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 an 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 Sept. 13, 2024; Revision accepted Dec. 17, 2024; Crosschecked July 17, 2025

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, we propose a novel reconfigurable intelligent surface (RIS)-aided secret key generation approach using an autoencoder and K-means quantization algorithm. The proposed method uses 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, thereby 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. Simulations demonstrate that, under various signal-to-noise ratios (SNRs), the proposed method performs excellently in terms of KGR and KDR. Furthermore, the randomness of the generated keys is validated through the National Institute of Standards and Technology (NIST) test suite.

Key words: Reconfigurable intelligent surface (RIS); Physical layer key generation; Quantization; Autoencoder
https://doi.org/10.1631/FITEE.2400799 **CLC number:** TN918.4

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 relies on electromagnetic waves, which are inherently exposed to potential eavesdropping and malicious interference. The openness 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 communications in dynamic and hostile environments.

Traditional cryptographic approaches, while effective, often rely on computational complexity to secure information. However, they may be insufficient 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

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (No. 62361010), 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

wireless channel to generate symmetric keys for encryption. One notable method, proposed by Mathur et al. (2008), capitalizes on the inherent properties of the wireless channel reciprocity, time-variability, and spatial decorrelation to generate highly secure and dynamic keys for data encryption.

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. Time-variability 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 positions.

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 smaller 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.

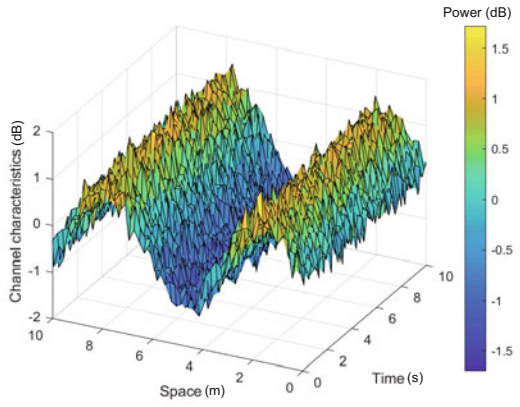

Fig. 1 Quasi-static scene in the time–space domain

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 QQ 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). Further work has shown that RIS-assisted reconfigurable antennas can effectively mitigate multipath fading and significantly enhance the KGRs in physical layer key generation systems (Wan et al., 2023).

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, we propose 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 secure method for key generation in quasi-static and dynamic environments. The specific contributions are outlined below:

1. Construction of a fast-varying channel: The reflection coefficients of RIS are 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.

2. Autoencoder and K-means (AE-K-means) quantization algorithm for key generation: First, the channel feature values are denoised and compressed through an AE, effectively preserving the essential structural characteristics of the data. Then, K-means clustering is applied to the compressed data, optimizing the quantization process and minimizing KDRs during encoding.

3. 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 is conducted. Furthermore, the randomness of generated keys is validated through rigorous testing using the National Institute of Standards and Technology (NIST) test suite.

2 Related works

In the early 20$^{\text{th}}$ 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 channel" 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 using 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 (Han et al., 2020; Luo et al., 2023). 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). In addition to enhancing randomness, large-scale RIS has also been explored for its ability to improve physical layer security by mitigating eavesdropping threats and jamming in near-field communications (Cui et al., 2024). 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., 2024a). 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 beamforming (GMLB) (Wang et al., 2024a) have been proposed. These methods use manifold learning and meta-learning techniques to optimize RIS parameters without requiring pre-training, 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, addressing the challenges of dynamic and highly variable channels by using differential equations-based liquid neurons to enhance robustness and efficiency (Wang et al., 2024b). 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. (2020) proposed a direct input deep neural network (DNN) for channel estimation, demonstrating superior performance over traditional methods. Yu et al. (2020) introduced CSINet, a deep learning-based channel state information (CSI) sensing and recovery mechanism, which uses compressed sensing to improve reciprocity in key generation. 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 been further employed to enhance channel characteristic prediction. Mathur et al. (2008) combined CNNs with GANs to improve downlink CSI prediction, thereby enhancing the accuracy of channel estimation and the key generation process. Fully connected neural networks have also been used to model channel mapping functions, improving the reciprocity of uplink and downlink channels (Wu XH 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 AE 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 the 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 offers two major advantages: (1) RIS enables us to customize the spatial and temporal properties of the channel, directly influencing key entropy; (2) Our method is applicable in static environments or scenarios 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 (Alice), a legitimate user (Bob), a passive eavesdropper (Eve), and the RIS itself. Time division duplexing (TDD) mode is employed for transmitting narrowband signals between Alice and Bob, ensuring channel reciprocity. Alice is outfitted with M transmit antennas, while Bob and Eve are equipped with a single antenna, separately. 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.

In this paper, the following three types of channels are considered: direct channel, indirect channel,

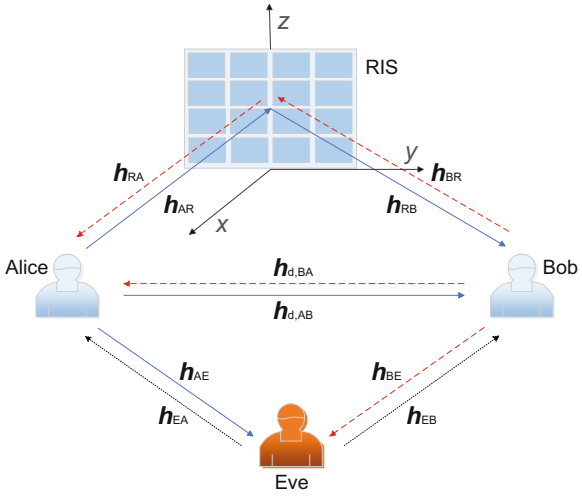

Fig. 2 System model for key generation based on RIS

and reflection channel (Zhou et al., 2020). The direct channel $\boldsymbol{h}_{\mathrm{d,AB}} = [\boldsymbol{h}_{\mathrm{d,AB},1},\ \boldsymbol{h}_{\mathrm{d,AB},2},\ \ldots,\ \boldsymbol{h}_{\mathrm{d,AB},M}]$ $\mathbb{C}^{1\times M}$ represents the link between Alice and Bob, while the indirect channel $\boldsymbol{H}_{\mathrm{AR}} = [h_{\mathrm{AR},1},\ h_{\mathrm{AR},2},\ \ldots,\ h_{\mathrm{AR},N}]^{\mathrm{T}} \in \mathbb{C}^{N\times M}$ pertains to the connection between Alice and the RIS. Here, each $\boldsymbol{h}_{\mathrm{AR},i} = [h_{\mathrm{AR},i,1},\ h_{\mathrm{AR},i,2},\ \ldots,\ h_{\mathrm{AR},i,M}] \in \mathbb{C}^{1\times M}$. The reflection channel $\boldsymbol{h}_{\mathrm{RB}} = [h_{\mathrm{RB},1},\ h_{\mathrm{RB},2},\ \ldots,\ h_{\mathrm{RB},N}] \in \mathbb{C}^{1\times N}$ denotes the path between the RIS and Bob. To simulate the actual channel environment, this section models the subchannel in the system model as a Rayleigh fading channel, expressed as

