Zhenling LI, Panpan XU, Qiangqiang GAO, Chunguo LI, Weijie TAN, 2025. Reconfigurable intelligent surface-aided secret key generation using an autoencoder and *K*-means quantization. *Frontiers of Information Technology & Electronic Engineering*, 26(8):1486-1500. https://doi.org/10.1631/FITEE.2400799

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

Key words: Reconfigurable intelligent surface (RIS); Physical layer key generation; Quantization; Autoencoder

Weijie TAN
E-mail: wjtan@gzu.edu.cn
ORCID: Weijie TAN, https://orcid.org/0000-0001-6590-5757

Motivation

1. To address the challenge of invariant spatial and temporal channel characteristics in quasi-static wireless channel scenarios, which results in a high key disagreement rate (KDR) and low key generation rate (KGR).

2. To dynamically adjust the reflection coefficients of the RIS to create a rapidly fluctuating channel, enabling the extraction of dynamic channel parameters and thereby enhancing channel randomness.

3. To integrate the autoencoder with the *K*-means clustering quantization algorithm for efficiently extracting random bits from complex, ambiguous, and high-dimensional channel parameters, significantly reducing KDR.

Main idea

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.

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 evaluations of KGR and KDR under different SNR conditions are conducted.

System model

1. The key generation system model based on RIS, as depicted in Fig. 1, consists of a base station (Alice), a legitimate user (Bob), a passive eavesdropper (Eve), and the RIS itself.

2. Time division duplexing (TDD) mode is employed for transmitting narrow band signals between Alice and Bob, ensuring channel reciprocity.

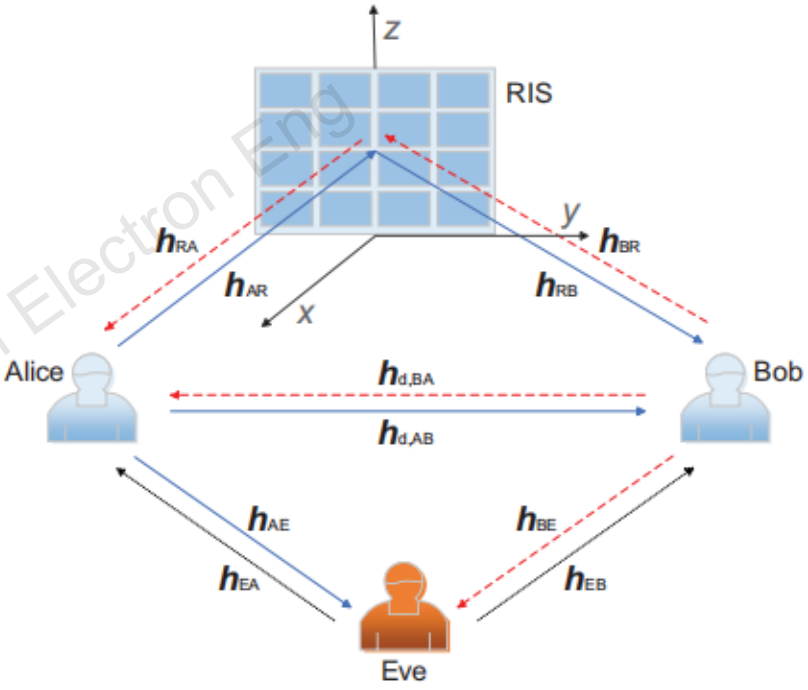


Fig. 1 System model for key generation based on RIS

Method

1. Construction of a fast-varying channel

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 estimates and constructing a fast-changing channel.

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.

