Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 6
ISET 2024

A Review of Challenges and Developments in Wireless Channel Key Generation Technology

Yu Zhang *

School of WenHua College, WuHan, China

* Corresponding Author Email: 986329310@qq.com

Abstracts. In recent years, physical layer security has become one of the core technologies for wireless communication system security. Physical layer encryption is based on the inherent reciprocity, time-varying, spatial uniqueness and unpredictability of wireless communication systems to generate keys, which are naturally unforgeable and steganography-proof. However, the research of physical layer key generation technology also faces many challenges, such as the problem of poor key generation performance due to signal interference, the problem of lower randomness and slower key generation rate in quasi-static channel environment, and the problem of lower key consistency between two legitimate communication parties due to the existence of channel estimation errors; this paper provides a systematic explanation of the traditional model of key generation for wireless channels and a typical solution for this series of problems. In this paper, the traditional model of wireless channel key generation is systematically explained, and the typical solutions to this series of problems are studied, analysed and compared in terms of performance.

Keywords: Wireless channel key generation; Quasi-stationary channel; anti-interference.

1. Introduction

Physical Layer Security (PLS) refers to the use of wireless channel characteristics and signal processing techniques to achieve security protection for wireless communication systems, including physical layer authentication and physical layer encryption. Physical Layer Security is one of the core technology solutions of 6G, in 6G network, Physical Layer Security technology will cooperate and be compatible with the upper layer security mechanism with cryptographic system as the core, and complement and support each other in the endogenous security system of 6G, and this thesis mainly focuses on the research in the field of Physical Layer Encryption.

Physical layer encryption is based on the inherent reciprocity, time-varying, spatial uniqueness and unpredictability of wireless communication systems to generate keys, which are naturally unforgeable and steganography-proof. The PLS algorithm, which generates keys based on wireless channel characteristics, originates from Shannon's information theory. In 1949, Shannon defined the perfect encryption model for the first time, and theoretically proved that the "One Time Pad (OTP)" can make the communication absolutely secure [1]. In 1993, Maurer [2], based on Shannon's private channel "Ome Time Pad", proposed a model for key extraction using correlated random sources and public authorised channels, which is called the source-based key generation model.Maurer elaborated on the key generation problem under non-authenticated negotiation channels, including completeness results, simulatability conditions and privacy amplification, which are the key generation problems under non-authenticated negotiation channels. simulatability conditions and privacy amplification, which is the first theoretical analysis on PLKG.In 1995 Hershey et al [3] used the public channel as a source of random signals, from which the legitimate parties can generate their own keys without transmitting information, and due to the time-varying nature of the wireless channel the communicating parties can update their keys frequently. Meanwhile, Hershey et al [3] proposed the first practical key generation protocol which consists of four basic phases: channel probing, quantisation, message negotiation and privacy amplification. By now, the research on wireless channel key generation technology has entered a heated phase, with many researchers showing great interest in it, and a variety of experimental and theoretical researches are being carried out extensively and intensively.

It can be applied to large-scale and lightweight communication scenarios, especially in emerging communication technologies such as Internet of Things (IoT) and 5G.

Most of the existing wireless channel key generation methods are studied in scenarios with good channel reciprocity, fast spatio-temporal variations and no signal interference. However, there are many more challenges in key generation in real situations.

1. Unknown signal interference, which leads to errors in channel estimation on both sides of the communication;

2. Encountering a quasi-static channel environment makes the rate, randomness of key generation reduced;

3. If the legitimate communicating parties have errors in channel estimation, this can lead to a lower key generation rate as well as a higher inconsistency rate.

In the subsequent chapters, Chapter 2 focuses on a more comprehensive introduction to the traditional model of wireless channel key generation; Chapter 3 provides a systematic introduction to typical methods of wireless channel key generation. Chapter 4 provides a comprehensive performance comparison analysis of the methods studied in the paper.

2. Wireless channel key generation model

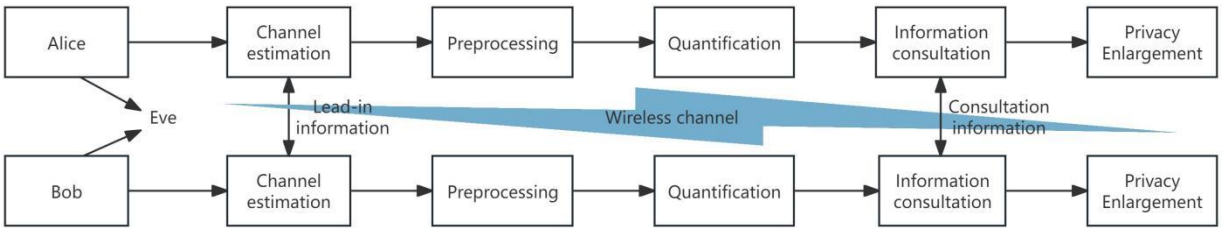


Figure 1. Wireless channel key system for TDD systems

According to Maurer et al. the physical layer key generation technique based on wireless channel characteristics is divided into five main stages which are channel estimation, preprocessing, quantisation, message negotiation and privacy amplification (Figure 1).

2.1. Channel estimation

In the channel probing phase, both parties will periodically send pre-designed probing signals, which can be known training sequences, guided frequency signals, or specially modulated signals, and the sent signals need to have good correlation in order to facilitate accurate channel estimation at the receiving end. The common channel characteristics from both single-antenna and multi-antenna key generation scenarios along with their advantages and disadvantages are listed below as shown in the Table 1.