$$h = \sqrt{\frac{a}{1+a}}h^{\mathrm{LOS}} + \sqrt{\frac{1}{1+a}}h^{\mathrm{NLOS}}, \tag{1}$$

where h denotes the subchannel characteristics, a denotes the Rayleigh factor, and h^{LOS} and h^{NLOS} represent the line-of-sight (LOS) and non-line-of-sight (NLOS) Rayleigh fading components, respectively. Since the RIS is close to Alice, the size of the LOS component in the indirect channel depends on a, 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 a is set to 0. The channel follows a complex Gaussian distribution with a mean of 0. To further characterize the quasi-static scenario of the Internet of Things (IoT), all channels are modeled as block fading channels, remain constant over a longer coherence time, 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 the information transmission and key generation processes.

4 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 uses an AE-K-means quantization algorithm, including five steps: channel detection, pretreatment, quantization and encoding, information reconciliation, and privacy amplification. During the coherent time, the base station Alice conducts 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.

4.1 Construction of a fast-varying channel

As shown in Fig. 3, let $\boldsymbol{h}_{\mathrm{AB}} \in \mathbb{C}^{1\times M}$ represent the combined channel linking the base station Alice and the legitimate user Bob, with

$$\begin{aligned}\boldsymbol{h}_{\mathrm{AB}} &= \boldsymbol{h}_{\mathrm{d,AB}} + \boldsymbol{h}_{\mathrm{RB}}\boldsymbol{\Theta}\boldsymbol{h}_{\mathrm{AR}}\\ &= \boldsymbol{h}_{\mathrm{d,AB}} + \left[\sum_{i=1}^{N} h_{\mathrm{RB},i}\mathrm{e}^{\mathrm{j}\phi_i}h_{\mathrm{AR},i,1},\right.\\ &\quad \sum_{i=1}^{N} h_{\mathrm{RB},i}\mathrm{e}^{\mathrm{j}\phi_i}h_{\mathrm{AR},i,2},\ \ldots,\\ &\quad \left.\sum_{i=1}^{N} h_{\mathrm{RB},i}\mathrm{e}^{\mathrm{j}\phi_i}h_{\mathrm{AR},i,M}\right],\end{aligned} \tag{2}$$

where $\mathrm{j} = \sqrt{-1}$ denotes the imaginary unit, ϕ_i represents the phase shift introduced by the i^{th} ($i \in \{1,\ 2,\ \ldots,\ N\}$) reflection unit of the RIS, and $\boldsymbol{\Theta} = \mathrm{diag}(\boldsymbol{\theta}) \in \mathbb{C}^{N\times N}$ represents the reflection coefficient of the RIS, $\boldsymbol{\theta} = [\theta_1,\ \theta_2,\ \ldots,\ \theta_N]^{\mathrm{T}} \in \mathbb{C}^{N\times 1}$, $\theta_i \in \Phi$. Φ represents the value range of the reflection coefficient θ_i of the i^{th} reflection unit. Considering the discrete change of θ_i, Θ_i is as follows:

$$\Theta_i = \left\{\theta_i \mid \theta_i = \mathrm{e}^{\mathrm{j}\phi_i},\ \phi_i \in [0, 2\pi)\right\}. \tag{3}$$

Before each channel estimation, the base station Alice randomly updates the value of Θ_i and makes it independent of each other, thus greatly improving the time-variability and randomness of the channel

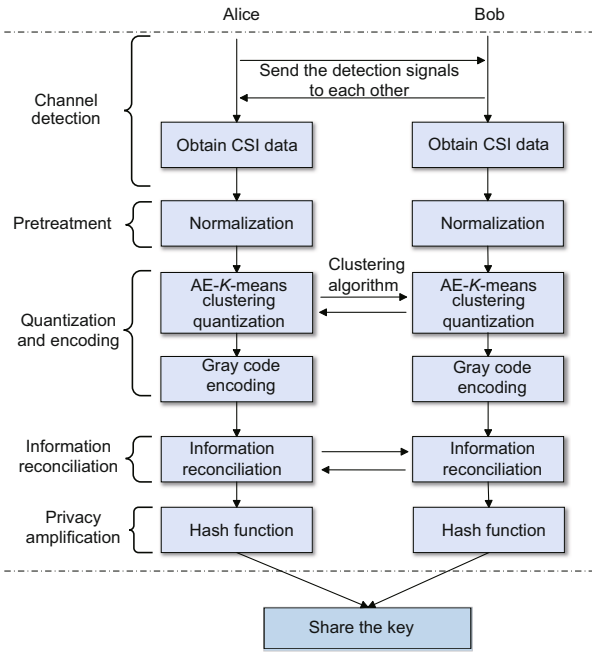

Fig. 3 Flowchart of key generation based on RIS

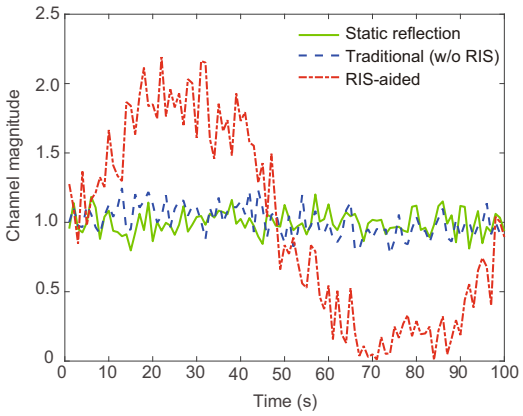

Fig. 4 Channel magnitude for different key generation methods (w/o: without)

estimates and constructing a fast-changing channel.

To validate the effect of dynamic adjustment of RIS reflection coefficients on channel fluctuation, we conduct comparative simulations. 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.