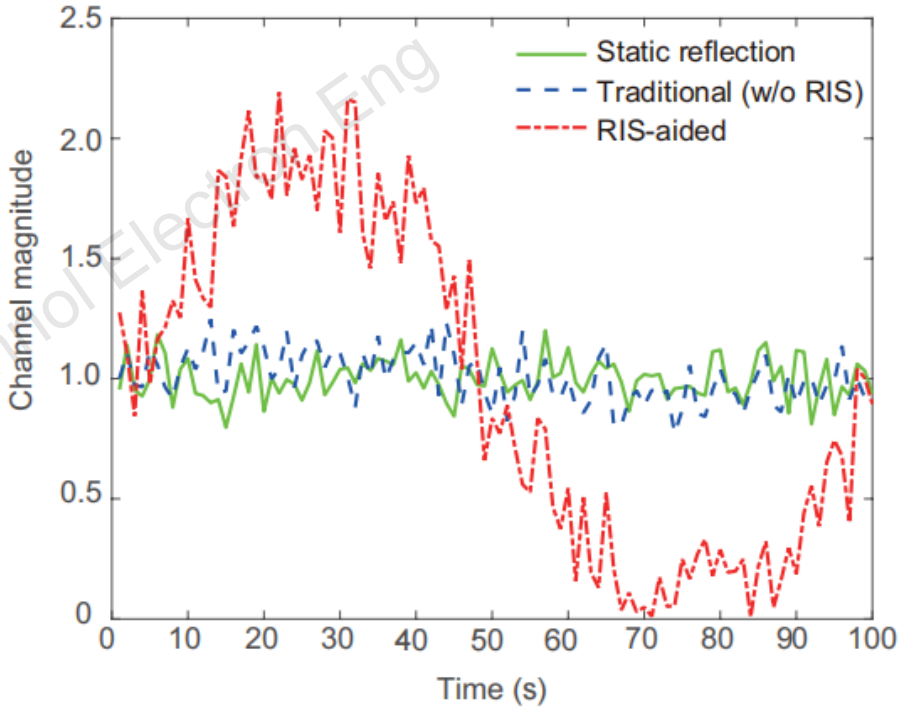


Fig. 2 Channel magnitude for different key generation methods (w/o: without)

Method (Cont'd)

3. Quantization algorithm based on AE-*K*-means clustering

The AE significantly reduces data complexity, ensuring that the essential channel characteristics required for key generation are retained. Subsequently, *K*-means clustering ensures the precision and reliability of the quantization process.