Table 1. Enumeration of channel characteristics

take	channel characterisation	vantage	drawbacks
single antenna	RSS	Simple extraction and easy execution	Low key generation rate
	phase (waves)	Easy extraction with good randomisation	Lower key consistency
	envelope	Weak reflection of interference and noise and high key consistency	Low key generation rate
	CIR	More accurate channel information and high key generation rate can be obtained	Higher hardware requirements
multi-antenna	Virtual Arrival Corner virtual departure angle	High interoperability at low SNR and high key generation efficiency	Full CSI required
	Add the angle of arrival of the perturbation angle	High key generation rate and consistency, which can prevent eavesdropping to a certain extent.	Full CSI required

The receiver measures the characteristics of the wireless channel through the received probe signal, Received Signal Strength (RSS) [4], Channel Impulse Response (CIR) [5], Envelope [6], Phase [7], etc. RSS can be captured by the off-the-shelf wireless device The RSS can be collected by off-the-shelf wireless devices, and the process is simple, but the key generation rate is low. Literature [8] proposed a scheme to generate key based on RSS, which uses wireless network card to receive signal strength, and the feasibility of the scheme is verified in both stationary and mobile states, but RSS reflects the fuzzy channel information, which leads to a low key generation rate.CIR contains two kinds of information, phase and amplitude, so the key generation rate can be improved. Literature [5] based on CIR feature extraction for key generation, and proved that the key generated based on CIR has the ability to resist channel attacks. However, in practice, it is difficult to obtain accurate CIR and has high requirements on hardware devices. In addition, literature [6] proposes a feature extraction scheme using the signal reception envelope as a random source, using the characteristics of the envelope insensitive to noise and interference, the initial key generated is more consistent, but due to the slow transformation of the envelope leads to a slower key generation rate, so it is only applicable to special scenarios, such as ultra-wideband. In literature [9] for millimetre wave Massive MIMO communication system, the authors propose two new channel features namely virtual Angle of Arrival (virtual AoA) and angle of Departure (virtual AoD) as random sources for key generation. In addition, literature [10] utilises the angle of arrival with the addition of a random perturbation angle as a random source for feature extraction.

2.2. Pre-processing

In practice, the wireless communication system will receive the influence of non-reciprocity factors, in order to reduce the measurement error and the influence of channel noise, the receiver will be measured data preprocessing to eliminate the error of the two sides of the detection value, to improve the channel reciprocity. For example, when the period of channel detection is smaller than the channel coherence time, there will be redundancy between the detected channel samples, and then the pre-processing should be carried out to improve the reciprocity of channel samples between the two sides and reduce the correlation of their respective samples, so as to make the quantised key sequences more consistent and random. Common preprocessing schemes are Discrete Cosine Transform (DCT) [11] and Wavelet Transform (WT) [12]. Literature [13] applies the DCT transform to key generation, which improves the consistency of the quantitatively generated key by intercepting some of the measurements to attenuate the effect of channel noise. In literature [12] channel measurement samples are mapped to the WT domain and only the low frequency portion is used to build the key as a way to reduce the key mismatch rate.

2.3. Quantification

The quantisation stage transforms the processed continuous channel measurements into a discrete sequence of bits. Some of the existing channel feature quantisation methods and their characteristics are listed in the Table 2.

Table 2. Enumeration of quantitative methods

Existing methods	specificities
probabilistic quantification	The quantised sample values are evenly distributed in each quantisation interval so that the key sequences "0" and "1" are obtained with equal probability.
quantify evenly	Quantisation is done by dividing the quantisation intervals into equal intervals; as the number of quantisation bits increases, the rate of sequence inconsistency rises
Adaptive quantisation	Exploiting the independence of the quantised noise and the sequence, one side shares the quantised noise and the other side adaptively adjusts the quantisation thresholds
Quantification of k-mean clustering	Both sides are into the K-mean clustering partition respectively, and each region has the same value after quantisation, which can improve the consistency of the initial key by clustering first and then quantising.

In the existing research results, the purpose of equal probability quantisation[14] is to make the measured eigenvalues uniformly distributed in each quantisation interval, so that the probability of occurrence of "0" and "1" in the key sequence is the same. Although equal probability quantisation has the same probability of occurrence of "0" and "1" in the key sequence, each of its quantisation intervals may not necessarily be the same, while uniform quantisation[15] divides the quantisation intervals into equal intervals and ensures that the size of each interval is the same. Literature [16] proposes an adaptive quantisation method based on one side sharing the quantisation noise while the other side adaptively adjusts the quantisation intervals or thresholds. In addition, literature [17] proposes a quantisation method based on K-mean clustering partitioning, which improves the consistency of the initial key by clustering before quantisation.

2.4. Information consultation

In the message negotiation phase, the two parties exchange part of the bit information through the negotiation protocol to ensure the consistency of the bit sequence of the two parties, and at the same time to ensure the security of the exchanged information. 1993, Maurer[2] proposed a negotiation method based on the "dichotomous method" for error checking of the quantised key, checking the location of inconsistency bits and correcting the error, but only one bit can be corrected at a time. In 1993, Maurer[2] proposed a negotiation method based on "dichotomy" for error checking of quantised generated keys, which checks the position of inconsistent bits in the key bit string and corrects the error, but only one bit can be corrected at a time, for this reason, the Cascade protocol is proposed in the literature [18], which can record the key bit information in the course of error correction, and has a stronger ability to correct the error.