4.2 Channel detection

When the base station Alice controls the RIS to induce rapid phase changes, both Alice and the legitimate user Bob perform pilot-based channel estimation. This process can be repeated multiple times within the coherence time. Taking the i^{th} ($i \in \{1,2,\ldots,L\}$, L represents the number of channel estimates) channel estimate as an example, let $\boldsymbol{\Theta}_i$ and $h_{\text{AB},i}$ indicate the values of $\boldsymbol{\Theta}$ and $\boldsymbol{h}_{\text{AB}}$ at the i^{th} channel estimation, respectively. $\boldsymbol{X}_{\text{AB},i} \in \mathbb{C}^{M\times l}$ and $\boldsymbol{x}_{\text{BA},i} \in \mathbb{C}^{1\times l}$ represent the pilot information of length l transmitted during the i^{th} channel estimation, with $\boldsymbol{X}_{\text{AB},i}$ denoting the pilot from Alice to Bob, and $\boldsymbol{x}_{\text{BA},i}$ denoting the pilot from Bob to Alice. In this phase, Alice applies maximum ratio transmission (MRT) to her multi-antenna signal, adjusting the amplitude and phase of each antenna's transmission to ensure coherent addition and maximize signal power and quality at the receiver. Let $\boldsymbol{y}_{\text{BA},i} \in \mathbb{C}^{1\times l}$ and $\boldsymbol{Y}_{\text{AB},i} \in \mathbb{C}^{1\times l}$ represent the signals received by Bob and Alice, respectively, and the expression of the received signals is as follows:

$$\boldsymbol{y}_{\text{BA},i} = \left(\boldsymbol{h}_{\text{d,AB}} + \boldsymbol{h}_{\text{RB}}\boldsymbol{\Theta}_i\boldsymbol{h}_{\text{AR}}\right)\boldsymbol{X}_{\text{AB},i} + \boldsymbol{n}_{\text{BA},i}, \quad (4)$$

$$\boldsymbol{Y}_{\text{AB},i} = \boldsymbol{w}\left(\boldsymbol{h}_{\text{d,AB}}^{\text{T}} + \boldsymbol{h}_{\text{AR}}^{\text{T}}\boldsymbol{\Theta}_i\boldsymbol{h}_{\text{RB}}^{\text{T}}\right)\boldsymbol{x}_{\text{BA},i} + \boldsymbol{w}\boldsymbol{n}_{\text{AB},i}, \quad (5)$$

where $\boldsymbol{w} \in \mathbb{C}^{1\times M}$ denotes the MRT vector, and $\boldsymbol{n}_{\text{BA},i}$ and $\boldsymbol{n}_{\text{AB},i}$ represent the noise received by Alice and Bob during the i^{th} channel estimation, respectively. Using the forced zero algorithm, $\tilde{\boldsymbol{h}}_{\text{BA},i}$ and $\tilde{\boldsymbol{h}}_{\text{AB},i}$ represent the estimate of channel $\boldsymbol{h}_i$ by Bob and Alice, respectively, then

$$\begin{aligned}\tilde{\boldsymbol{h}}_{\text{BA},i} &= \frac{\boldsymbol{X}_{\text{AB},i}^{\text{T}}}{\|\boldsymbol{X}_{\text{AB},i}\|^2}\boldsymbol{y}_{\text{BA},i} \\ &= \boldsymbol{h}_{\text{d,AB},i} + \boldsymbol{h}_{\text{RB},i}\boldsymbol{\Theta}_i\boldsymbol{h}_{\text{AR},i} + \frac{\boldsymbol{X}_{\text{AB},i}^{\text{T}}}{\|\boldsymbol{X}_{\text{AB},i}\|^2}\boldsymbol{n}_{\text{BA},i},\end{aligned} \quad (6)$$

$$\begin{aligned}\tilde{\boldsymbol{h}}_{\text{AB},i} =& \frac{\boldsymbol{x}_{\text{BA},i}^{\text{T}}}{\|\boldsymbol{x}_{\text{BA},i}\|^2}\boldsymbol{Y}_{\text{AB},i} \\ =& \boldsymbol{w}^{\text{T}}\left(\boldsymbol{h}_{\text{d,AB},i}^{\text{T}} + \boldsymbol{h}_{\text{AR},i}^{\text{T}}\boldsymbol{\Theta}_i\boldsymbol{h}_{\text{RB},i}^{\text{T}}\right) \\ &+ \frac{\boldsymbol{x}_{\text{BA},i}^{\text{T}}}{\|\boldsymbol{x}_{\text{BA},i}\|^2}\boldsymbol{w}^{\text{T}}\boldsymbol{n}_{\text{AB},i}.\end{aligned} \quad (7)$$

Following multiple channel estimates, $\boldsymbol{H}_{\text{AB}}$ and $\boldsymbol{H}_{\text{BA}}$ denote the comprehensive channel estimates

obtained by Alice and Bob, respectively:

$$\boldsymbol{H}_{\mathrm{AB}}=[\tilde{\boldsymbol{h}}_{\mathrm{AB},1},\ \tilde{\boldsymbol{h}}_{\mathrm{AB},2},\ldots,\ \tilde{\boldsymbol{h}}_{\mathrm{AB},L}]^{\mathrm{T}}, \tag{8}$$

$$\boldsymbol{H}_{\mathrm{BA}}=[\tilde{\boldsymbol{h}}_{\mathrm{BA},1},\ \tilde{\boldsymbol{h}}_{\mathrm{BA},2},\ldots,\ \tilde{\boldsymbol{h}}_{\mathrm{BA},L}]^{\mathrm{T}}. \tag{9}$$

Due to the time-varying nature of the channel parameters $\boldsymbol{h}_{\mathrm{AR}}$ and $\boldsymbol{h}_{\mathrm{RB}}$ and the fact that the value of $\boldsymbol{\Theta}$ at each channel estimation is independent, the channel $\boldsymbol{h}_{\mathrm{AB}}$ is highly random and time-varying compared with $\boldsymbol{h}_{\mathrm{d,AB}}$, 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 computational efficiency and quantization accuracy, we integrate AE-K-means clustering into the quantization process. This combination leverages the strengths of both techniques to achieve optimal performance.

The AE efficiently compresses high-dimensional channel data into a lower-dimensional representation, significantly reducing data complexity while preserving the 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 the precision and reliability of the quantization process.