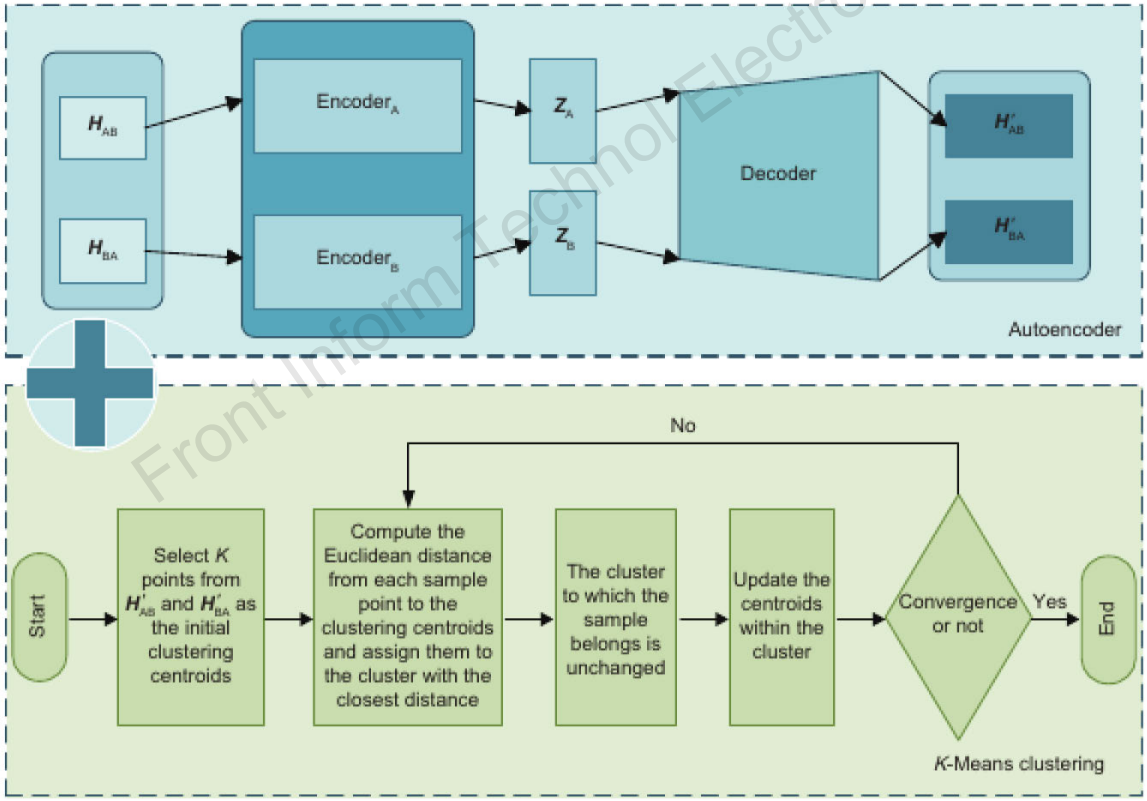


Fig. 3 Flowchart of the AE-*K*-means quantization algorithm

Method (Cont'd)

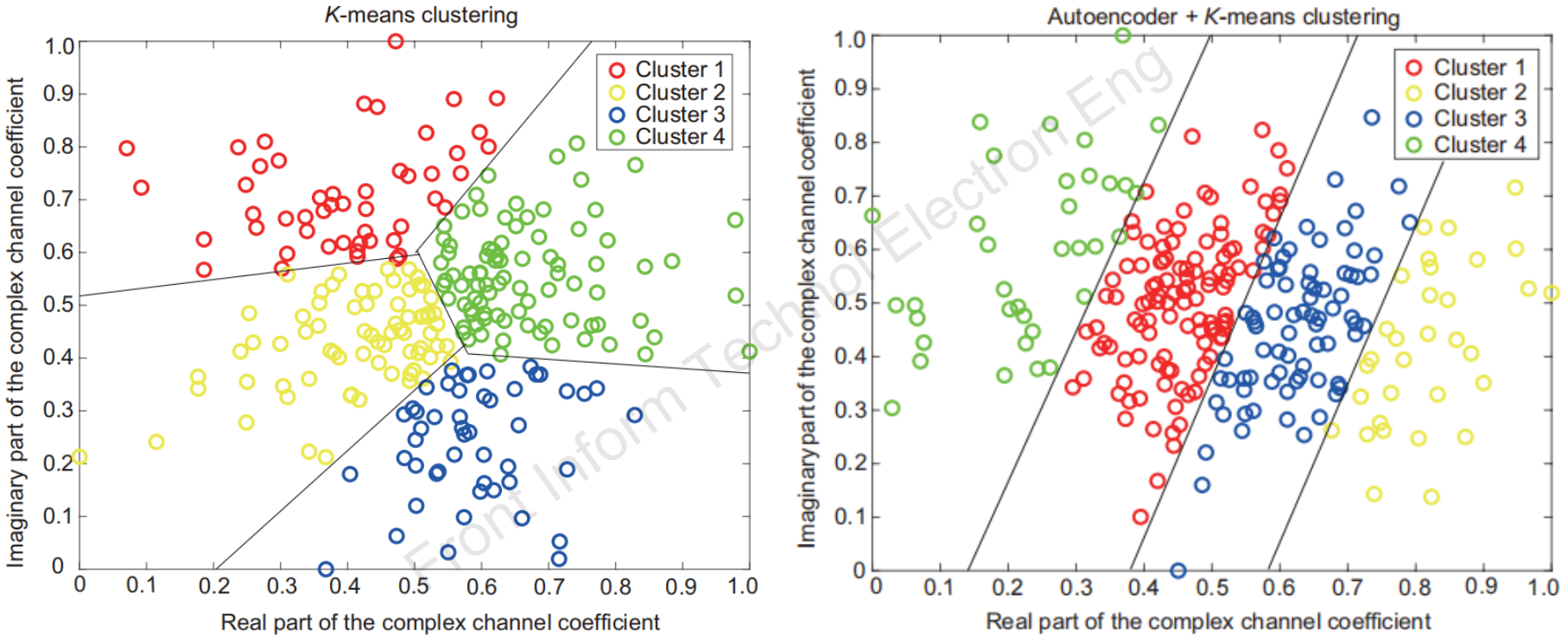


Fig. 4 Differences between the *K*-means quantization algorithm and the autoencoder combined with the *K*-means quantization algorithm

