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

Reconfigurable intelligent surface-aided secret key generation using autoencoder and K-means quantization*

Zhenling LI†[1], Panpan XU[1], Qiangqiang GAO[2,3], Chunguo LI[4], Weijie TAN‡[2,3]

[1]*School of Mathematics and Statistics, GuiZhou University, Guiyang 550025, China*

[2]*State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China*

[3]*School of Computer Science and Technology, Guizhou University, Guiyang 550025, China*

[4]*School of Information Science and Engineering, Southeast University, Nanjing 212013, China*

‡E-mail: wjtan@gzu.edu.cn

Received Seb. 13, 2024; Revision accepted Dec. 17, 2024; Crosschecked

Abstract: In quasi-static wireless channel scenarios, the generation of physical layer keys faces the challenge of invariant spatial and temporal channel characteristics, resulting in a high key disagreement rate (KDR) and low key generation rate (KGR). To address these issues, this paper proposes a novel reconfigurable intelligent surface (RIS)-aided secret key generation approach using an autoencoder (AE) and K-means quantization algorithm. The proposed method utilizes channel state information (CSI) for channel estimation and dynamically adjusts the reflection coefficients of the RIS to create a rapidly fluctuating channel. This strategy enables the extraction of dynamic channel parameters, enhancing channel randomness. Additionally, by integrating the autoencoder with the K-means clustering quantization algorithm, the method efficiently extracts random bits from complex, ambiguous, and high-dimensional channel parameters, significantly reducing KDR. Simulation experiments demonstrate that, under various signal-to-noise ratios (SNRs), the proposed method performs excellently in terms of KGR and KDR. Additionally, the randomness of the generated keys is validated through the National Institute of Standards and Technology (NIST) test suite.

Key words: Reconfigurable intelligent surface; Physical layer key generation; Quantization; Autoencoder
https://doi.org/10.1631/FITEE.2400799 **CLC number:** TP

Unedited

1 Introduction

With the rapid advancement of wireless communication technologies, ensuring secure data transmission has become an increasingly critical challenge. Unlike wired networks, wireless communication operates via electromagnetic waves, which are inherently exposed to potential eavesdropping and malicious interference. The open nature of wireless transmission, coupled with the broadcast characteristics of radio frequency signals, significantly increases the risk of unauthorized interception, tampering, and data leakage. This vulnerability has spurred the demand for more robust encryption methods to safeguard communication in dynamic and hostile environments.

Traditional cryptographic approaches, while effective, often rely on computational complexity to secure information. However, they may not be sufficient to counter evolving threats, particularly in resource-constrained environments. In response, physical layer key generation has emerged as a promising solution, leveraging the unique characteristics of the wireless channel itself to generate symmetric keys for encryption. One notable method, proposed by Mathur, capitalizes on the inherent properties of the wireless channel reciprocity, chronicity, and spatial decorrelation to generate highly secure and dynamic keys for data encryption Mathur et al. (2008).

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (No. 62361010), the Research Project of Guizhou University for Talent Introduction (No. [2020]61), the Cultivation Project of Guizhou University (No. [2019]56), and the Major Scientific and Technological Special Project of Guizhou Province (No. [2024]014)

ORCID: Weijie TAN, https://orcid.org/0000-0001-6590-5757

© Zhejiang University Press 2025

Reciprocity ensures that both communicating parties, typically referred to as Alice and Bob, experience correlated channel responses, allowing them to independently generate identical cryptographic keys without transmitting sensitive information over the air. Chronicity exploits the time-varying nature of the wireless environment to continuously update keys, enhancing their unpredictability and resilience against eavesdropping, even in the presence of fading and interference. Finally, spatial decorrelation ensures that an eavesdropper, located beyond a half-wavelength distance from the legitimate users, cannot reconstruct the shared key due to the uncorrelated nature of the channel at their position.

However, the variability required for robust key generation can be limited in real-world applications, particularly in time-domain quasi-static environments where the wireless channel changes gradually. These scenarios often suffer from reduced time-domain randomness and slower key update rates, making it difficult to maintain a high level of security and efficiency in key generation. Fig 1 illustrates the challenges presented by such quasi-static environments, where maintaining sufficient channel randomness becomes a crucial concern.

To address these challenges, the advent of reconfigurable intelligent surface (RIS) offers a promising solution. RIS comprises a large number of passive, programmable scattering elements that can dynamically modify the amplitude and phase of reflected electromagnetic waves in a controlled manner Wu et al. (2021). Through precise coordination, RIS can actively manipulate the propagation environment, introducing additional degrees of freedom into the wireless channel. This capability not only enhances the randomness and uniqueness of the channel but also enables higher key generation rates (KGRs) without increasing transmission power or introducing complex signal processing, as is the case with traditional relay technologies Shlezinger et al. (2021).

While existing research predominantly focuses on improving the randomness of key sources to enhance KGRs, challenges such as key disagreement rates (KDRs) remain significant Zeng (2015). To overcome these limitations, this paper proposes a novel RIS-aided secret key generation scheme. By integrating an autoencoder (AE) and a K-means quantization algorithm, we aim to reduce KDRs while simultaneously increasing key generation efficiency. This approach leverages the reconfigurable nature of RIS to dynamically influence the wireless channel, providing a more reliable and

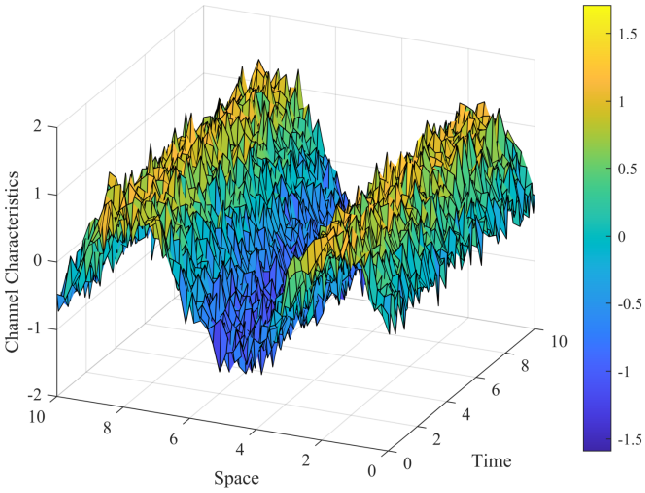

Fig. 1 Quasi-static scene in time-space domain.

secure method for key generation in both quasi-static and dynamic environments. The specific contributions of this paper are outlined below.

- Construction of a fast-varying channel: The reflection coefficient of RIS is changed to enhance the randomness and variability of the channel under quasi-static conditions. This adjustment facilitates coherent time-based channel estimation between the base station (Alice) and the authorized user (Bob), thereby enabling effective key extraction.
- Autoencoder and K-means (AE-K-means) clustering quantization algorithm for key generation: Initially, the channel feature values are denoised and compressed through an autoencoder, effectively preserving the key structural characteristics of the data. Afterward, K-means clustering is applied to the compressed data, optimizing the quantization process and minimizing KDRs during encoding.
- Performance evaluation via simulation: Simulation-based assessments demonstrate the efficacy of the proposed method across varied signal-to-noise ratios (SNRs). The evaluation of KGR and KDR under different SNR conditions was conducted. Furthermore, the randomness of generated keys is validated through rigorous testing using the National Institute of Standards and Technology (NIST) test suite.

The rest of this article is organized as follows. Section 2 delves into the related work, while Section 3

Unedited

presents the system model. Section 4 presents the key generation method and Section 5 provides simulation results and analysis. Finally, Section 6 concludes this article.