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

Specifically, the combination method processes the real and imaginary parts of each subcarrier as multidimensional data. The AE reduces the dimensionality of the data, simplifying its topology while retaining essential features. The dimensionality-reduced data are then input into the K-means quantization 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. The AE-K-means quantization algorithm 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 Alice and Bob are $\boldsymbol{H}_{\mathrm{AB}}$ and $\boldsymbol{H}_{\mathrm{BA}}$ respectively, as specified in Eqs. (8) and (9). $R_{\mathrm{Norm}}(\boldsymbol{h}_i)$ and $I_{\mathrm{Norm}}(\boldsymbol{h}_i)$ represent the normalized real and imaginary parts of the i^{th} channel estimate, respectively; then, $\tilde{\boldsymbol{h}}_{\mathrm{AB},i}$ and $\tilde{\boldsymbol{h}}_{\mathrm{BA},i}$ can be expressed as

$$\tilde{\boldsymbol{h}}_{\mathrm{AB},i}=R_{\mathrm{Norm}}(\boldsymbol{h}_{\mathrm{AB},i})+\mathrm{j}I_{\mathrm{Norm}}(\boldsymbol{h}_{\mathrm{AB},i}), \tag{10}$$

$$\tilde{\boldsymbol{h}}_{\mathrm{BA},i}=R_{\mathrm{Norm}}(\boldsymbol{h}_{\mathrm{BA},i})+\mathrm{j}I_{\mathrm{Norm}}(\boldsymbol{h}_{\mathrm{BA},i}). \tag{11}$$

2. Normalize the real and imaginary parts of the overall channel estimates to obtain

$$\boldsymbol{R}_{\mathrm{Norm}}=[R_{\mathrm{Norm}}(\boldsymbol{h}_1),\ R_{\mathrm{Norm}}(\boldsymbol{h}_2),\ \ldots,\ R_{\mathrm{Norm}}(\boldsymbol{h}_M)]^{\mathrm{T}}, \tag{12}$$

$$\boldsymbol{I}_{\mathrm{Norm}}=[I_{\mathrm{Norm}}(\boldsymbol{h}_1),\ I_{\mathrm{Norm}}(\boldsymbol{h}_2),\ \ldots,\ I_{\mathrm{Norm}}(\boldsymbol{h}_M)]^{\mathrm{T}}, \tag{13}$$

$$R_{\mathrm{Norm}}(\boldsymbol{h}_i)=\frac{R_{\mathrm{Norm}}(\boldsymbol{h}_i)-\min R_{\mathrm{Norm}}(\boldsymbol{h}_i)}{\max R_{\mathrm{Norm}}(\boldsymbol{h}_i)-\min R_{\mathrm{Norm}}(\boldsymbol{h}_i)}, \tag{14}$$

$$I_{\mathrm{Norm}}(\boldsymbol{h}_i)=\frac{I_{\mathrm{Norm}}(\boldsymbol{h}_i)-\min I_{\mathrm{Norm}}(\boldsymbol{h}_i)}{\max I_{\mathrm{Norm}}(\boldsymbol{h}_i)-\min I_{\mathrm{Norm}}(\boldsymbol{h}_i)}. \tag{15}$$

3. The AE network is built using the matrix $\boldsymbol{X}=[\boldsymbol{R}_{\mathrm{Norm}},\ \boldsymbol{I}_{\mathrm{Norm}}]$. The parameters for the AE network are listed in Table 1.

Table 1 Parameter values for the AE network

Parameter	Value	
	Alice	Bob
Input layer size	32	2
Encode layer size	1	1
Number of epochs	100	100
Learning rate	0.01	0.01

4. K-means clustering is performed using the dimensionality reduction of the AE network, where K=4. The traditional K-means quantization algorithm is shown in Fig. 6, and the AE combined with the K-means quantization algorithm is shown in Fig. 7. The four quantization intervals are divided

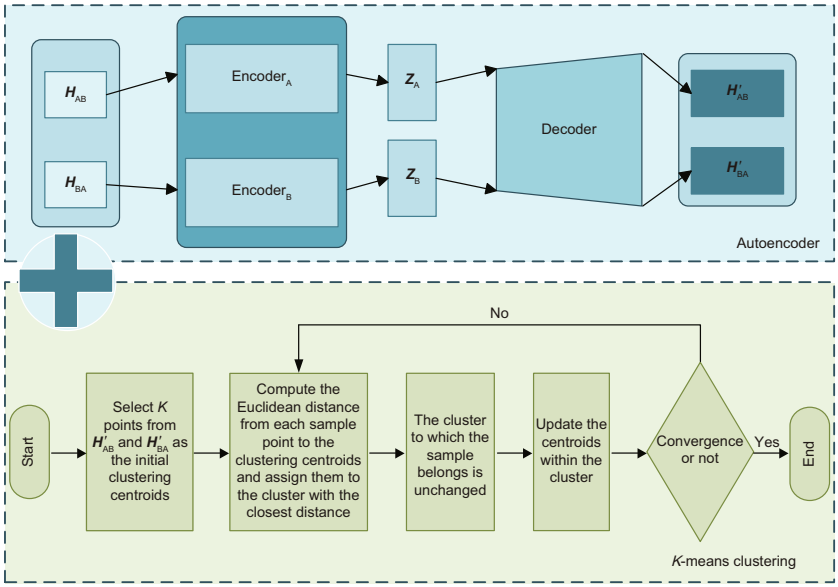

Fig. 5 Flowchart of the AE-K-means quantization algorithm

by black lines.

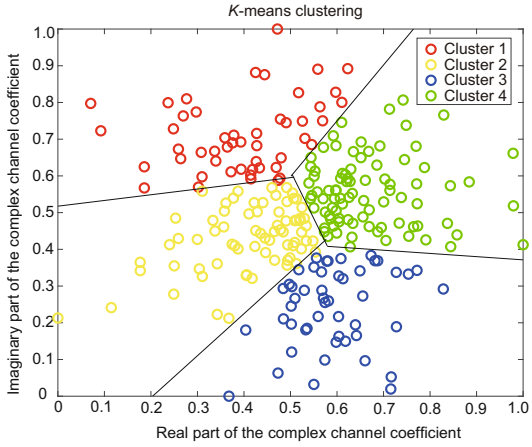

Fig. 6 Cluster results of the K-means quantization algorithm. References to color refer to the online version of this figure

5. A quantifiable initial key, represented as a Gray code, encodes two adjacent categories into initial keys that differ by only one digit, that is,

$$K_i = \begin{cases} 00, & i \in \text{Cluster 1}, \\ 11, & i \in \text{Cluster 2}, \\ 10, & i \in \text{Cluster 3}, \\ 01, & i \in \text{Cluster 4}. \end{cases} \tag{16}$$

The AE-K-means quantization algorithm is compared with the traditional K-means quantization algorithm. 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.