2.5. Privacy amplification

The privacy amplification phase, in order to eliminate the information leakage caused by the information negotiation phase. Through privacy amplification, even if the eavesdropper Eve obtains part of the information after the message negotiation still can maintain a high degree of security. Currently, the most commonly used is to use the Hash function for key transformation of the key, using the unidirectionality of the Hash function to achieve the key security enhancement.[19]

3. Wireless channel response key generation key technology analysis

3.1. Technical challenges

There are many difficulties and technical challenges in practical applications. Firstly, in the process of key generation for legitimate communicators, the channel estimation of both legitimate communicators can be inaccurate due to unknown signal interference, which reduces the key generation rate. Second, in the quasi-stationary channel environment, most of the communication devices are fixed or only slightly moving, which leads to very slow changes in the wireless channel or even remain unchanged for a long time, which results in a low key generation rate and a large number of repetitive bits between the generated keys, and the randomness of the key becomes poor, and the theoretical effect of "one secret at a time" can not be achieved in the practical use of the key. "This makes the key generation rate low and there will be a large number of repeated bits between the generated keys. Thirdly, in the channel estimation phase, the two legitimate communicating parties have errors in the estimation due to other reasons such as the strength of their own algorithms, which results in a high rate of inconsistency in key generation. To address these challenges, this chapter analyses some solutions in the light of current research.

3.2. Channel key generation algorithm against signal interference

Signal interference in the key generation process is an important issue, it will lead to errors in the channel estimation of the two communicating parties, thus affecting the accuracy and security of key generation, for the impact of interference signals on the key generation of the wireless channel, the literature [11][20] have respectively proposed the use of the use of Discrete Cosine Transform (DCT) preprocessing technique to reduce the effect of interference on the channel probe values. In order to resist the influence of signal interference on key generation, Dai's team constructed the DCT-LMS adaptive filtering algorithm based on the Least Mean Square (LMS) algorithm proposed by Widrow.

3.2.1. Key generation method based on DCT-LMS public guide frequency detection protocol

The literature "Application of Wireless Physical Layer Key Generation Technology in Research" combines the public guide frequency detection protocol with the adaptive filtering algorithm, and proposes a public guide frequency detection protocol based on DCT-LMS, which performs the DCT transform de-correlation process on the input interference-containing signal, and then processes it with the LMS adaptive filtering algorithm, which solves the effect of the interfering signals on the estimation results in the process of channel estimation, and improves the The estimation accuracy is improved. The specific steps include: firstly, inputting the received signals of Alice and Bob's main and auxiliary antennas, the step factor, the initialised filter coefficients, the initialised power, and the impulse response length of the filters; firstly, calculating the maximum number of iterations at the output stage, and then Alice and Bob carry out the DCT transform of the received signals and calculate the estimated values after the transform, and then carry out the power normalisation of the DCT transformed values and the power normalised values according to the power normalisation. update the filter coefficients according to the value obtained from the power normalisation and the error function; finally Alice and Bob go through the channel detection values of the LMS algorithm.

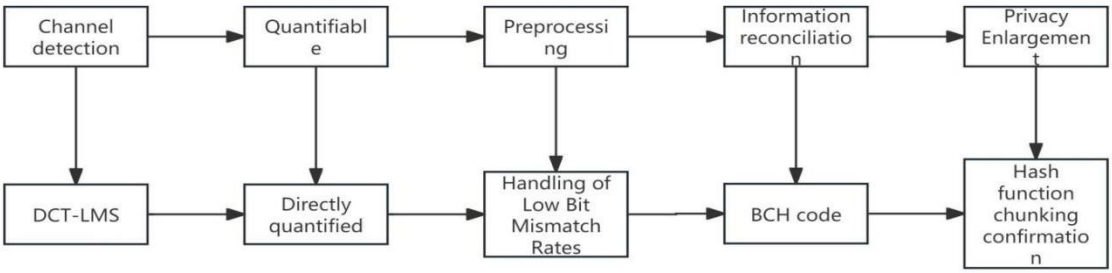


Figure 2. Flow of key generation scheme based on DCT-LMS public guide frequency detection protocol

The flow of the key generation scheme proposed in the literature includes: the channel detection phase adopts the public guide frequency detection association of DCT-LMS mentioned above (Figure 2); the quantisation phase adopts direct quantisation; the quantisation pre-processing phase improves the quantisation processing method that quickly reduces the initial bit mismatch rate, and performs the modulo-2-addition operation on the initial key sequences of the two sides of the communication and then the two sides remove the erroneous bits according to the results, which can further reduce the key inconsistency rate and improve the key generation rate; the message reconciliation phase adopts BCH code; the confidentiality enhancement phase adopts hash chunk confirmation mechanism[20]. The key inconsistency rate can be further reduced and the key generation rate can be improved; BCH code is used in the message reconciliation phase; and the hash chunk confirmation mechanism is used in the confidentiality enhancement phase [21].

3.2.2. Performance analysis

Figure 3 shows the simulation curves of key generation rate, KGR for the overall scheme of key generation, based on the results we can draw the following conclusions:(1) Among the different channel probing protocols, the channel probing protocols of LMS-PP and DCT-LMS-PP significantly improve the KGR compared to the one that does not take the adaptive filtering algorithm (2) Among the different quantisation pre-processing schemes, the improved scheme proposed in this chapter has the highest KGR. In summary, the key generation scheme combining the DCT-LMS-PP detection protocol and the improved scheme has the best KGR performance.