2 Related work

In the early 20th century, Claude Shannon laid the foundation for physical layer security with his theoretical model aimed at achieving absolute security through the principle of "one secret at a time" Shannon (1949). While this model was groundbreaking, its practical implementation has proven challenging. Abraham Wyner later proposed the "wiretap channe" model to improve security by leveraging the noise inherent in communication channels. However, this model faced limitations in scenarios where an eavesdropper could potentially acquire more information than the legitimate receiver Wyner (1975). Hershey et al. (1995) advanced these concepts by utilizing channel reciprocity and fast temporal variations to generate cryptographic keys from wireless channels, thus paving the way for physical layer key generation techniques.

Physical layer key generation typically follows a structured process: channel estimation, key quantization, information reconciliation, and privacy amplification Luo et al. (2023); Han et al. (2020). While these techniques are effective, challenges persist in improving the randomness of key sources and enhancing KGRs. Efforts to address these limitations have included the introduction of artificial random sources Lou et al. (2017), exploitation of Multiple input multiple output (MIMO) systems Li et al. (2017), and utilization of multipath fading for enhanced randomness Liu et al. (2012). Relay collaboration has also been explored to increase the number of reciprocal channels and boost KGRs Shimizu et al. (2011). However, many of these methods struggle in environments with limited channel variability, such as quasi-static scenarios.

To overcome these limitations, RIS has gained significant attention for its ability to dynamically manipulate wireless propagation environments. By steering incident signals in fully customizable ways, RIS introduces artificial randomness into the channel, enhancing key generation in quasi-static environments Ji et al. (2021); Lu et al. (2021). Recent studies have also demonstrated its potential to improve energy efficiency and scalability in future communication systems through the joint optimization of active and passive beamforming Wang et al. (2024b). However, the optimization space in RIS-aided systems is often highly non-convex due to the interdependencies between base station (Alice) precoding matrices and RIS phase-shifting matrices. To address this problem, gradient-based meta-learning approaches such as gradient-based manifold meta learning (GMML) Zhu et al. (2024) and gradient-based meta learning (GMLB) Wang et al. (2024b) have been proposed. These methods utilize manifold learning and meta-learning techniques to optimize RIS parameters without requiring pretraining, achieving significant improvements in spectral efficiency and energy consumption.

Recent advancements have also explored the synergy between RIS and machine learning (ML) techniques. For instance, a novel gradient-based liquid neural network (GLNN) framework has been proposed for millimeter-wave (mmWave) MIMO systems, which addresses the challenges of dynamic and highly variable channels by utilizing differential equations-based liquid neurons to enhance robustness and efficiency Wang et al. (2024a). These methods underscore the potential of combining RIS with advanced ML paradigms to tackle the complexity of modern wireless environments.

Parallel to the progress in RIS-based systems, ML has emerged as a powerful tool to enhance the efficiency of physical layer key generation. ML techniques have been applied to improve various stages of the key generation process, including channel estimation, quantization, and reconciliation. For example, Ye *et al.* a direct input deep neural network (DNN) for channel estimation, demonstrating superior performance over traditional methods Ye et al. (2020). Yu *et al.* introduced CSINet, a deep learning-based channel state information (CSI) sensing and recovery mechanism, which uses compressed sensing to improve reciprocity in key generation Yu et al. (2020). Additionally, adaptive multilevel quantization techniques incorporating ML algorithms have shown promise in optimizing quantization thresholds and reducing KDRs under dynamic channel conditions Zhou et al. (2020). Generative adversarial networks (GANs) and convolutional neural networks (CNNs) have further been employed to enhance channel characteristic prediction. Mathur *et al.* combined CNNs with GANs to improve downlink CSI prediction, enhancing the accuracy of channel estimates and the key generation process Mathur et al. (2008). Fully connected neural networks have also been used to model channel mapping functions, improving the reciprocity of uplink

Unedited

and downlink channels Wu et al. (2013).

Despite these advancements, challenges remain in improving the robustness of key generation in quasi-static or slow-changing environments. Building on these developments, our proposed method integrates RIS with an AE-K-means quantization algorithm, combining the strengths of ML and RIS to address the limitations of traditional key generation methods. Specifically, the autoencoder is used to capture and compress the high-dimensional features of the channel, while K-means clustering is applied to efficiently quantize the channel features, reducing KDRs and improving overall key generation efficiency. Unlike traditional deep learning-based approaches, our method leverages RIS to dynamically adjust the channel environment, enhancing the randomness and variability of the key source. Moreover, our method's hybrid approach integrates RIS flexibility with ML's predictive capabilities, offering a robust solution for physical layer key generation in both quasi-static and highly dynamic environments.

3 System model

Existing physical layer key generation techniques often rely on passive random variations in the wireless channel. These techniques face limitations in quasi-static environments where the channel remains stable over time, reducing the randomness necessary for secure key generation. Our proposed RIS-aided method overcomes this by introducing dynamic control over the channel conditions. Specifically, by adjusting the reflection coefficients of the RIS, we can artificially induce rapid, controlled variations in the channel state. This added layer of control allows us to generate a highly fluctuating channel even in otherwise stable conditions, increasing the randomness and security of the generated keys.

Unlike conventional approaches, which depend on natural multipath effects or user mobility, our method leverages RIS as an active component in the key generation process. This distinct capability provides two major advantages: (1) RIS enables us to customize the spatial and temporal properties of the channel, directly influencing key entropy and (2) our method is applicable in static environments or where user movement is minimal, as RIS adjustments replace the need for external variations. Through these characteristics, our RIS-aided key generation method addresses inherent limitations in traditional approaches.

The key generation system model based on RIS, as depicted in Fig. 2, consists of a base station named Alice, a legitimate user referred to as Bob, a passive eavesdropper known as Eve, and the RIS itself. Time division duplexing (TDD) mode is employed for transmitting narrowband signals between the base station and legitimate user Bob, ensuring channel reciprocity. The base station Alice is outfitted with M root antennas, while both legitimate users Bob and Eve are equipped with single antennas. The RIS incorporates N reflection units. The RIS controller rapidly adjusts the reflection unit coefficients through a wired control link based on random control signals, inducing quick and random changes in the phase information of the reflected signals. This model establishes a framework for secure key generation leveraging the distinctive functionalities of RIS within the wireless communication setting.

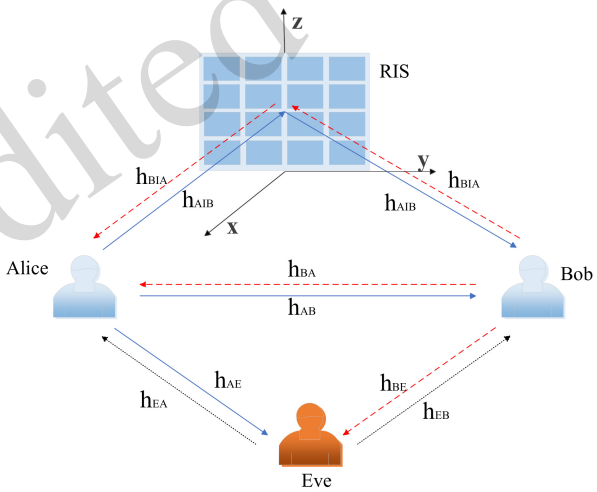

Fig. 2 The system model for key generation based on RIS. RIS: Reconfigurable intelligent surfaces.