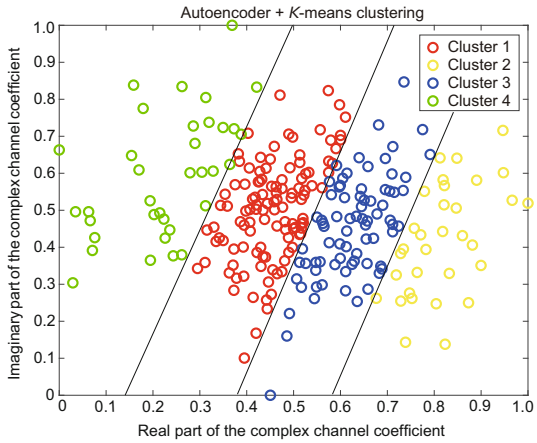

Fig. 7 Cluster results of the autoencoder combined with the K-means quantization algorithm. References to color refer to the online version of this figure

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 employs the privacy amplification method outlined by Aldaghri and Mahdavifar (2020) to generate a key hash value. The SHA256 (secure hash algorithm 256-bit) function is used for this purpose, followed by a verification process to ensure key consistency based on the generated hash value. The specific algorithm is illustrated in Algorithm 1.

4.6 Computational complexity analysis

In this subsection, 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 AE 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.

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:

1. Encoding and decoding complexity: The encoder and decoder in the AE consist of several fully connected layers, with F layers and G neurons per layer. The complexity of a forward pass through the encoder or decoder is proportional to $O(F \cdot G \cdot Q)$, where Q represents the number of training samples.

2. Training complexity: The AE model is trained using optimization techniques such as gradient descent. For each epoch, the training complexity is $O(F \cdot G \cdot Q)$. Over E epochs, the total training complexity is $O(E \cdot F \cdot G \cdot Q)$. 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 its training phase is conducted offline, ensuring minimal computational burden during real-time key generation.

Algorithm 1 AE-K-means quantization algorithm

1: Initialize the total distance between Alice and Bob d, the distance from Alice to RIS d_0, the distance from RIS to Bob d_{v}, the path loss constant C_0, SNR, the number of antennas at Alice and Bob M, the number of reflection units on the RIS N, the length of pilot sequence l, and the variance of the complex Gaussian noise σ^2.

2: Generate pilot signals $\boldsymbol{X}_{\mathrm{AB}} \in \mathbb{C}^{M\times l}$ and $\boldsymbol{x}_{\mathrm{BA}} \in \mathbb{C}^{1\times l}$ following Rayleigh distribution, and channel coefficients as

$$\boldsymbol{h}_{\mathrm{d,AB}} \sim \mathcal{CN}(0,\sigma^2), \boldsymbol{h}_{\mathrm{RB}} \sim \mathcal{CN}(0,\sigma^2),$$
$$\boldsymbol{h}_{\mathrm{AR}} \sim \mathcal{CN}(0,\sigma^2), \boldsymbol{n}_{\mathrm{AB}}, \boldsymbol{n}_{\mathrm{BA}} \sim \mathcal{CN}(0,\sigma^2).$$

The reflection matrix is given by $\boldsymbol{\Theta} = \mathrm{diag}(\theta_1, \theta_2, \ldots, \theta_N)$ for RIS.

3: Compute received signals at Bob and Alice:

$$\boldsymbol{y}_{\mathrm{BA},i} = \left(\boldsymbol{h}_{\mathrm{d,AB}} + \boldsymbol{h}_{\mathrm{RB}}\boldsymbol{\Theta}_i\boldsymbol{h}_{\mathrm{AR}}\right)\boldsymbol{X}_{\mathrm{AB},i} + \boldsymbol{n}_{\mathrm{BA},i},$$
$$\boldsymbol{Y}_{\mathrm{AB},i} = \boldsymbol{w}\left(\boldsymbol{h}_{\mathrm{d,AB}}^{\mathrm{T}} + \boldsymbol{h}_{\mathrm{AR}}^{\mathrm{T}}\boldsymbol{\Theta}_i\boldsymbol{h}_{\mathrm{RB}}^{\mathrm{T}}\right)\boldsymbol{x}_{\mathrm{BA},i} + \boldsymbol{w}\boldsymbol{n}_{\mathrm{AB},i}.$$

4: Apply min–max normalization to the received signals:

$$\hat{\boldsymbol{y}}_{\mathrm{BA}} = \frac{\boldsymbol{y}_{\mathrm{BA}} - \min(\boldsymbol{y}_{\mathrm{BA}})}{\max(\boldsymbol{y}_{\mathrm{BA}}) - \min(\boldsymbol{y}_{\mathrm{BA}})},$$
$$\hat{\boldsymbol{Y}}_{\mathrm{AB}} = \frac{\boldsymbol{Y}_{\mathrm{AB}} - \min(\boldsymbol{Y}_{\mathrm{AB}})}{\max(\boldsymbol{Y}_{\mathrm{AB}}) - \min(\boldsymbol{Y}_{\mathrm{AB}})}.$$

Then, train an AE to encode and decode the normalized signals $\hat{\boldsymbol{y}}_{\mathrm{BA}}$ and $\hat{\boldsymbol{Y}}_{\mathrm{AB}}$, respectively.

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

$$\mathcal{C}_{\mathrm{A}} = K\text{-means}(\hat{\boldsymbol{y}}_{\mathrm{BA}}, 4),\ \mathcal{C}_{\mathrm{B}} = K\text{-means}(\hat{\boldsymbol{Y}}_{\mathrm{AB}}, 4),$$

where $\mathcal{C}_{\mathrm{A}}$ and $\mathcal{C}_{\mathrm{B}}$ denote the clustering results at Alice and Bob, respectively.

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

$$K_{\mathrm{A}} = \mathrm{Gray}(\mathcal{C}_{\mathrm{A}}),\ K_{\mathrm{B}} = \mathrm{Gray}(\mathcal{C}_{\mathrm{B}}),$$

where K_{A} and K_{B} are the final binary key sequences at Alice and Bob, respectively.

7: Compute the KGR and KDR:

$$\mathrm{KGR} = \lim_{\Delta\to 0}\frac{I(\tilde{\boldsymbol{H}}_{\mathrm{AB}};\ \tilde{\boldsymbol{H}}_{\mathrm{BA}} \mid \tilde{\boldsymbol{H}}_{\mathrm{E}})}{T},$$
$$\mathrm{KDR} = \frac{\sum_{i=1}^{n}|N_{K_{\mathrm{A}}}(i) - N_{K_{\mathrm{B}}}(i)|}{W},$$

where $I(\tilde{\boldsymbol{H}}_{\mathrm{AB}};\ \tilde{\boldsymbol{H}}_{\mathrm{BA}} \mid \tilde{\boldsymbol{H}}_{\mathrm{E}})$ represents the conditional mutual information shared between Alice and Bob, given the channel information $\tilde{\boldsymbol{H}}_{\mathrm{E}}$ of Eve. T is the time duration of a single probing for channel-based key generation. $N_{K_{\mathrm{A}}}$ and $N_{K_{\mathrm{B}}}$ represent the total numbers of key bits generated at Alice and Bob, respectively. W represents the total number of key bits generated.