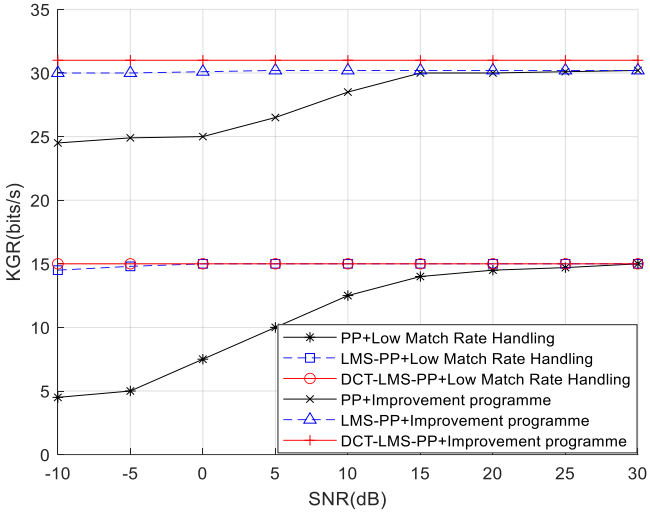


Figure 3. Overall scheme key generation rate with signal-to-noise

3.3. Key generation for quasi-static environments

Since many wireless communication application scenarios are fixed or change very little, many indoor environments, the surrounding objects and structures remain basically unchanged, this low mobility will lead to small changes in the wireless channel characteristics, forming a quasi-static environment, which leads to a longer correlation time for the channel and a reduction in the rate and randomness of key generation. In order to solve the problem of low performance of key generation in quasi-static channel environment Huang's team proposes a key generation scheme based on private frequency guide and singular value decomposition; Li's team achieves the purpose of enhancing the channel randomness by adding RIS reflection link in the communication link, which in turn improves the performance of generating keys; Yang's team investigates the effect of cyclic scheduling and random scheduling of antennas on enhancing channel By studying the effect of cyclic scheduling and random scheduling of antennas on enhancing channel variations, Yang's team proposes a key generation method based on channel obfuscation and verifies the method's performance enhancement of key generation in slow-varying environments.

3.3.1. Key generation scheme based on private guide and singular value decomposition

Under static or quasi-static wireless channel conditions, in order to improve the randomness and key generation rate of key generation based on wireless channel. The literature "Research on Private Guide Frequency Based Physical Layer Key Generation and Application Techniques" combines the private guide frequency and singular value decomposition techniques, and proposes a key generation scheme based on the private guide frequency and singular value decomposition, firstly, the wireless channel is reconstructed with singular value decomposition technique to increase the channel richness, and then, the private guide frequency is combined with the reconstructed equivalent wireless channel, and the private guide frequency is dynamically updated in the process of key generation. The key is dynamically updated during key generation. The problem of slow wireless channel change in quasi-stationary environment is solved, and the security of key generation is further enhanced. The specific steps of singular value decomposition include: firstly, Alice and Bod perform channel training and channel estimation by sending each other private guide signals and perform singular value decomposition on the channel estimation values respectively; according to the first two steps, Alice and Bod generate random diagonal matrices and reconstruct the wireless channel matrix respectively; finally, Alice and Bob use the reconstructed wireless channel to modulate the transmitted private guide frequency, which results in a new private guide frequency that Alice and Bob use to generate keys. equivalent channel that Alice and Bob use to generate the key (Figure 4).

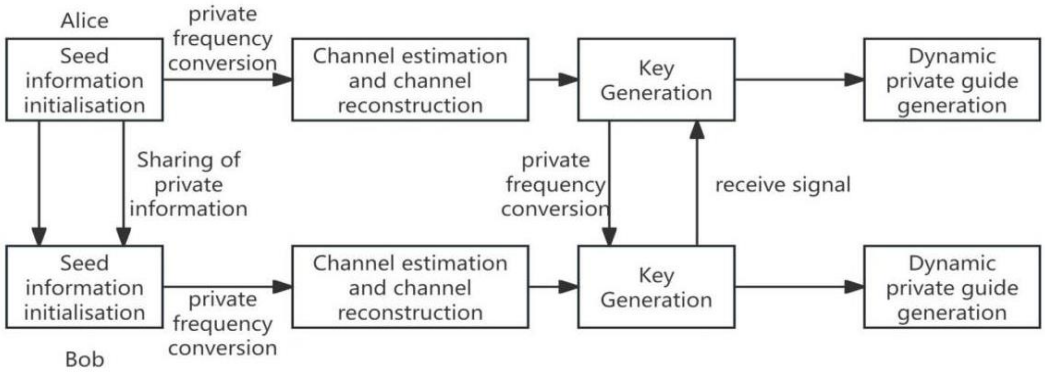


Figure 4. Key generation scheme based on dynamic private guide and singular value decomposition techniques

The specific process of the key generation scheme proposed in the literature includes: firstly, the seed information of the private guide is initialised and the private guide is generated. Then Alice and Bob perform channel training and channel estimation on the wireless channel, obtain the channel estimation value, perform singular value decomposition on it, and reconstruct the wireless channel matrix. After that Alice uses the reconstructed wireless channel to modulate the private guide frequency that needs to be sent, sends the modulated signal to Bob, and Alice generates the key based on the signal received by Bob. Finally new seed information of the private guide is generated and new private guide is generated.