Major results

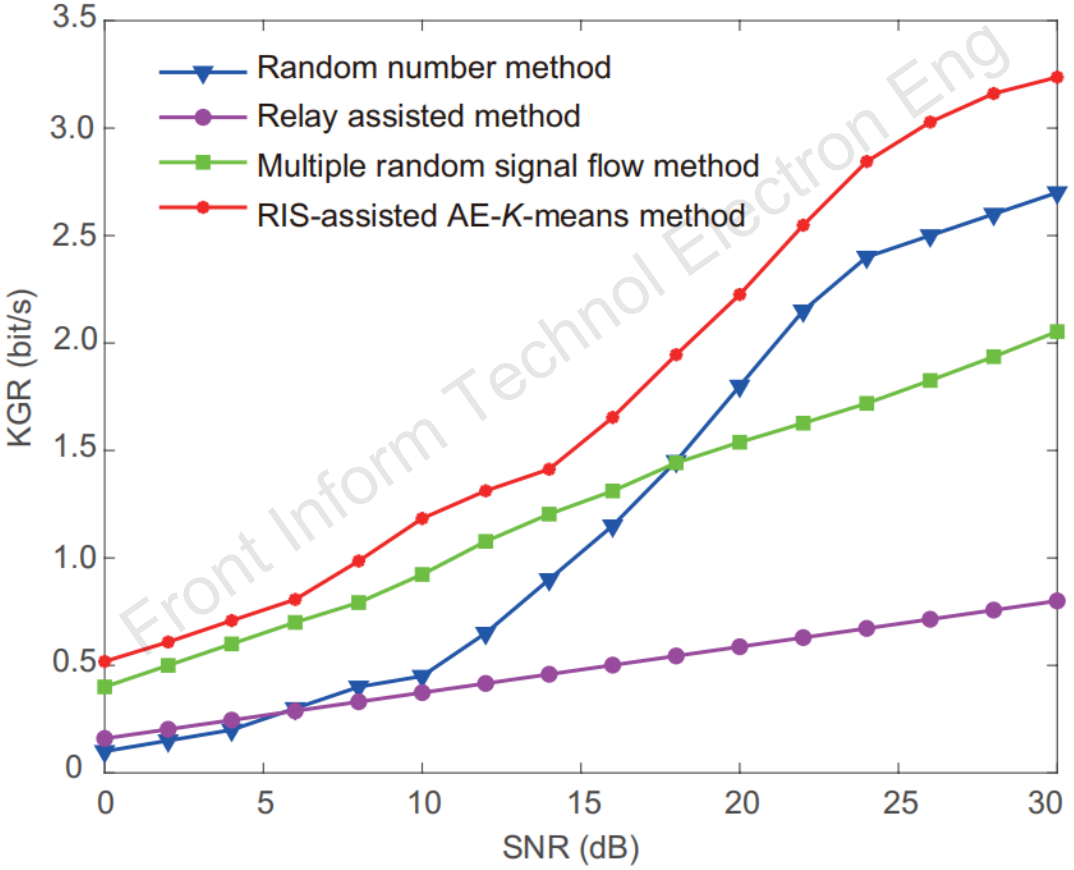


Fig. 5 KGR performance versus different testing SNRs

Major results (Cont'd)

