/10.31026/j.eng.2022.03.06.

Sabir, F. and Abdulhussain, S., 2011. Image based multi-length random key generator. *Journal of engineering*, 17(03), pp. 486–498. https://doi.org/10.31026/j.eng.2011.03.11.

Samy, M., Al-Hraishawi, H., Adam, A.B.M., Chatzinotas, S. and Otteresten, B., 2025. Beyond diagonal RIS-aided networks: Performance analysis and sectorization tradeoff. *IEEE Open Journal of the Communications Society*, 6, pp. 302–315. https://doi.org/10.1109/OJCOMS.2024.3514696.

Santamaria, I., Soleymani, M., Jorswieck, E. and Gutiérrez, J., 2024. MIMO capacity maximization with beyond-diagonal RIS. In: *2024 IEEE 25th International Workshop on Signal Processing Advances in*

Wireless Communications (SPAWC). pp. 936–940. https://doi.org/10.1109/SPAWC60668.2024.10694491.

Shahiri, V., Behroozi, H., Kuhestani, A. and Wong, K.-K., 2024. Reconfigurable-intelligent-surface-assisted secret key generation under spatially correlated channels in quasi-static environments. *IEEE Internet of Things Journal*, 11(9), pp. 15808–15822. https://doi.org/10.1109/JIOT.2023.3349354.

Shen, S., Clerckx, B. and Murch, R., 2022. Modeling and architecture design of reconfigurable intelligent surfaces using scattering parameter network analysis. *IEEE Transactions on Wireless Communications*, 21(2), pp. 1229–1243. https://doi.org/10.1109/TWC.2021.3103256.

Shlezinger, N., Alexandropoulos, G.C., Imani, M.F., Eldar, Y.C. and Smith, D.R., 2021. Dynamic metasurface antennas for 6G extreme massive MIMO communications. *IEEE Wireless Communications*, 28(2), pp.106–113. https://doi.org/10.1109/MWC.001.2000267.

Singh, S., Raviteja, A., Singh, K., Singh, S.K., Kaushik, A. and Ku, M.L., 2024. Secrecy rate maximization for active RIS-aided robust uplink NOMA communications. *IEEE Wireless Communications Letters*. https://doi.org/10.1109/LWC.2024.3424332.

Staat, P., Elders-Boll, H., Heinrichs, M., Kronberger, R., Zenger, C. and Paar, C., 2021. Intelligent reflecting surface-assisted wireless key generation for low-entropy environments. In: *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. pp. 745–751. https://doi.org/10.1109/PIMRC50174.2021.9569556.

Wan, Z., Lou, Y., Xu, X., Yang, J., Jiang, W., Huang, K. and Jin, L., 2023. Physical-layer key generation based on multipath channel diversity using dynamic metasurface antennas. *China Communications*, 20(4), pp. 153–166. https://doi.org/10.23919/JCC.fa.2022-0637.202304.

Wang, Q., Su, H., Ren, K. and Kim, K., 2011. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In: *Proceedings - IEEE INFOCOM*. pp.1422–1430. https://doi.org/10.1109/INFCOM.2011.5934929.

Yang, S., Han, H., Liu, Y., Guo, W., Pang, Z. and Zhang, L., 2023. Reconfigurable intelligent surface-induced randomness for mmwave key generation. In: *ICC 2023 - IEEE International Conference on Communications*. pp. 2909–2914. https://doi.org/10.1109/ICC45041.2023.10278950.

Zhang, J., Marshall, A., Woods, R. and Duong, T.Q., 2016. Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers. *IEEE Transactions on Communications*, 64(6), pp. 2578–2588. https://doi.org/10.1109/TCOMM.2016.2552165.

Zhang, J., Rajendran, S., Sun, Z., Woods, R. and Hanzo, L., 2019. Physical layer security for the internet of things: authentication and key generation. *IEEE Wireless Communications*, 26(5), pp. 92–98. https://doi.org/10.1109/MWC.2019.1800455.

تحسين كفاءة توليد المفاتيح السرية المعتمدة على الطبقة المادية في نظام متعدد المدخلات والمخرجات ولمستخدمين عدة عن طريق استخدام الأسطح الذكية القابلة لإعادة التشكيل غير القطرية

مينا فاضل حسن*، عقيل نعمة المعموري

قسم هندسة الإلكترونيات والاتصالات، كلية الهندسة، جامعة بغداد، بغداد، العراق

الخلاصة

يعتبر توليد المفاتيح السرية المعتمدة على الطبقة المادية (PLKG) نهجًا واعدًا لإنشاء مفاتيح تشفير آمنة بين الأطراف الشرعية. ومع ذلك، في البيئات الساكنة وشبه الساكنة، يكون معدل توليد المفاتيح محدودًا بشكل كبير نتيجة انخفاض العشوائية في القناة اللاسلكية. للتغلب على هذا التحدي، تم اقتراح الأسطح الذكية القابلة لإعادة التشكيل (RIS) لتعزيز عشوائية القناة عبر تعديل طور الموجات الكهرومغناطيسية الساقطة. يعالج هذا البحث هذه المشكلة من خلال اقتراح بنية أمنية تدمج نظام متعدد المدخلات والمخرجات (MIMO) مع سطح ذكي قابل لإعادة التشكيل غير القطري (BD-RIS) في سيناريوهات متعددة المستخدمين، مع وجود طرف متنصت. على عكس الأسطح الذكية التقليدية (RIS)، فإن BD-RIS لا يقوم فقط بتعديل الطور فحسب، ولكنه يستطيع أيضًا من ضبط مقدار الإشارات الساقطة، مما يوفر درجة إضافية من الحرية والتي تحسن من عشوائية القناة بشكل أكبر. تمت مقارنة سعة المفتاح السري للنظام المقترح مع نظام RIS التقليدي في حالتين: الأولى عند وجود رابط مباشر بالإضافة إلى المسار المساعد عبر BD-RIS، والثانية عندما يكون الرابط المباشر محجوبًا تمامًا بسبب وجود عائق. أظهرت نتائج المحاكاة أن البنية المقترحة لـ BD-RIS تتفوق على الأسطح الذكية القطرية التقليدية (D-RIS) في جميع السيناريوهات المدروسة. علاوة على ذلك، خضعت المفاتيح المولدة لاختبارات العشوائية، حيث نجحت في اجتياز جميع اختبارات العشوائية الخاصة بالمعهد الوطني للمعايير والتكنولوجيا (NIST) بالإضافة إلى اختبار الارتباط الذاتي (AC)، مما يؤكد صلاحيتها للتطبيقات الاتصالية الآمنة. تؤكد هذه النتائج أن BD-RIS يُعدّ تقنية واعدة لتعزيز أمن الطبقة الفيزيائية في البيئات الساكنة لشبكات الجيل الخامس (G5) والجيل السادس (G6) وتطبيقات إنترنت الأشياء (IoT).

الكلمات المفتاحية: اختبار الارتباط الذاتي (AC)، BD-RIS، NIST، RIS، توليد المفتاح السري.