3.3.1.1. Performance analysis

In order to calibrate the randomness of the key generation based on the private guide and singular value decomposition techniques in a quasi-static wireless channel environment, a comparison is made with the random beamforming based key generation scheme described in the literature [22].

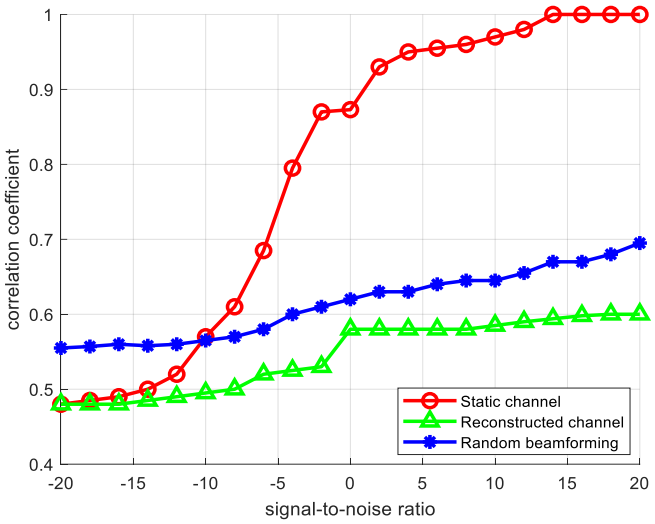


Figure 5. Variation of correlation coefficient of neighbouring keys with signal-to-noise ratio

As shown in Figure 5 the randomness of the key generated from the wireless channel is good at low SNR, but as the SNR increases, the randomness of the generated key becomes less and less and its correlation coefficient becomes higher and higher. From the figure it can be obtained that the randomness of key generation based on private guide and singular value decomposition technique is better than the randomness of key generation by random beamforming.

In the case of passive eavesdropping, the key generation rate of the key generation scheme based on the private frequency guide and singular value decomposition technique and the variation of the key generation rate according to the random beamforming with the signal-to-noise ratio are shown in Figure 6. From this, we can conclude that in the quasi-static channel environment, the key generation rate of the key generation scheme based on dynamic private frequency guide and singular value decomposition is fast and the leakage rate is small, i.e., this scheme has a strong ability to prevent passive eavesdropping.

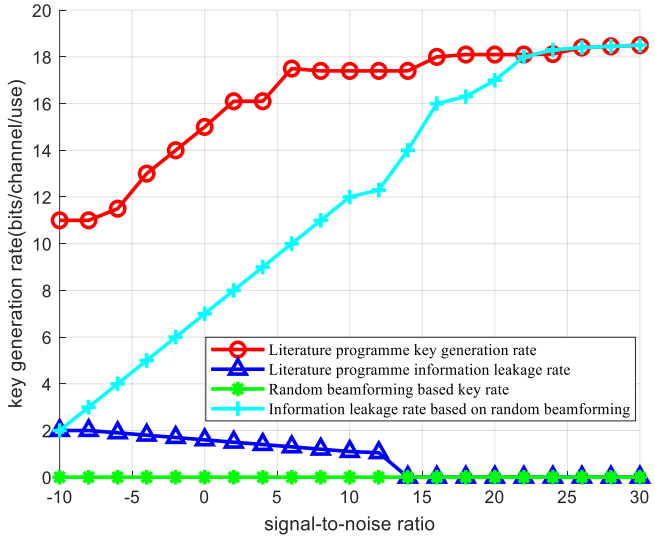


Figure 6. Variation of key generation rate with SNR under passive eavesdropping

3.3.2. RIS-assisted Wireless Physical Layer Key Generation Based Scheme

Starting from the time-varying and randomness of the channel on which the wireless channel key generation technique relies, since RIS can adjust the propagation direction of the reflected electromagnetic waves in real time, it can improve the problems of weakened temporality, slow key update rate as well as low randomness of the quasi-static channel environment, and the literature [23] points out that RIS has reciprocity below 6 GHz and millimetre wave frequencies, which can be used

for key generation. Therefore, RIS is introduced as a public random source into the wireless channel to add randomness and time-varying nature to the static channel and to solve the problem of weakened key randomness as well as reduced update rate. The article uses two USRPs to simulate two communicating parties (Alice and Bob) to send and receive data.The experimental results show that the addition of RIS to the communication link can effectively improve the key generation rate and key randomness,which helps in the physical layer key generation. However, when RIS is controlled by an illegal person,it will hinder the key generation.

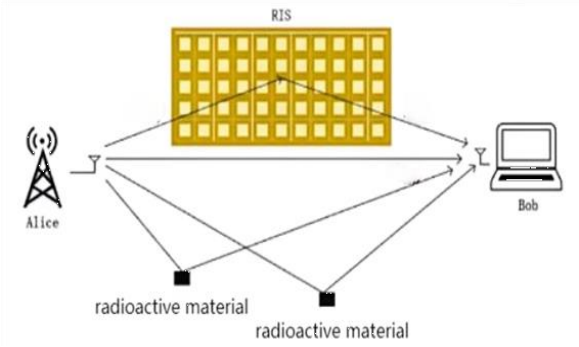


Figure 7. RIS-assisted key generation system

Considering the weakening of the time-varying nature of the channel in a quasi-stationary channel environment, the literature "Research on the Theory and Technology of Wireless Physical Layer Key Generation" introduces RIS into the key generation system, and then analyses the enhancement effect of RIS on the key generation.The RIS-assisted key generation system consists of the two legitimate communicating parties, Alice and Bob, the intelligent hypersurface RIS, and the illegitimate user, Eve. Introducing RIS into the process of key generation is equivalent to introducing a channel between the legitimate communicating parties while outside, as shown in Figure 7, RIS receives the guided frequency signal from Alice and then intelligently regulates the amplitude and phase of the reflected signal in reflecting to Bob, forming an Alice-RIS-Bob link.