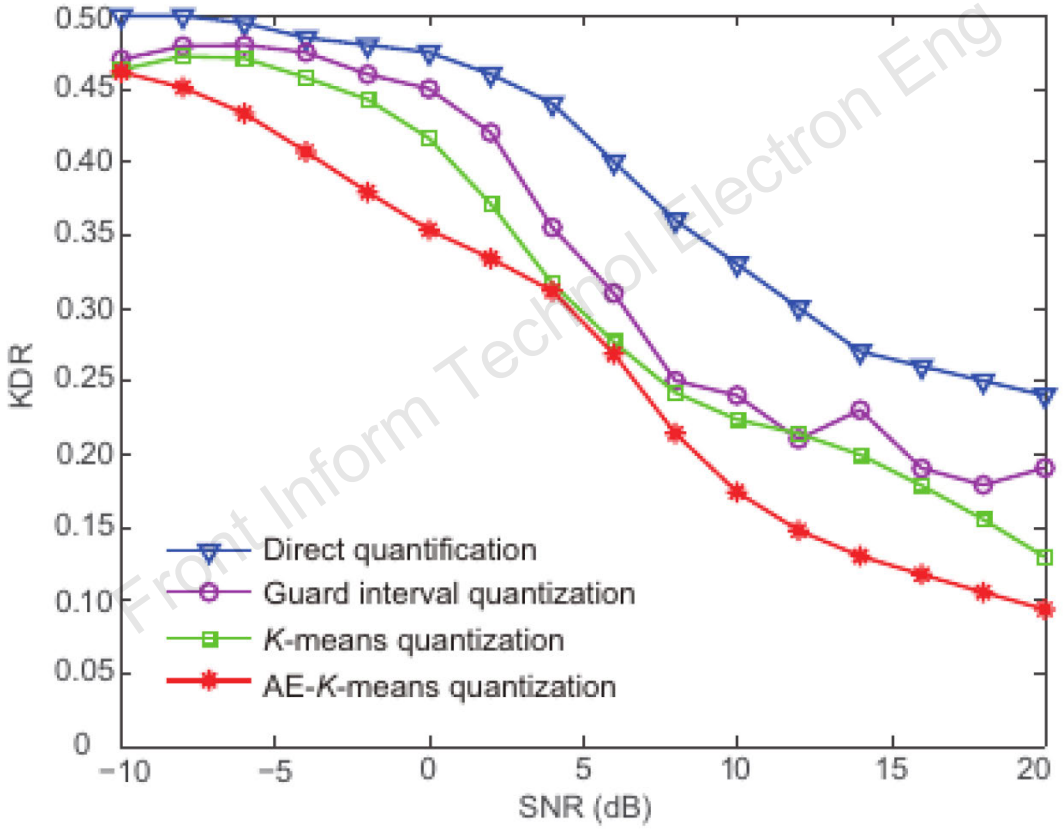


Fig. 6 KDR performance versus different testing SNRs

Major results (Cont'd)