In this paper, the following three types of channels are considered: direct channel, indirect channel, and reflection channel Zhou et al. (2020). The direct channel $h_{d,AB} = [h_{d,AB,1}, h_{d,AB,2}, \ldots, h_{d,AB,M}] \in C^{1\times M}$ represents the link between the base station Alice and the legitimate user Bob, while the indirect channel $H_{AR} = [h_{AR,1}, h_{AR,2}, \ldots, h_{AR,N}]^T \in C^{N\times M}$ pertains to the connection between the base station Alice and the RIS. The reflection channel $h_{RB} = [h_{RB,1}, h_{RB,2}, \ldots, h_{RB,N}] \in C^{1\times N}$ denotes the path between the RIS and the legitimate user Bob. Where, $h_{AR,i} = [h_{AR,i,1}, h_{AR,i,2}, \ldots, h_{AR,i,N}] \in C^{1\times M}$. To simulate the actual channel environment, this section models the subchannel in the system model as a Rayleigh

Unedited

fading channel, expressed as

$$h = \sqrt{\frac{\alpha}{1+\alpha}} h^{LOS} + \sqrt{\frac{1}{1+\alpha}} h^{NLOS} \tag{1}$$

where, α is the Rayleigh factor and h^{LOS} and h^{NLOS} represent the Line of sight (LOS) component and the Non-Line of sight (NLOS) Rayleigh fading component, respectively. Since the RIS is close to the base station, the size of the LOS component in the indirect channel depends on α, referring to the far field communication channel model. Both the direct channel and the reflection channel are characterized by a Rayleigh fading model, where the fading parameter α is set to zero. The channel follows a complex Gaussian distribution with a mean of 0. To further characterize the quasi-static scenario of Internet of things (IoT), all channels are modeled as block fading channels, remain constant over longer coherence times, and are independent of each other when they have different coherence times.

According to the spatial propagation characteristics of electromagnetic waves, there is independence between different channels and reciprocity between upstream and downstream channels. The channel is assumed to have a mean of 0 and a variance of σ^2, with both legitimate users, Alice and Bob, experiencing independent and identically distributed Gaussian white noise. To maintain anonymity, the distance between Eve and the legitimate users is greater than half a wavelength, allowing only passive eavesdropping without interfering with information transmission and key generation processes.

4 The proposed key generation method

Building upon the described system model and traditional physical layer key generation techniques, a novel approach to physical layer key generation is introduced. This method incorporates RIS and utilizes an AE-K-means quantization algorithm, including five steps: constructing fast-changing channel, channel detection, quantization and coding, information coordination, and privacy amplification. During the coherent time, the base station Alice conducts the channel estimation with the legitimate user Bob and takes the channel estimation result as the secret key source. Before each channel estimation, the base station Alice randomly changes the RIS reflection coefficient through the controller and ensures that the reflection coefficients are independent of each other to construct the fast-changing channel. During the coherence time, the above step is repeated several times until a key of sufficient length is generated. The specific flowchart is shown in Fig. 3.

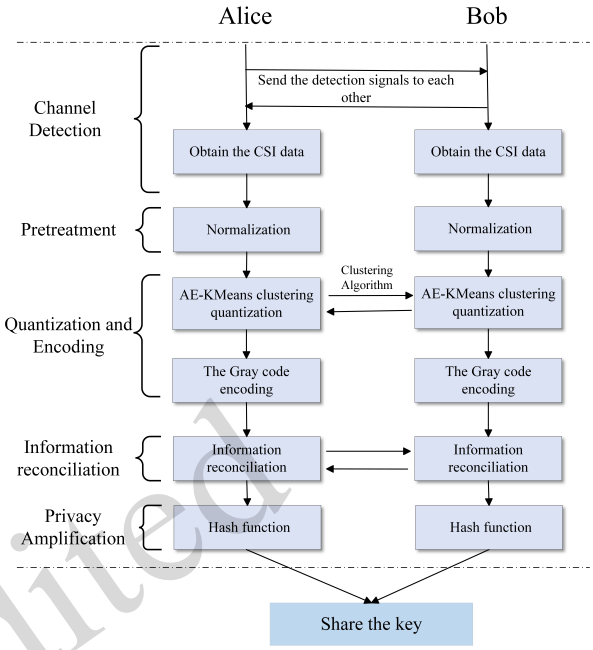

Fig. 3 Flow chart of key generation based on RIS. RIS: Reconfigurable intelligent surfaces.

4.1 Construction of a fast-varying channel

As shown in Fig. 3, defining $h_{AB} \in C^{1\times M}$ represents the combined channel linking the base station Alice and the legitimate user Bob, with:

$$\begin{aligned} h_{AB} &= h_{d,AB} + h_{RB}\Theta H_{AR} \\ &= h_{d,AB} + [\sum_{n}^{N} h_{RB,n} e^{j\phi_n} h_{AR,n,1}, \sum_{n}^{N} h_{RB,n} e^{j\phi_n} h_{AR,n,2}, \\ &\ldots, \sum_{n}^{N} h_{RB,n} e^{j\phi_n} h_{AR,n,M}] \end{aligned} \tag{2}$$

where Θ=$diag(\theta) \in C^{N\times N}$ represents the reflection coefficient of the RIS, θ=$[\theta_1, \theta_2, \ldots, \theta_N] \in C^{N\times 1}$, $\theta_n \in \Phi$. Φ represents the value range of the reflection coefficient θ_n of the n-$th(n \in 1, 2, \ldots, N)$ reflection unit. Considering the discrete change of θ, the value of Θ is as follows :

$$\Theta = \left\{\theta_n | \theta_n = e^{j\phi_n}, \phi_n \in [0, 2\pi)\right\} \tag{3}$$

Before each channel estimation, the base station Alice randomly changes the value of θ and makes it

Unedited

independent of each other, thus greatly improving the chronotaxis and randomness of each channel estimation result and constructing a fast-changing channel.

To validate the effect of dynamic adjustment of RIS reflection coefficients on channel fluctuation, we conducted comparative experiments. As illustrated in Fig. 4, the channel magnitude characteristics of the three key generation methods reveal stark differences. Static reflection and traditional key generation methods exhibit minimal variation, resulting in limited channel randomness. In contrast, the dynamic RIS-aided method demonstrates significant fluctuations in channel magnitude over time, attributed to the active adjustment of RIS reflection coefficients. This enhanced randomness directly improves the mutual information between the transmitter and receiver, thereby improving the KGR.

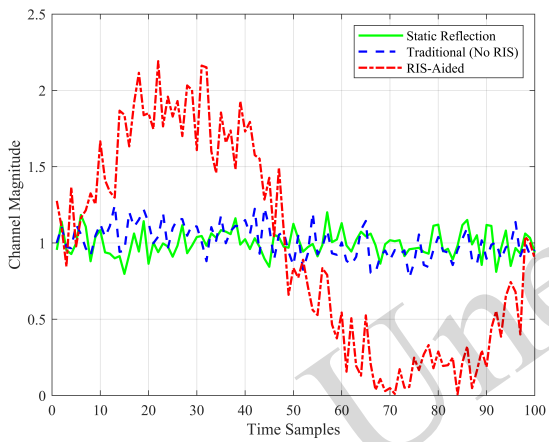

Fig. 4 Channel magnitude for different key generation methods.