4.6.2 K-means quantization complexity

K-means clustering is used 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:

1. Cluster assignment complexity: For each data point, the distance to each of the K cluster centers must be computed. The complexity of this operation is $O(K)$ for a single data point and $O(K \cdot U)$ for U data points.

2. Cluster update complexity: After assigning the data points to the clusters, the cluster centers are updated. This update process also has a complexity of $O(K \cdot U)$.

Consequently, the overall complexity for P iterations of K-means is then $O(P \cdot K \cdot U)$.

The K-means algorithm is highly parallelizable and can be efficiently implemented in real-time systems. By leveraging parallel computing resources like graphics processing units (GPUs), K-means can be executed efficiently even on large datasets.

4.6.3 Combined complexity of the 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

$$O(E \cdot F \cdot G \cdot Q) + O(P \cdot K \cdot U). \tag{17}$$

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

1. High 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.

2. Scalability 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. Although 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.

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 AE-K-means quantization in terms of KGR and randomness. The simulations are conducted on a computer with an Intel Core i5-10500 central processing unit (CPU), using MATLAB for numerical channel modeling. The specific experimental parameters are detailed in Table 2.

Table 2 Simulation parameter setting

Parameter	Symbol	Value
Coherence time	T_c	0.001 s
Rayleigh scattering factor	α	2
Alice antenna quantity	M	2
Number of RIS reflection units	N	4
Pilot sequence length	l	128 bits
Noise power density	noise_power	0.1 W/Hz
Alice–RIS link distance	d_{AR}	50 m
Alice–Bob horizontal separation	d_{AB}	50 m
Sampling frequency	f_s	20 MHz
Carrier frequency	f_c	5.25 GHz

Simulations are conducted with a sampling frequency of 20 MHz, ensuring sufficient resolution to capture signal variations and channel characteristics.

The carrier frequency is set to 5.25 GHz, which falls within the sub-6 GHz band commonly used in wireless communications. At this frequency, 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:

$$\mathrm{KGR}=\lim_{\triangle\to 0}\frac{I(\tilde{\boldsymbol{H}}_{\mathrm{AB}};\ \tilde{\boldsymbol{H}}_{\mathrm{BA}}\mid\tilde{\boldsymbol{H}}_{\mathrm{E}})}{T}. \tag{18}$$

The proposed physical layer key generation scheme exhibits clear advantages over existing schemes, as demonstrated in Fig. 8. In our simulations, the conditional mutual information $I(\boldsymbol{H}_{\mathrm{AB}};\ \boldsymbol{H}_{\mathrm{BA}}|\boldsymbol{H}_{\mathrm{E}})$ is employed to quantify the KGR, with Eve generating the key in the same way as for the legitimate parties. Specifically, the relay-assisted method employs a strategy where the relay sends auxiliary information, successfully improving the KGR by increasing the number of reciprocal channels in the shared random source. Concurrently, the random signal flow method uses the transmitter to send independent random signal flows across multiple antennas and extracts the superimposed signals at the receiver as a shared random source.

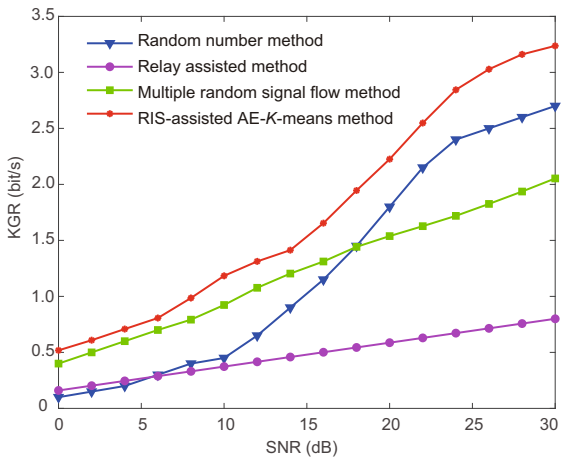

Fig. 8 KGR performance versus different testing SNRs

In contrast to the relay auxiliary method, the proposed method uses the RIS to enhance the randomness and temporal variation of the channel, thereby increasing the number of channel estimations within the coherence time. Compared to the random signal flow method, the RIS in the proposed method has a considerable number of reflection units, each establishing a distinct reflection link and thus increasing the number of signal flows. Furthermore, compared with the random number method, the shared random source in our 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 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 during 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:

$$\mathrm{KDR}=\frac{\sum_{i=1}^{n}|N_{K_{\mathrm{A}}}(i)-N_{K_{\mathrm{B}}}(i)|}{W}. \tag{19}$$

Fig. 9 presents an analysis and comparison of the key disagreement trends for various classical quantization schemes. As the SNR increases, 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 the direct quantization scheme, the protection interval quantization scheme, and the traditional K-means quantization algorithm. This observation can be attributed to the denoising and dimensionality reduction processes that the signal values undergo through the AE network.

As a result, the AE network 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.

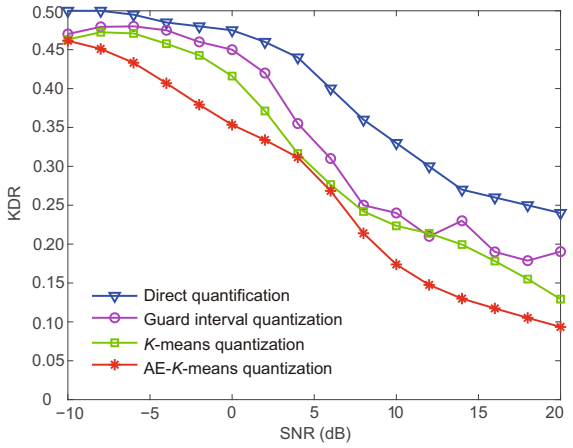

Fig. 9 KDR performance versus different testing SNRs

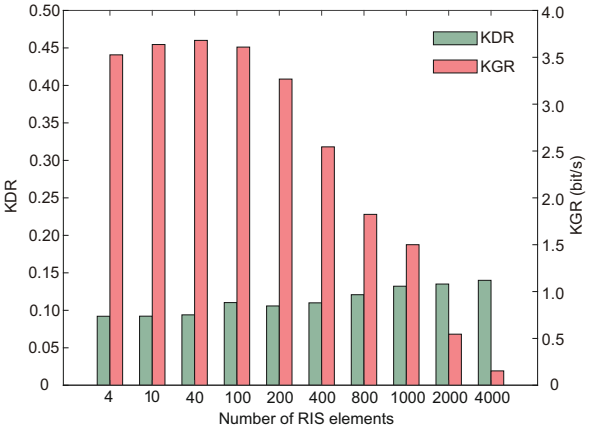

Fig. 10 Impact of RIS configuration size on KGR and KDR

5.3 Scalability to large RIS configurations

In this subsection, 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. Experiments are conducted with the number of RIS elements ranging from 4 to 4000, providing valuable insights into the trade-offs between performance and efficiency in larger configurations. The impact of RIS configuration size on KGR and KDR is analyzed to understand how performance evolves as the number of RIS elements increases.