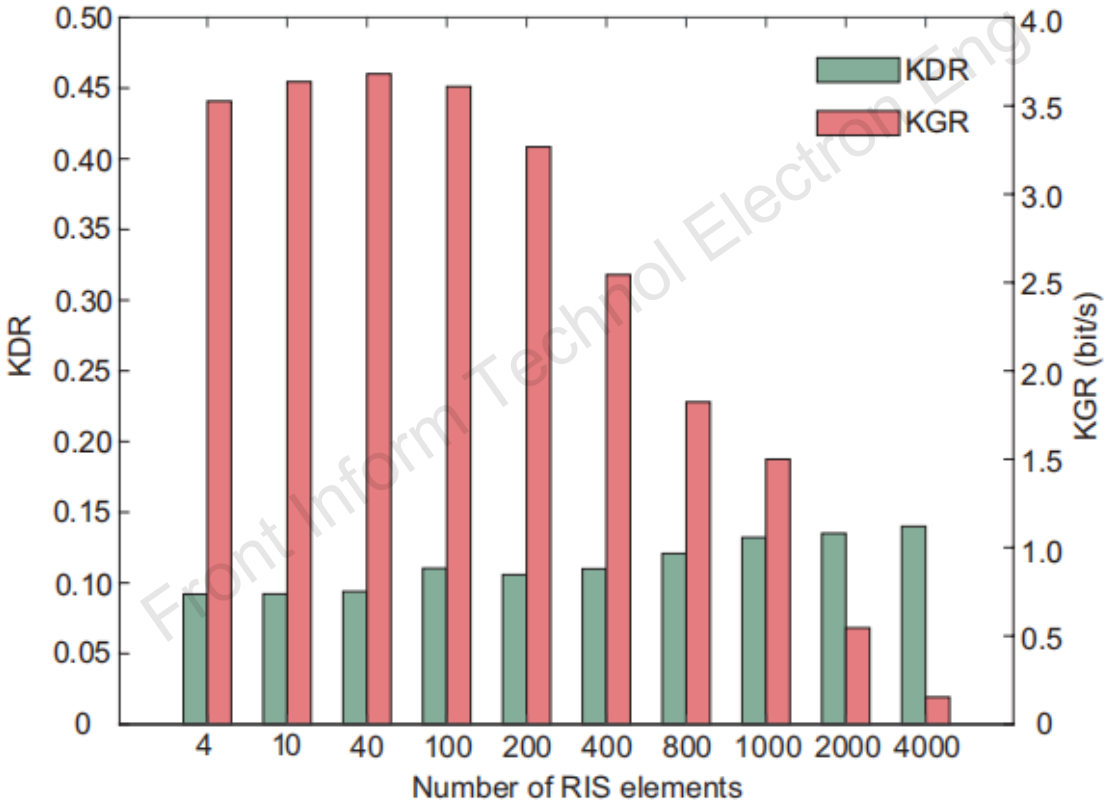


Fig. 7 Impact of RIS configuration size on KGR and KDR

Major results (Cont'd)