4.2 Channel detection

When the base station Alice controls the RIS to induce rapid phase changes, both the base station Alice and the legitimate user Bob perform pilot-based channel estimation. This process can be repeated multiple times within the coherence time. Taking the number $i(i \in 1, 2, \ldots, L)$ channel estimate as an example, order Θ_i and $h_{AB,i}$ indicate the values of Θ and h_{AB} at the secondary channel estimation, respectively. $X_{AB,i} \in C^{M\times l}$ and $x_{BA,i} \in C^{1\times l}$ represent the pilot information of length l transmitted during the i-th channel estimation, with $X_{AB,i}$ denoting the pilot from the base station Alice to the legitimate user Bob, and $x_{BA,i}$ denoting the pilot from Bob to Alice. In this phase, the multiple antenna signal transmitted by the base station Alice undergoes maximum ratio combining (MRC). Order $y_{BA,i} \in C^{1\times l}$ and $Y_{AB,i} \in C^{1\times l}$ represent the signals received by the legitimate user Bob and the base station Alice, respectively, and the expression of the received signals is as follows:

$$y_{BA,i} = (h_{d,AB} + h_{RB}\Theta_i H_{AR})X_{AB,i} + n_{BA,i} \quad (4)$$

$$Y_{AB,i} = w(h_{d,AB}^H + H_{AR}^H\Theta_i h_{RB}^H)x_{BA,i} + wn_{AB,i} \quad (5)$$

where $w \in C^{1\times M}$ is the MRC vector and $n_{BA,i}$ and $n_{AB,i}$ represent the noise received by the base station Alice and the legitimate user Bob when the i-th channel is estimated, respectively. Using the forced zero algorithm, $\tilde{h}_{BA,i}$ and $\tilde{h}_{AB,i}$ represent the estimate of channel h_i by the legitimate user Bob and the base station Alice, respectively, then

$$\begin{aligned}\tilde{h}_{BA,i} =& \frac{X_{AB,i}^T}{||X_{AB,i}||^2} y_{BA,i} \\ =& h_{d,AB,i} + h_{RB,i}\Theta_i H_{AR,i} + \frac{X_{AB,i}^T}{||X_{AB,i}||^2} n_{BA,i}\end{aligned} \quad (6)$$

$$\begin{aligned}\tilde{h}_{AB,i} =& \frac{x_{BA,i}^T}{||x_{BA,i}||^2} y_{AB,i} \\ =& w^H(h_{d,AB,i}^H + H_{AR,i}^H\Theta_i h_{RB,i}^H) + \frac{x_{BA,i}^T}{||x_{BA,i}||^2} w^H n_{AB,i}\end{aligned} \quad (7)$$

Following multiple channel estimates, H_{AB} and H_{BA} denote the comprehensive channel estimates acquired by the base station Alice and the legitimate user Bob, respectively.

$$H_{AB} = [\tilde{h}_{AB,1}, \tilde{h}_{AB,2}, \ldots, \tilde{h}_{AB,L}]^T \quad (8)$$

$$H_{BA} = [\tilde{h}_{BA,1}, \tilde{h}_{BA,2}, \ldots, \tilde{h}_{BA,L}]^T \quad (9)$$

where L represents the number of channel estimates. Because the channel parameters of H_{AR} and h_{RB} change rapidly over time and Θ at each channel estimation are independent, the channel h_{AB} is highly randomness and time-varying compared with $h_{d,AB}$, which can greatly improve the KGR.

4.3 Quantization algorithm based on AE-K-means clustering

Quantization transforms channel features into a binary form, known as the initial key. To enhance both computational efficiency and quantization accuracy, we integrate an AE-K-means clustering for the quantization process. This combination leverages the strengths of both techniques to achieve optimal performance.

The autoencoder efficiently compresses high-dimensional channel data into a lower-dimensional representation, significantly reducing data complexity while

Unedited

preserving critical features necessary for accurate quantization. This step ensures that the essential channel characteristics required for key generation are retained. Subsequently, K-means clustering refines this compressed output by categorizing similar data points, which minimizes quantization errors and ensures that the quantization process is both precise and reliable.

This approach also provides robustness to variations in channel conditions. The adaptive nature of the autoencoder and the iterative optimization process of K-means clustering enable the system to dynamically adjust to changes in the channel structure. This adaptability ensures the stability and consistency of the generated keys, even in complex and fluctuating wireless environments.

Specifically, the combined method processes the real and imaginary parts of each subcarrier as multidimensional data. The autoencoder reduces the dimensionality of the data, simplifying its topology while retaining essential features. The reduced dimensional data are then input into the K-means clustering algorithm, which categorizes the data into four clusters. These clusters are subsequently encoded using Gray coding, further enhancing the KGR by reducing bit errors. The detailed workflow is illustrated in Fig. 5.

This AE-K-means clustering was chosen because it balances computational efficiency, accuracy, and adaptability, making it particularly effective for physical layer key generation in dynamic wireless communication scenarios. The quantization steps are as follows:

① Suppose that the overall channel estimates obtained by both Alice and Bob are H_{AB} and H_{BA}, as specified in Eqs (8) and (9). $R_{Norm}(h_i)$ and $I_{Norm}(h_i)$ indicate the real and imaginary part of the j-th channel

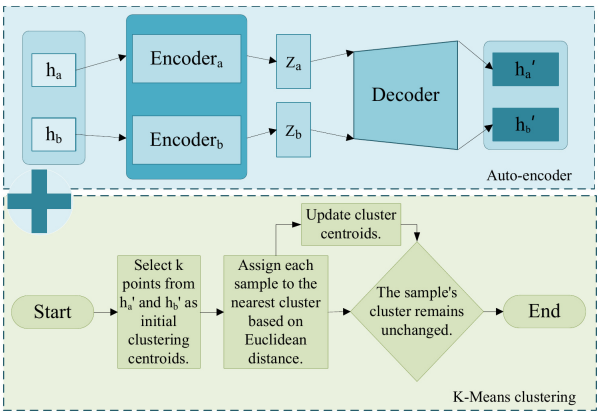

Fig. 5 Flowchart of the AE-K-means cluster quantization algorithm.

estimate, respectively; then, $\tilde{h}_{AB,i}$ and $\tilde{h}_{BA,i}$ can be expressed as: $\tilde{h}_{AB,i}$=$R_{Norm}(h_{AB,i})$+$I_{Norm}(h_{AB,i})i$, $\tilde{h}_{BA,i}$=$R_{Norm}(h_{BA,i})$+$I_{Norm}(h_{BA,i})i$.

② Normize the solid and imaginary parts of the overall channel estimates obtained by Alice and Bob to obtain:

$$\begin{aligned} R_{Norm} &= [R_{Norm}(h_1), R_{Norm}(h_2), \ldots, R_{Norm}(h_M)]^H \\ I_{Norm} &= [I_{Norm}(h_1), I_{Norm}(h_2), \ldots, I_{Norm}(h_M)]^H \end{aligned} \tag{10}$$

where $R_{Norm} = \frac{R_{Norm}(h_i)-minR_{Norm}(h_i)}{maxR_{Norm}(h_i)-minR_{Norm}(h_i)}$, $I_{Norm} = \frac{I_{Norm}(h_i)-minI_{Norm}(h_i)}{maxI_{Norm}(h_i)-minI_{Norm}(h_i)}$.

③ The autoencoder network was built using the matrix X=$[R_{Norm}((h_i), I_{Norm}((h_i)]$. The parameters for the autoencoder network are listed in Table 1.

Table 1 The parameter values for the autoencoder network

Parameter	Alice	Bob	Parameter meaning
Input_size	32	2	Input layer size
Encoding_size	1	1	Encode layer size
Epochs	100	100	Number of training iterations
Learning_rate	0.01	0.01	Learning rate

④ K-means clustering will be performed using the dimensionality reduction of the autoencoder network, where K=4. The traditional K-means clustering quantization method is shown in Fig. 6, and the autoencoder combined with K-means clustering quantization method is shown in Fig. 7. The four quantization intervals are divided by black lines.

⑤ A quantifiable initial key in the form of a Gray code encodes two adjacent categories into initial keys that differ by only one digit, that is,

$$K_i = \begin{cases} 00, i \in \text{cluster1} \\ 11, i \in \text{cluster2} \\ 10, i \in \text{cluster3} \\ 01, i \in \text{cluster4} \end{cases} \tag{11}$$

The AE-K-means clustering quantization method is contrasted with using only the K-means clustering quantization method. When encoding using Gray code, neighboring categories in the code sequence differ by only one digit, effectively minimizing the disagreement rate of the initial key.