3.3.2.1. Key generation process and performance analysis

The key generation process in this paper revolves around assisting key generation when the RIS is controlled by a legitimate party and hindering key generation when it is controlled by an illegal party, to verify the enhancement and hindering effects of the RIS on key generation, and the generation process is shown in Figure 8.

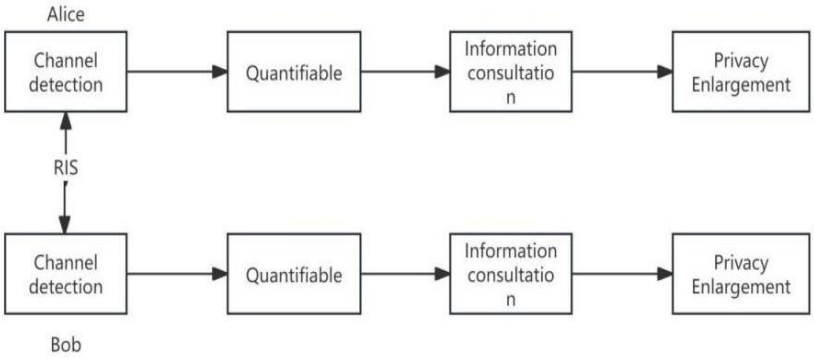


Figure 8. RIS auxiliary key generation process

The key generation process proposed in the literature includes: channel detection stage using RIS can only regulate the amplitude and phase of the reflected electromagnetic wave to enhance the time-varying nature of the electromagnetic propagation environment; RIS can change its own update rate to ensure that the two sides of the communication can complete the upstream and downstream channel detection one or more times within an update of the RIS, and according to the continuous change of the RIS, the rate of key updating can also be guaranteed; quantisation stage using CDF-based

quantisation algorithm and dual-threshold quantisation method. The quantisation phase uses the CDF-based quantisation algorithm and the double threshold quantisation method. In the message negotiation phase, BCH error correction code is used for error correction; in the privacy amplification phase, hash function is used to eliminate the risk of key leakage.

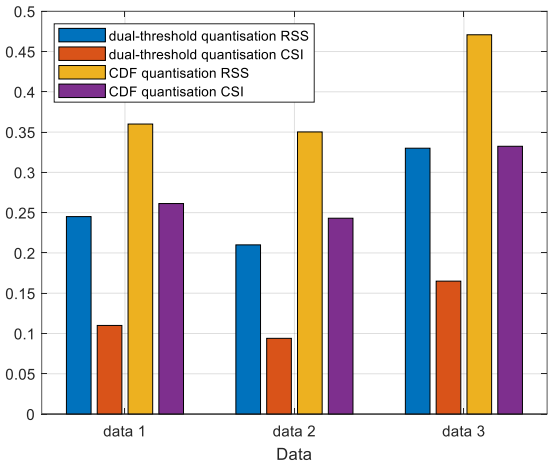


Figure 9. Inconsistency rate of generated key bits when Alice and Bob's positions are fixed

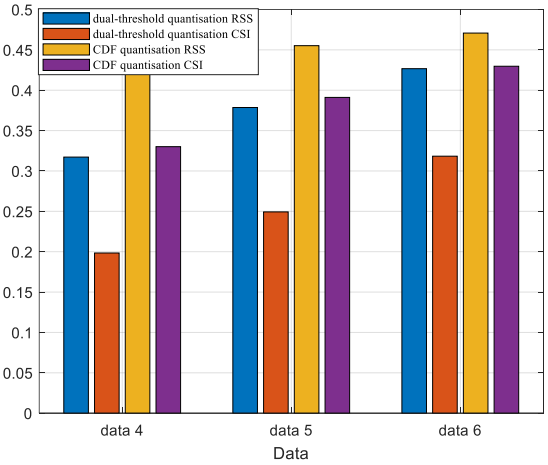


Figure 10. Bob can generate key bit inconsistency rates while moving horizontally

From Figures 9-10, it can be seen that the bit inconsistency rate using CSI is significantly lower than that using RSS, and the bit inconsistency rate of Data 3 is significantly higher than that of Data 1 and Data 2, which indicates that RIS can enhance the reflected path energy and improve the signal-to-noise ratio while reducing the bit inconsistency rate, which helps in key generation. The results also show that the bit inconsistency rate increases as Bob gets further away from the RIS centre.