As shown in Fig. 10, the KGR initially increases as the number of RIS elements grows from 4 to 40, rising from approximately 3.5 to 3.8 bits/s. 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 of the number of RIS elements positively impacts the efficiency of key generation.

However, as the number of RIS elements exceeds 40, the KGR begins to decline, eventually dropping to less than 0.25 bits/s for configurations with up to 4000 elements. One contributing factor is the computational overhead associated with optimizing the phase shifts 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 the 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 remains 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.

5.4 Key randomness test

To evaluate the randomness of a cryptographic algorithm's output sequence, statistical hypothesis testing is typically used. The initial key output sequence is a binary sequence composed of 0 s and 1 s. The null hypothesis (H_0) assumes that the sequence is random, and the alternative hypothesis (H_1) posits that the sequence is not random. Under the null hypothesis (H_0), the sample statistics of this binary sequence should follow a corresponding theoretical distribution, such as a uniform distribution or chi-square distribution, as would be observed with a truly random sequence. To accurately interpret the test results, it is necessary to understand the possible conclusions of the test and their associated risks. Furthermore, two types of errors can occur in hypothesis testing, as shown in Table 3.

For a fixed sample size, the probabilities of committing these two types of errors are mutually restricted and they cannot be reduced simultaneously. The first type of error probability, known as the

Table 3 Statistical tests for the error probability

Situation results of the sample	Statistical calculation	Error probability
H_0 is true	Accept H_0	0
	Refuse H_0	α
H_1 is true	Accept H_0	β
	Reject H_0	0

significance level and denoted by 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 symbol β, represents the probability of erroneously classifying a non-random sequence as a random sequence.

The randomness of the generated keys is assessed using the NIST SP 800-22 statistical test suite (Rukhin, 2010), which consists of 15 tests designed to detect various types of non-randomness in the key sequence. According to the test protocol, a key sequence is considered. According to the test protocol, a sequence is considered to pass a test (indicating no significant evidence of non-randomness) at the 1% significance level if the output probability (P-value) exceeds 0.01. The testing is conducted with a quasi-static channel coefficient algorithm under an SNR of 20 dB.

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, block frequency, and other tests. Results are shown in Fig. 11. Specifically, the P-values for keys generated using the AE-K-means quantization algorithm are consistently the highest across all tests, suggesting superior randomness. In contrast, the other algorithms show lower P-values, indicating the presence of non-random patterns in their generated keys. These results highlight that the AE-K-means quantization algorithm provides more robust randomness, making it a more reliable choice for physical layer key generation applications where high key unpredictability is essential for ensuring security.

6 Conclusions

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 channels. To overcome these issues, we propose a RIS-aided secret key generation scheme using 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 method significantly improves the KGR and effectively reduces the KDR while ensuring superior key randomness. The key randomness is validated using the NIST SP 800-22 statistical test suite, where the AE-K-means quantization algorithm consistently shows higher P-values, indicating stronger randomness and reliability for physical layer key generation. Furthermore, we analyze the computational complexity and scalability of the method, demonstrating its high performance with large-scale RIS configurations. The method is particularly effective within the SNR range of 20–30 dB, achieving a favorable balance between 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 conceived the study, designed the experiment, and drafted the paper. Panpan XU analyzed the experimental data and created visualizations. Qiangqiang GAO designed the experiments and conducted the experimental validation. Chunguo LI and Weijie TAN supervised the research, provided guidance, and revised the paper. Weijie TAN managed the project and secured funding.

Conflict of interest

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

Data availability

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

References

Aldaghri N, Mahdavifar H, 2020. Physical layer secret key generation in static environments. *IEEE Trans Inform Forens Sec*, 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 Trans Inform Theory*, 46(2):344-366. https://doi.org/10.1109/18.825796