Unedited

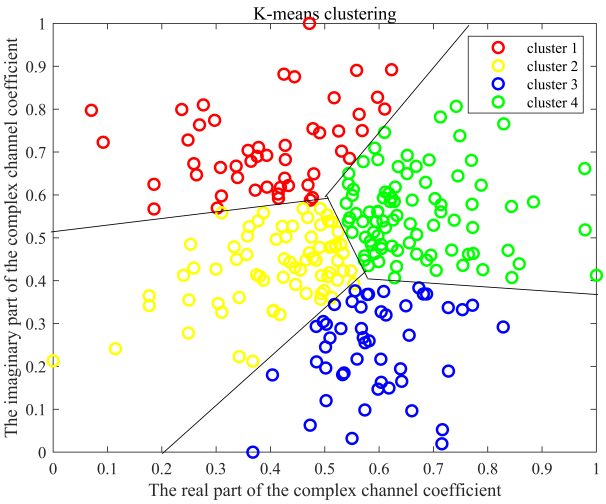

Fig. 6 K-means clustering quantization method

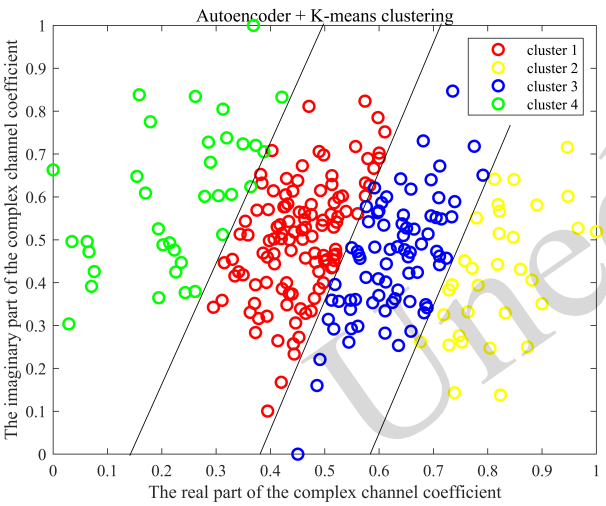

Fig. 7 Autoencoder combined with the K-means cluster quantization method

4.4 Information reconciliation

The information reconciliation scheme based on error correction coding described by Juels and Wattenberg (1999) is adopted; that is, Alice groups the quantified keys and generates coordination information based on error correction coding. Bob uses the error correction ability of error correction coding to correct errors and finally realizes the key consistency of both parties.

4.5 Privacy amplification

To enhance key security, this study will employ the privacy amplification method outlined by Aldaghri and Mahdavifar (2020) to generate a key hash value. The SHA256 (Secure Hash Algorithm 256-bit) function will be utilized for this purpose, followed by a verification process to ensure key consistency based on the generated hash value.

The specific algorithm is as follows:

Algorithm 1 AE-K-means quantization algorithm

Step 1: Initialize the following parameters:

$$d, d_0, d_v, C_0, SNR, M, N, l, \sigma^2$$

Step 2: Generate pilot signals X_{AB}, X_{BA} following Rayleigh distribution, and channel coefficients as:

$$h_{d,AB} \sim \mathcal{CN}(0,\sigma^2), \quad h_{RB} \sim \mathcal{CN}(0,\sigma^2), \quad H_{AR} \sim \mathcal{CN}(0,\sigma^2)$$

The reflection matrix Θ=diag$(\theta_1, \theta_2, \ldots, \theta_N)$ for RIS.

Step 3: Compute received signals at Bob and Alice:

$$y_{BA,i} = \left(h_{d,AB} + h_{RB}\Theta_i H_{AR}\right) X_{AB,i} + n_{BA,i}$$
$$Y_{AB,i} = w\left(h_{d,AB}^H + H_{AR}^H \Theta_i h_{RB}^H\right) x_{BA,i} + wn_{AB,i}$$

where $n_{AB} \sim \mathcal{CN}(0,\sigma^2)$, $n_{BA} \sim \mathcal{CN}(0,\sigma^2)$ are the noise terms.

Step 4: Apply min-max normalization to the received signals:

$$\hat{y}_{BA} = \frac{y_{BA} - \min(y_{BA})}{\max(y_{BA}) - \min(y_{BA})},$$
$$\hat{Y}_{AB} = \frac{Y_{AB} - \min(Y_{AB})}{\max(Y_{AB}) - \min(Y_{AB})}$$

Then, train an autoencoder to encode and decode $\hat{y}_{BA}$ and $\hat{Y}_{AB}$.

Step 5: Apply K-means clustering to the autoencoder's output:

$$\mathcal{C}_A = \text{K-means}(\hat{y}_{BA}, 4), \quad \mathcal{C}_B = \text{K-means}(\hat{Y}_{AB}, 4)$$

Step 6: Perform Gray encoding on the clustered outputs to obtain bit strings:

$$K_A = \text{Gray}(\mathcal{C}_A), \quad K_B = \text{Gray}(\mathcal{C}_B)$$

Step 7: Compute the KGR and KDR:

$$KGR = \lim_{\triangle \to 0} \frac{I(\tilde{H}_{AB}; \tilde{H}_{BA} | \tilde{H}_E)}{T}$$
$$KDR = \frac{\sum_{i=1}^{n} |K_A(i) - K_B(i)|}{M}$$

4.6 Computational complexity analysis

In this section, we analyze the computational complexity of the AE-K-means quantization algorithm, focusing on its efficiency and applicability to real-time applications.

The AE-K-means quantization algorithm combines the power of an autoencoder for feature extraction with K-means clustering for data quantization. The computational complexity of this approach can be broken down into the complexities of the AE and K-means processes, as well as their combined effect.

Unedited

4.6.1 AE complexity

The AE is a deep learning model used for learning efficient representations of input data. The complexity of the AE process can be described in terms of two main components:

①Encoding and Decoding Complexity: The encoder and decoder in the AE consist of several fully connected layers, with L layers and N neurons in each layer. The complexity of a forward pass through the encoder or decoder is proportional to $O(L \times N \times T)$, where T represents the number of training samples.

②Training Complexity: The AE model is trained using optimization techniques such as gradient descent. For each epoch, the training complexity is $O(L \times N \times T)$. Over E epochs, the total training complexity is $O(E \times L \times N \times T)$. However, training is typically performed offline, which reduces the real-time computational overhead. The trained model can be reused for key generation without any additional computational cost during real-time execution.

The AE process enables compact representation learning, and the training phase is conducted offline, ensuring minimal computational burden during real-time key generation.

4.6.2 K-means quantization complexity

K-means clustering is utilized in the quantization step of the AE-K-means algorithm. The complexity of the K-means algorithm can be broken down into two main steps:

①Cluster Assignment Complexity: For each data point, the distance to each of the k cluster centers must be computed. The complexity of this operation for a single data point is $O(k)$, and for N data points, the complexity becomes $O(k \times N)$.

②Cluster Update Complexity: After assigning the data points to the clusters, the cluster centers are updated. This update process also has a complexity of $O(k \times N)$.

The overall complexity for I iterations of K-means is then $O(I \times k \times N)$.

K-means is highly parallelizable and can be efficiently implemented in real-time systems. Using optimized techniques such as leveraging parallel computing resources like Graphics Processing Units (GPUs), K-means can be executed efficiently even with large datasets.