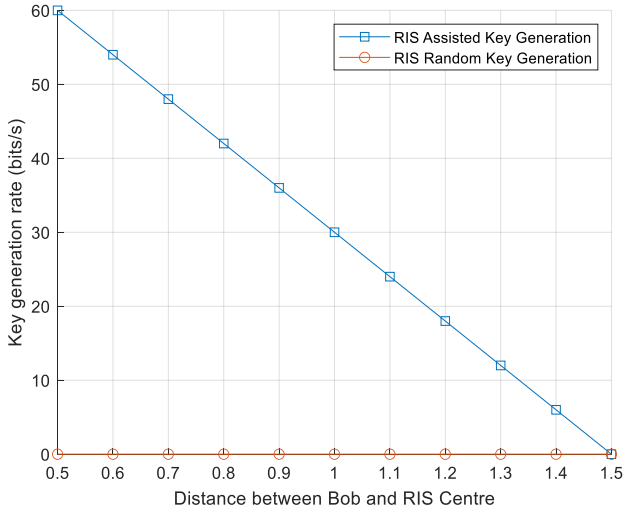


Figure 11. Key generation rate

3.3.3. Key Generation Method Based on Channel Obfuscation

To address the problem of slow channel feature changes and low key generation rate and randomness in quasi-static channel environments, the literature "Security Assessment and Enhancement Methods for Wireless Channel Keys" proposes a channel obfuscation-based key generation method for wireless channels, which proposes a channel obfuscation protocol to obfuscate the channel using stochastic filtering and antenna scheduling, which allows the legitimate parties to obtain the reciprocal channel features, and to extracts the key through K-L variation and adaptive quantisation, which solves the problem of slow channel feature variation and low key generation rate and randomness. The specific flow of the channel obfuscation protocol consists of the following: after inputting the guide signal in the input phase Alice starts executing the algorithm, Alice performs n rounds of loops, and a random variable is generated in each loop In each round of loops Alice uses these random variables to multiply them with a periodic function to generate a new vector. Each element of this vector is a complex random variable whose phase is determined by the random variable. Finally Alice uses this newly generated vector to perform some form of convolution with her derivative signal S to generate two new CSI vectors and output them (Figure 12).

The flow of the key generation scheme proposed in the literature includes: channel confusion phase Alice and Bob obtain the channel estimation by sequentially trying to send the guide signals to each other during the channel confusion; in the key generation phase firstly, the elements in the collected CSI matrix are partitioned into multiple blocks, and the CSI values in the same block are vectorially worded into a single column, and then the matrices are rearranged. Then Alice calculates the channel covariance matrix and decomposes its eigenvalues to obtain the eigenvector matrix and eigenvalue matrix, selects the first P-column vectors of the eigenvector matrix to construct the transform matrix, Alice sends the constructed transform matrix to Bob, and the new CSI matrix is obtained by multiplying the rearranged CSI matrix with it. After that quantisation phase in the new CSI matrix the CSI values are converted into a sequence of bits by adaptive quantisation algorithm respectively; message reconciliation phase uses BCH codes to correct the inconsistent bits in the original key according to their inconsistency rate; privacy amplification phase uses MD5 algorithm to perform privacy amplification, which maps the data of arbitrary size to 128-bit data.

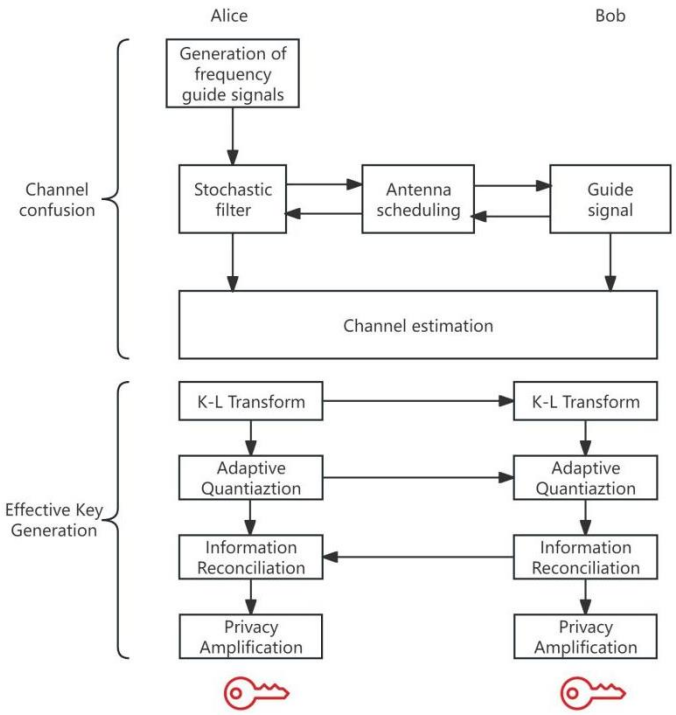
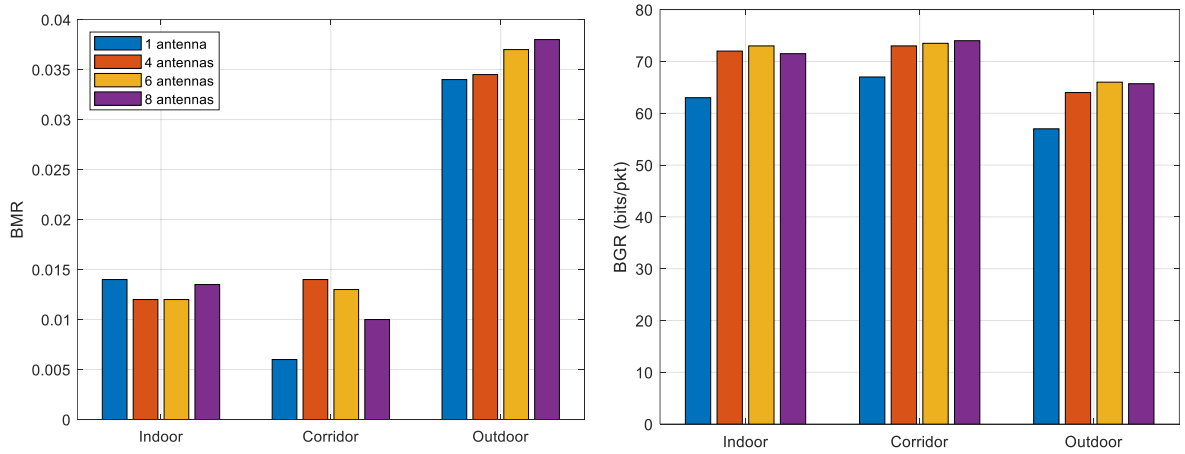