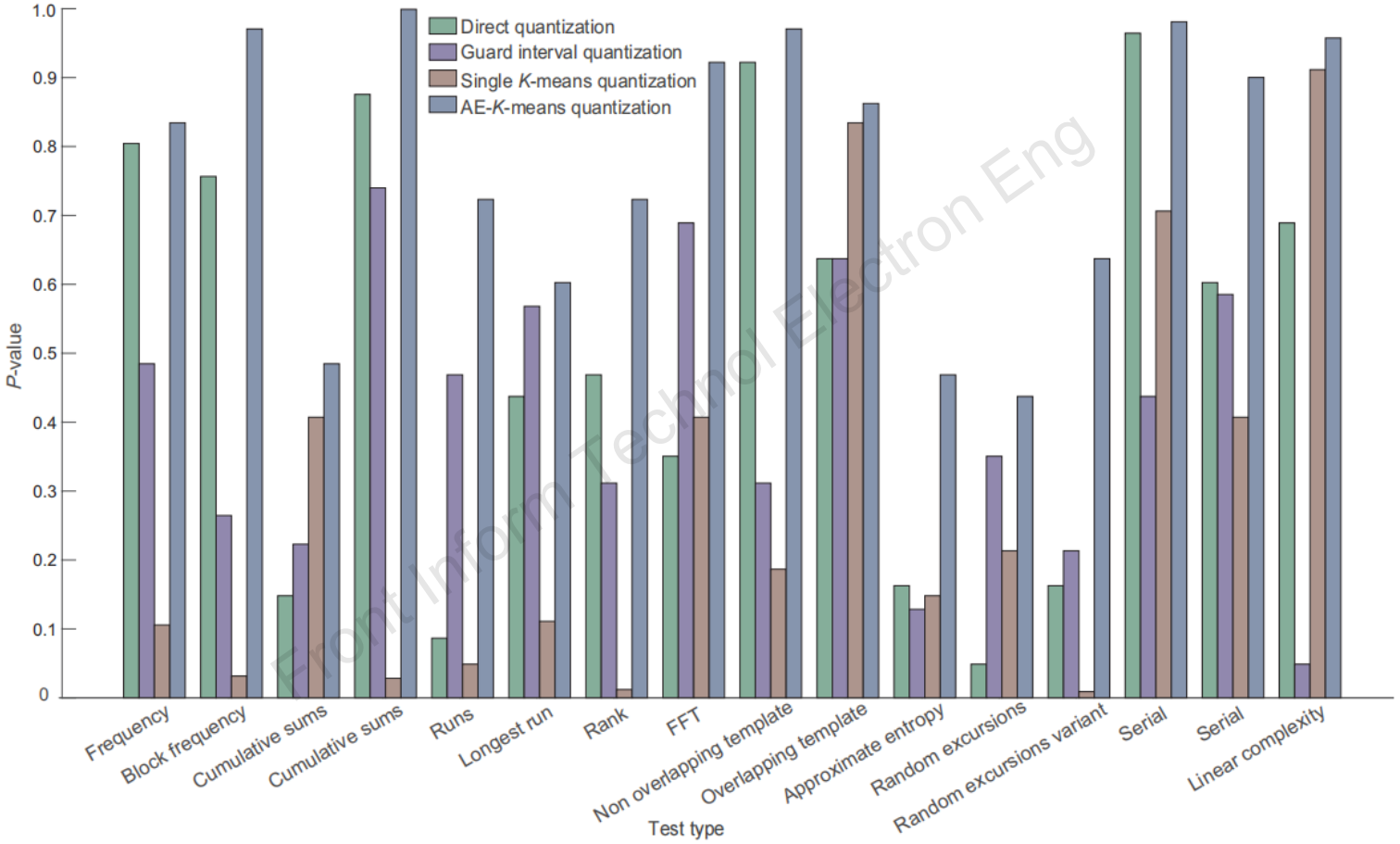


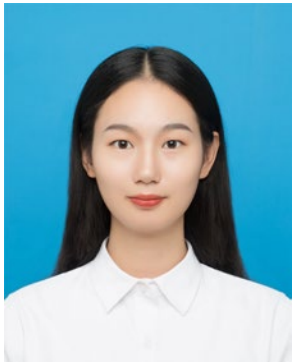
Fig. 8 Comparison of *p*-values in NIST randomness tests for four different quantization algorithms. Note that the cumulative sums test is conducted in both forward and reverse directions, and the serial test provides two statistics (*m*-bit and (*m*−1)-bit patterns); hence, two results are shown for each

Conclusions

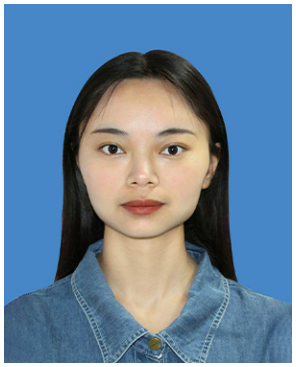
1. This paper addresses the issues of low KGR, high KDR, and poor key randomness in the quasi-static channel scenarios, caused by the low temporal variability of channels. To overcome these issues, we propose a RIS-aided secret key generation scheme using an AE-*K*-means quantization algorithm.

2.Compared to existing methods, our method significantly improves the KGR and effectively reduces the KDR while ensuring superior key randomness.

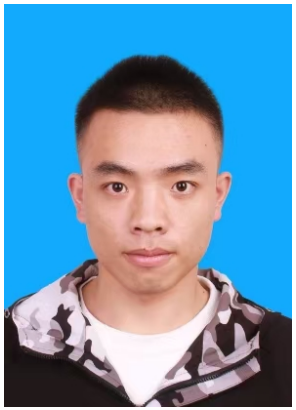
3.In conclusion, the proposed method outperforms existing schemes in terms of KGR, KDR, and key randomness, offering a robust and efficient solution for physical layer security in quasi-static environments.



Zhenling Li received the M.S. degree in applied statistics from the School of Mathematics and Statistics, Guizhou University. Her research interests include physical layer key generation, wireless network security, and physical layer security.



Panpan Xu received the M.S. degree in applied statistics from the School of Mathematics and Statistics, Guizhou University. Her research interests include physical layer security, secrecy capacity, and alternating optimization.



Qiangqiang Gao is currently pursuing an M.S. degree in electronic information from the School of Computer Science and Technology, Guizhou University, where he is also a member of the State Key Laboratory of Public Big Data. His research interests include key generation, information security, and cryptography.

Chunguo Li received the B.S. degree in wireless communications from Shandong University, China, in 2005, and the Ph.D.degree in wireless communications from Southeast University, Nanjing, China, in 2010. He is a fellow of the IET and the China Institute of Communications (CIC). He also serves as the Chair of IEEE Computational Intelligence Society Nanjing Chapter and the Advisory Committee for Instruments Industry, Jiangsu Province. His research interests include 6G cell-free distributed MIMO wireless communications and AI-based image signal processing.

Weijie Tan received the M.S. degree in communication and information system from the Communication University of China, Beijing, China, in 2011, and the Ph.D. degree in information and communications engineering from Northwestern Polytechnical University, Xi'an, China, in 2019. From 2016 to 2017, he was a visiting researcher with the Audio Analysis Laboratory, Aalborg University, Denmark. He is currently with the faculty of the State Key Laboratory of Public Big Data, Guizhou University. His research interests include communication signal processing and network and information security.