4.6.3 Combined complexity of AE-K-means quantization

The total complexity of the AE-K-means quantization algorithm is the sum of the AE training complexity and the K-means quantization complexity. Therefore, the overall complexity is:

$$O(E \times L \times N \times T) + O(I \times k \times N) \tag{12}$$

where E is the number of epochs for AE training, L is the number of layers, N is the number of neurons per layer, T is the number of training samples, I is the number of iterations for K-means, and k is the number of clusters.

While the AE training process requires significant computational resources, it is conducted offline, leaving only the encoding, decoding, and quantization steps to be performed in real-time. These steps are computationally efficient, ensuring that the algorithm is well-suited for real-time key generation.

4.6.4 Real-Time performance evaluation

The AE-K-means quantization algorithm is designed to meet the needs of real-time applications. During the key generation process, the AE model's trained weights are applied to generate encoded representations, followed by K-means clustering for quantization. The real-time key generation process involves minimal computational resources:

①Efficient Real-Time Performance: In real-time key generation, the AE model performs only the encoding and decoding steps, which are efficient. The K-means clustering step, involving both cluster assignment and center update, can be efficiently executed even with a large number of data points and clusters due to the parallelizability of the K-means algorithm and its optimizations.

②Optimization for Larger Systems: For systems with thousands of data points or large-scale RIS elements, additional optimization techniques such as hardware acceleration using GPUs can be applied to reduce computational time and maintain real-time performance.

In summary, the AE-K-means quantization algorithm provides a highly efficient solution for real-time physical layer key generation. While training the AE requires significant computational resources, the real-time key generation process is lightweight and efficient, making it an ideal choice for practical applications, even in large-scale and real-time environments.

Unedited

5 Simulation results and analysis

By comparing RIS-assisted key generation methods based on the AE-K-means quantization algorithm with traditional approaches, such as the K-means quantization algorithm and random source key generation, we validate the benefits of employing the AE-K-means quantization calculation in terms of KGR and randomness. The simulations were conducted on a computer with an Intel Core i5-10500 CPU, using MATLAB for numerical channel modeling. The specific experimental parameters are outlined in Table 2.

Table 2 Simulation parameter table

Project	Parameter	Value
Coherence time	Tc	0.001 s
Rayleigh factor	α	2
The quantity of antennas in Alice	M	2
The number of RIS cells	N	4
Pilot length	l	128 bit
Noise power	noise_power	0.1
The distance between Alice and the RIS	d_{AR}	50 m
The horizontal distance separating Bob and Alice	d_{AB}	50 m
Sampling frequency	f_s	20 MHz
Carrier frequency	f_c	5.25 GHz

RIS: Reconfigurable intelligent surfaces.

The simulations were conducted with a sampling frequency of 20 MHz, which ensures sufficient resolution for capturing the signal variations and channel characteristics. The carrier frequency was set to 5.25 GHz, which falls within the sub-6 GHz band commonly used in wireless communications. At this frequency, the propagation characteristics, including susceptibility to obstacles and reflection behavior, are well documented.

5.1 Performance comparison of the KGR

The KGR represents the proportion of key bits generated by each probe to the total number of channel features. A higher KGR indicates greater key generation efficiency, resulting in faster key generation and enhanced security of the communication system. According to Csiszar and Narayan (2000), the expression for the KGR is as follows:

$$KGR = \lim_{\triangle \to 0} \frac{I(H_{AB}; H_{BA}|H_E)}{T} \tag{13}$$

where $I(H_{AB}; H_{BA}|H_E)$ represents the mutual information shared between the base station Alice and the legitimate user Bob, given the information H_E of the eavesdropper Eve, and T represents the time of a single probe channel for key generation.

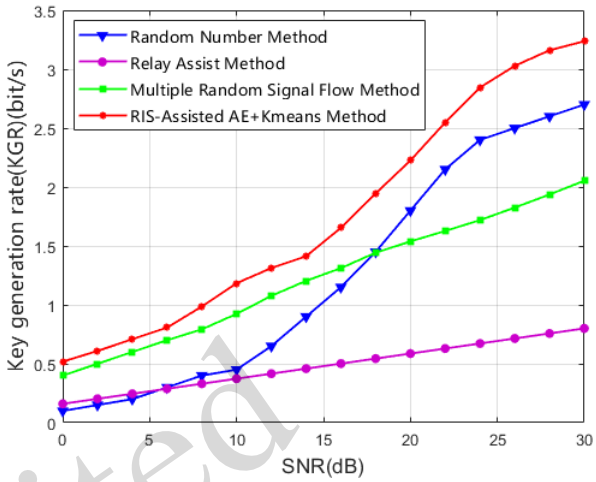

Fig. 8 The KGR performance versus different testing SNRs. KGR: Key generation rate; RIS: Reconfigurable intelligent surfaces; SNRs: Signal-to-noise ratios.

The proposed physical layer key generation scheme exhibits clear advantages when compared to existing schemes, as demonstrated in Fig.8. During the simulation experiment, the mutual information $I(H_{AB}; H_{BA}|H_E)$ is employed to quantify the KGR, with Eve generating the key in the same way as for the legal communication parties. Specifically, the relay-assisted method employs a strategy where the relay sends auxiliary information, which successfully improves the KGR by increasing the number of reciprocal channels in the shared random source. At the same time, the random signal flow method uses the sender to send independent random signal flow on multiple antennas and extracts the superimposed random signals on the receiving antenna as a shared random source. This facilitates the enhancement of the KGR by leveraging the randomness of the signal flow.

In contrast to the relay auxiliary method, the proposed approach utilizes the RIS to augment both the randomness and temporal variation of the channel, thereby increasing the number of channel estimations within the coherence time. Compared with the stochastic signal flow method, the RIS introduced by the proposed method has a considerable number of reflection units, each of which corresponds to a distinct reflection link, thus in-

Unedited

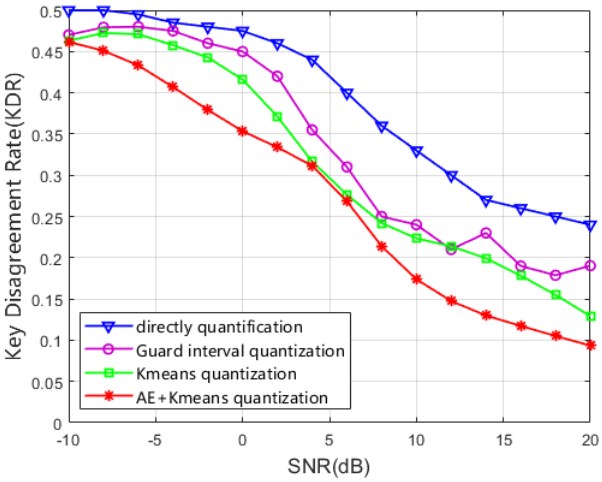

Fig. 9 The KDR performance versus different testing SNRs. KDR: Key disagreement rate; SNRs: Signal-to-noise ratios.

creasing the number of signal flow. Compared with the random number method, the shared random source of the proposed method consists of a large number of rapidly changing channels, and there is almost no leakage of key source information when the legitimate channel is unrelated is unrelated to the eavesdropping channel. Therefore, the proposed method can effectively improve the KGR.

5.2 KDR comparison

KDR quantifies the degree of mismatch in the keys generated by the legitimate communication parties. The lower the KDR, the fewer the interactions in the information coordination stage, resulting in a lower probability of leakage and a higher success rate for key generation. The formula for calculating the KDR is as follows:

$$KDR = \frac{\sum_{i=1}^{n} |N_{K_A}(i) - N_{K_B}(i)|}{M} \tag{14}$$

where N_{K_A} and N_{K_B} respectively represent the total quantity of keys generated at the Alice and Bob ends.