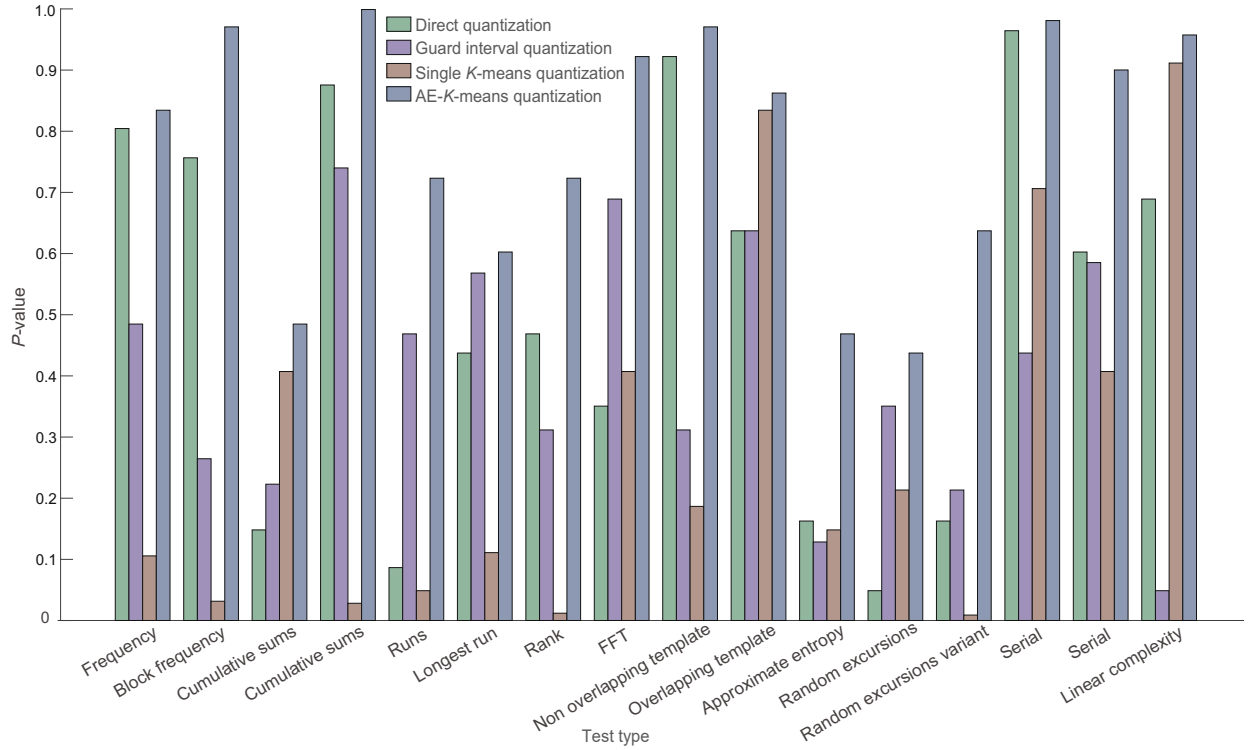

Fig. 11 Comparison of p-values in NIST randomness tests for four different quantization algorithms. Note that the Cumulative sums test is conducted in both forward and reverse directions, and the Serial test provides two statistics (for m-bit and $(m-1)$-bit patterns), hence two results are shown for each

Cui ZL, Liu J, Yang G, 2024. XL-RIS empowered near-field physical layer security against jamming and eavesdropping attacks. *Front Inform Technol Electron Eng*, 25(12): 1750-1758. https://doi.org/10.1631/FITEE.2400477

Han QQ, Liu JM, Shen ZW, et al., 2020. Vector partitioning quantization utilizing K-means clustering for physical layer secret key generation. *Inform Sci*, 512:137-160. https://doi.org/10.1016/j.ins.2019.09.076

Hershey JE, Hassan AA, Yarlagadda R, 1995. Unconventional cryptographic keying variable management. *IEEE Trans Commun*, 43(1):3-6. https://doi.org/10.1109/26.385951

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

Juels A, Wattenberg M, 1999. A fuzzy commitment scheme. Proc 6$^{\text{th}}$ ACM Conf on Computer and Communications Security, p.28-36. https://doi.org/10.1145/319709.319714

Li GY, Hu AQ, Zhang JQ, et al., 2017. Security analysis of a novel artificial randomness approach for fast key generation. Proc IEEE Conf on Global Communications, p.1-6. https://doi.org/10.1109/GLOCOM.2017.8254029

Liu YP, Draper SC, Sayeed AM, 2012. Exploiting channel diversity in secret key generation from multipath fading randomness. *IEEE Trans Inform Forens Sec*, 7(5):1484-1497. https://doi.org/10.1109/TIFS.2012.2206385

Lou YM, Jin L, Zhong Z, et al., 2017. Secret key generation scheme based on MIMO received signal spaces. *Sci Sin Inform*, 47(3):362-373. https://doi.org/10.1360/N112016-00001

Lu XJ, Lei J, Shi YX, et al., 2021. Intelligent reflection surface assisted secret key generation. *IEEE Signal Process Lett*, 28:1036-1040. https://doi.org/10.1109/LSP.2021.3061301

Luo HF, Garg N, Ratnarajah T, 2023. A channel frequency response-based secret key generation scheme in in-band full-duplex MIMO-OFDM systems. *IEEE J Sel Areas Commun*, 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. Proc 14$^{\text{th}}$ ACM Int Conf on Mobile Computing and Networking, p.128-139. https://doi.org/10.1145/1409944.1409960

Rukhin A, Soto J, Nechvatal J, et al., 2010. A statistical test suite for random and pseudorandom number generators for cryptographic applications (NIST SP 800-22 Rev. 1a). NIST, Gaithersburg, USA. https://doi.org/10.6028/NIST.SP.800-22r1a

Shannon CE, 1949. Communication theory of secrecy systems. *Bell Syst Tech J*, 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 Trans Inform Forens Sec*, 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 Wirel Commun*, 28(2):106-113. https://doi.org/10.1109/MWC.001.2000267

Wan Z, Yan MY, Huang KZ, et al., 2023. Pattern-reconfigurable antenna-assisted secret key generation from multipath fading channels. *Front Inform Technol Electron Eng*, 24(12):1803-1814. https://doi.org/10.1631/FITEE.2300126

Wang XQ, Zhu FH, Zhou QY, et al., 2024a. Energy-efficient beamforming for RISs-aided communications: gradient based meta learning. Proc IEEE Int Conf on Communications, p.3464-3469. https://doi.org/10.1109/ICC51166.2024.10622978

Wang XQ, Zhu FH, Huang CW, et al., 2024b. Robust beamforming with gradient-based liquid neural network. *IEEE Wirel Commun Lett*, 13(11):3020-3024. https://doi.org/10.1109/LWC.2024.3436576

Wu QQ, Zhang SW, Zheng BX, et al., 2021. Intelligent reflection surface-aided wireless communications: a tutorial. *IEEE Trans Commun*, 69(5):3313-3351. https://doi.org/10.1109/TCOMM.2021.3051897

Wu XH, Peng YX, Hu CJ, et al., 2013. A secret key generation method based on CSI in OFDM-FDD system. Proc IEEE Conf on Globecom Workshops, p.1297-1302. https://doi.org/10.1109/GLOCOMW.2013.6825173

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

Ye HY, Gao FF, Qian J, et al., 2020. Deep learning-based denoise network for CSI feedback in FDD massive MIMO systems. *IEEE Commun Lett*, 24(8):1742-1746. https://doi.org/10.1109/LCOMM.2020.2989499

Yu P, Zhou FQ, Zhang X, et al., 2020. Deep learning-based resource allocation for 5G broadband TV service. *IEEE Trans Broadcast*, 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 Commun Mag*, 53(6):33-39. https://doi.org/10.1109/MCOM.2015.7120014

Zhou G, Pan CH, Ren H, et al., 2020. Robust beamforming design for intelligent reflection surface aided MISO communication systems. *IEEE Wirel Commun Lett*, 9(10):1658-1662. https://doi.org/10.1109/LWC.2020.3000490

Zhu FH, Wang XQ, Huang CW, et al., 2024. Robust beamforming for RIS-aided communications: gradient-based manifold meta learning. *IEEE Trans Wirel Commun*, 23(11):15945-15956. https://doi.org/10.1109/TWC.2024.3435023