Fig.9 presents an analysis and comparison of the key disagreement trends for various classical quantization schemes. As illustrated in Fig. 9, it is clear that with an increase in SNR, the KDRs consistently decrease across all quantization schemes. Clearly, in scenarios with higher SNRs, the AE-K-means quantization demonstrates significantly lower KDRs compared to direct quantization schemes, protection interval quantization schemes, and traditional K-means methods. This observation can be attributed to the denoising and dimensionality reduction processes that the signal values undergo through the autoencoder network.

As a result, this significantly improves the reciprocity between base station Alice and legitimate user Bob. With the measured values at communication nodes continuously converging, the KDRs exhibit a more rapid decline under higher SNRs.

5.3 Scalability to large RIS configurations

In this section, we investigate the scalability of the proposed scheme to large-scale RIS configurations, focusing on how the number of RIS elements influences the KGR and KDR. The experiments were conducted with RIS element numbers ranging from 4 to 4000, and the results provide valuable insights into the trade-offs between performance and efficiency in larger configurations. The impact of RIS configuration size on both KGR and KDR was analyzed to understand how performance evolves as the number of RIS elements increases.

As shown in Fig. 10, the KGR initially increased as the number of RIS elements grew from 4 to 40, rising from 3.5 to 3.8. This improvement can be attributed to the enhanced channel randomness introduced by the additional RIS elements, which boosts the mutual information between the transmitter and receiver. Consequently, the initial increase in the number of RIS elements positively impacts the efficiency of key generation.

However, as the number of RIS elements exceeded 40, the KGR began to decline, eventually dropping to 0.25 for configurations with up to 4000 elements. One contributing factor is the computational overhead associated with optimizing the phase shift and precoding matrices, which increases significantly with the number of RIS elements. This higher complexity introduces delays and reduces the overall efficiency of the key generation process. Another factor is the diminishing marginal gain in channel randomness. Beyond a certain point, adding more RIS elements does not significantly enhance the channel randomness and may even introduce correlations between additional reflection paths, limiting the mutual information improvement and causing the KGR to plateau and decline.

Despite the reduction in KGR for large-scale RIS configurations, the KDR remained stable at approximately 0.14, even with up to 4000 RIS elements. This demonstrates the robustness of the proposed scheme in maintaining key consistency, ensuring reliable performance even as the system scales significantly.

Unedited

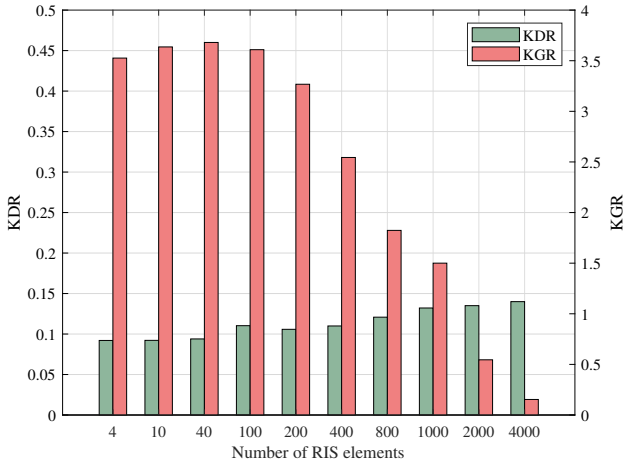

Fig. 10 KDR and KGR as the number of RIS elements increases. KDR: Key disagreement rate; KGR: Key generation rate; RIS: Reconfigurable intelligent surfaces.

5.4 Key randomness test

When detecting the randomness of the output sequence of the cryptographic algorithm, we usually use the hypothesis test method in statistics. The initial key output sequence is a binary sequence composed of 0 and 1, assuming that the sequence is random, which is called the null hypothesis or the null hypothesis (H_0). The alternative hypothesis (H_1) posits that the sequence is not random, in contrast to the null hypothesis. When testing, a statistic constructed on a known true random sequence conforms to a particular distribution. Through the null hypothesis, that is, it can be inferred that the sample statistics of this binary sequence should follow the corresponding specific distribution, which can be a uniform distribution, chi-square distribution, etc. Furthermore, in each test, there are two types of errors, as shown in Table 3.

With the fixed sample size, the probability of making these two types of errors is mutually restricted and cannot reduce them as much as possible simultaneously. The first type of error probability, known as the significance level and denoted by the symbol α, refers to the likelihood of incorrectly classifying a particular random sequence as a non-random sequence. Conversely, the second type of error probability, expressed by the symbol β, represents the probability of erroneously categorizing a random sequence as being non-random sequence.

Table 3 Statistics tests the probability of error

The overall situation results of the sample	Statistics calculation	Error probability
H_0 is true	Accept H_0	0
	Refuse H_0	α
H_1 is true	Accept H_0	β
	Refuse H_0	0

The randomness of the generated keys was assessed using the NIST SP 800-22 statistical test suite Rukhin (2001), which consists of 14 tests designed to detect various types of non-randomness in the key sequence. According to the test protocol, a key sequence is considered random with 99% confidence if the output probability (P-value) exceeds 0.01. The testing was conducted with a quasi-static channel coefficient algorithm under an SNR of 20 dB.

The initial keys generated by direct quantization, interval quantization, K-means quantization, and AE-K-means quantization are grouped into 256-bit segments and divided into 10,000 blocks for frequency test, block frequency test, cumulative sum test, run test, and others. The results are shown in Fig. 11. Specifically, the P-values for keys generated using the AE-K-means method were consistently the highest across all tests, suggesting superior randomness. In contrast, the other methods showed lower P-values, indicating the presence of non-random patterns in their generated keys. These results highlight that the AE-K-means method provides more robust randomness, making it a more reliable choice for physical layer key generation applications where key unpredictability is essential for ensuring security.

6 Conclusion

This paper addresses the issues of low KGR, high KDR, and poor key randomness in the quasi-static channel scenarios, caused by the low temporal variability of the channels. The secret key generation approach aided by RIS utilizes an AE-K-means quantization algorithm. By constructing a fast variable channel, the randomness and variability of the channel are increased. Compared to existing methods, our approach significantly improves the KGR and effectively reduces the KDR while ensuring superior key randomness. The key randomness is validated through the NIST SP 800-22 statistical test suite, where the AE-K-means method consistently shows higher P-values, indicating stronger randomness and reliability for physical layer key generation. In addition, we analyze the computational complexity and scalability of the method, demonstrating its efficient performance with larger RIS configurations. The method is particularly effective in the SNR range of 20–30 dB, balancing

Unedited

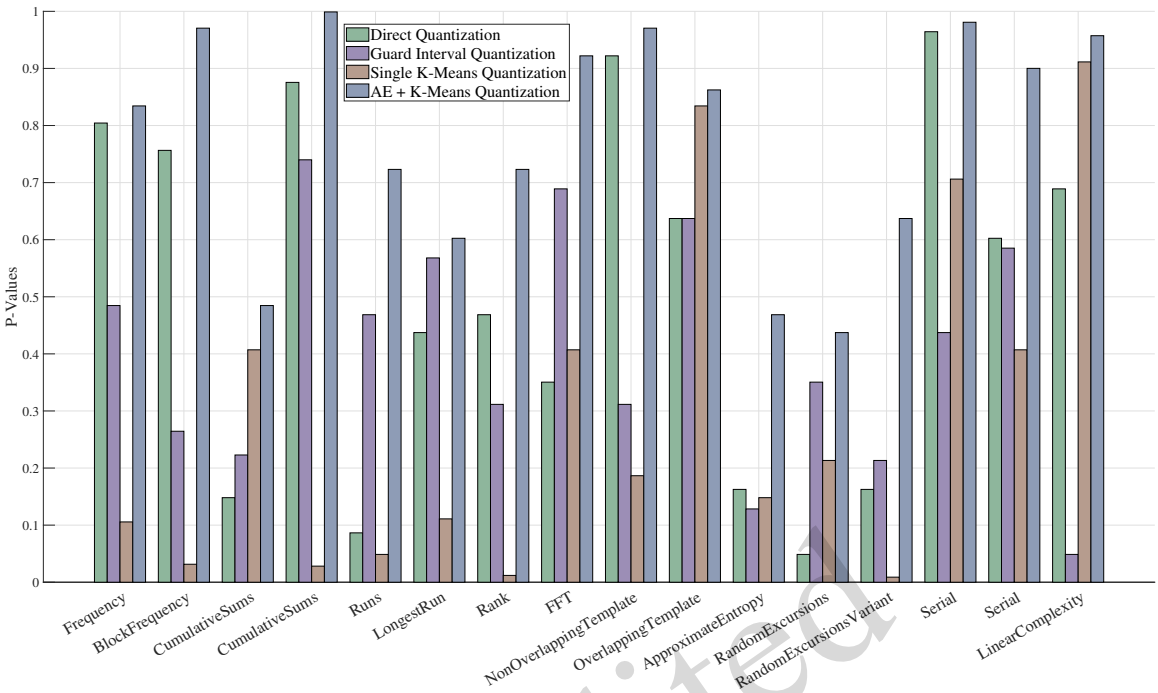

Fig. 11 NIST test results. NIST: National Institute of Standards and Technology; FFT: Fast fourier transform.

security and efficiency.

In conclusion, the proposed method outperforms existing schemes in terms of KGR, KDR, and key randomness, offering a robust and efficient solution for physical layer security in quasi-static environments.

Contributors

Zhenling LI and Qiangqiang GAO designed the research. Zhenling LI and Panpan XU conducted the experiments. Zhenling LI drafted the paper. Chunguo LI and Weijie Tan helped revise the paper. Weijie Tan supervised the project and finalized the paper.

Conflict of interest

All the authors declare that they have no conflict of interest.

References

Aldaghri N, Mahdavifar H, 2020. Physical layer secret key generation in static environments. *IEEE Transactions on Information Forensics and Security*, 15:2692-2705. https://doi.org/10.1109/TIFS.2020.2974621

Csiszar I, Narayan P, 2000. Common randomness and secret key generation with a helper. *IEEE Transactions on Information Theory*, 46(2):344-366. https://doi.org/10.1109/18.825796

Han Q, Liu J, Shen Z, et al., 2020. Vector partitioning quantization utilizing k-means clustering for physical layer secret key generation. *Information Sciences*, 512:137-160. https://doi.org/10.1016/j.ins.2019.09.076

Hershey J, Hassan A, Yarlagadda R, 1995. Unconventional cryptographic keying variable management. *IEEE Transactions on Communications*, 43(1):3-6. https://doi.org/10.1109/26.385951

Ji Z, Yeoh PL, Zhang D, et al., 2021. Secret key generation for intelligent reflecting surface assisted wireless communication networks. *IEEE Transactions on Vehicular Technology*, 70(1):1030-1034. https://doi.org/10.1109/TVT.2020.3045728

Juels A, Wattenberg M, 1999. A fuzzy commitment scheme. Proceedings of the 6th ACM Conference on Computer and Communications Security, New York, NY, USA, p.28–36. https://doi.org/10.1145/319709.319714

Li G, Hu A, Zhang J, et al., 2017. Security analysis of a novel artificial randomness approach for fast key generation. GLOBECOM 2017 - 2017 IEEE Global Communications Conference, p.1-6. https://doi.org/10.1109/GLOCOM.2017.8254029

Liu Y, Draper SC, Sayeed AM, 2012. Exploiting channel diversity in secret key generation from multipath fading randomness. *IEEE Transactions on Information Forensics and Security*, 7(5):1484-1497. https://doi.org/10.1109/TIFS.2012.2206385

Lou Y, Jin L, Zhong Z, et al., 2017. Secret key generation scheme based on mimo received signal spaces. *Scientia Sinica Informationis*, 47(3):362-373. https://doi.org/10.1360/N112016-00001

Lu X, Lei J, Shi Y, et al., 2021. Intelligent reflecting surface assisted secret key generation. *IEEE Signal Processing Letters*, 28:1036-1040. https://doi.org/10.1109/LSP.2021.3061301

Unedited

Luo H, Garg N, Ratnarajah T, 2023. A channel frequency response-based secret key generation scheme in in-band full-duplex mimo-ofdm systems. *IEEE Journal on Selected Areas in Communications*, 41(9):2951-2965.
https://doi.org/10.1109/JSAC.2023.3287610

Mathur S, Trappe W, Mandayam N, et al., 2008. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, New York, NY, USA, p.128–139.
https://doi.org/10.1145/1409944.1409960

Rukhin A, 2001. A statistical test suite for random and pseudorandom number generators for cryptographic applications. *Booz-Allen and Hamilton Inc Mclean Va*, .

Shannon CE, 1949. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656-715.
https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

Shimizu T, Iwai H, Sasaoka H, 2011. Physical-layer secret key agreement in two-way wireless relaying systems. *IEEE Transactions on Information Forensics and Security*, 6(3):650-660.
https://doi.org/10.1109/TIFS.2011.2147314

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

Wang X, Zhu F, Huang C, et al., 2024a. Robust beamforming with gradient-based liquid neural network. *IEEE Wireless Communications Letters*, 13(11):3020-3024.
https://doi.org/10.1109/LWC.2024.3436576

Wang X, Zhu F, Zhou Q, et al., 2024b. Energy-efficient beamforming for riss-aided communications: Gradient based meta learning. ICC 2024 - IEEE International Conference on Communications, p.3464-3469.
https://doi.org/10.1109/ICC51166.2024.10622978

Wu Q, Zhang S, Zheng B, et al., 2021. Intelligent reflecting surface-aided wireless communications: A tutorial. *IEEE Transactions on Communications*, 69(5):3313-3351.
https://doi.org/10.1109/TCOMM.2021.3051897

Wu X, Peng Y, Hu C, et al., 2013. A secret key generation method based on csi in ofdm-fdd system. 2013 IEEE Globecom Workshops (GC Wkshps), p.1297-1302.
https://doi.org/10.1109/GLOCOMW.2013.6825173

Wyner AD, 1975. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355-1387.
https://doi.org/10.1002/j.1538-7305.1975.tb02040.x

Ye H, Gao F, Qian J, et al., 2020. Deep learning-based denoise network for csi feedback in fdd massive mimo systems. *IEEE Communications Letters*, 24(8):1742-1746.
https://doi.org/10.1109/LCOMM.2020.2989499

Yu P, Zhou F, Zhang X, et al., 2020. Deep learning-based resource allocation for 5g broadband tv service. *IEEE Transactions on Broadcasting*, 66(4):800-813.
https://doi.org/10.1109/TBC.2020.2968730

Zeng K, 2015. Physical layer key generation in wireless networks: challenges and opportunities. *IEEE Communications Magazine*, 53(6):33-39.
https://doi.org/10.1109/MCOM.2015.7120014

Zhou G, Pan C, Ren H, et al., 2020. Robust beamforming design for intelligent reflecting surface aided miso communication systems. *IEEE Wireless Communications Letters*, 9(10):1658-1662.
https://doi.org/10.1109/LWC.2020.3000490

Zhu F, Wang X, Huang C, et al., 2024. Robust beamforming for ris-aided communications: Gradient-based manifold meta learning. *IEEE Transactions on Wireless Communications*, 23(11):15945-15956.
https://doi.org/10.1109/TWC.2024.3435023

Unedited