Figure 12. Key generation flow based on channel obfuscatio

3.3.3.1 Performance analysis

According to Figure 13 it can be seen that in different scenarios such as indoor, corridor and outdoor, the values of BMR and BGR change as the number of antennas increases. Especially in the outdoor environment, when the number of antennas increases, the increase in BGR slows down and may even become smooth. This suggests that after a certain number of antennas, adding more antennas has a limited effect on BGR enhancement, possibly because the capacity limit of the channel has been reached or the added antennas do not bring additional channel diversity.



(a) BMR (b) BGR

Figure 13. Performance with different number of antennas

3.4. Key Generation Algorithm against Channel Estimation Errors

Wireless signals in the propagation process will encounter a variety of obstacles, resulting in signal reflection, scattering and bypassing, the formation of multipath propagation phenomenon which leads to complex channel response and difficult to accurately estimate; secondly, the channel measurement and feature extraction process needs to quantify the continuous signal, that is, converted to digital signals, quantisation process inevitably generates errors, in the channel characteristics of the smaller

changes or weaker signals, the error is more The performance and complexity of the channel estimation algorithm will also affect the accuracy of the estimation. To this end, Huang's team designs a physical layer key generation scheme compatible with the existing 5GNR beam management framework, i.e., beam-based physical layer key generation, by studying the acquisition and quantization of beam direction information; Ren's team proposes a private frequency-guided channel detection protocol and 2D cyclic quantization based on existing channel detection protocols and quantization schemes, and in this way, puts forward a 2D cyclic quantization key generation scheme based on private frequency-guided 2D cyclic quantization. The key generation scheme is based on two-dimensional cyclic quantisation of the private guide frequency;

3.4.1. Beam-based physical layer key generation

Massive MIMO not only improves the spectral efficiency of the system, but also generates a new spatially dimensional channel feature, i.e., beam direction. Compared with other channel features it takes discrete values, which can avoid the error caused by quantisation in conventional physical layer key generation. The literature "Research on Key-Based Physical Layer Security Technology in 5G Large-Scale Antenna System" focuses on the acquisition and quantisation of beam direction information, and designs a physical layer key generation scheme compatible with the existing 5GNR beam management framework, i.e., beam-based physical layer key generation, which solves the error generated by channel estimation of the two legitimate communicating parties in the normal communication process. The specific phases of beam management include,Initial access: coarse wave scanning is performed first, after which a pair of coarse beams for upstream and downstream communication will be initially established between the UE (user-side) and the gNB (base-station-side);Beam refinement: the optimal pair of fine beams is determined. The coarse beam waves determined in the previous and previous stages are divided into several fine beam waves. The above two stages constitute beam management. At each stage, beam management is based on four different operations: beam scanning, beam measurement, beam determination and beam reporting.

3.4.1.1. Key Generation Algorithm Design Process and Performance Analysis

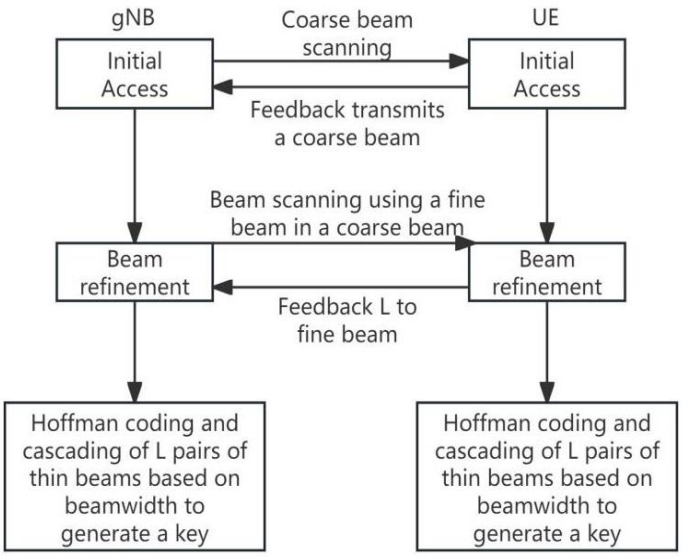


Figure 14. Key generation flowchart

The beam-based physical layer key generation process is mainly divided into three phases: initial access phase, beam refinement phase, and key generation phase, and the process is shown in Figure 14. In the initial access phase, the device determines the optimal beam direction by means of wave speed scanning and beam measurement, and both the base station and the user turn off part of the antenna to transmit/receive using the coarse beam. In the fine beam search phase, the beam direction and quality are further optimised by beam determination and beam reporting, and both the base station and the user turn on all antennas. Finally, the base station and the user each performs Hoffman coding

and cascading of L pairs of fine beams according to the probability of the beams being selected to generate the final physical layer security key.

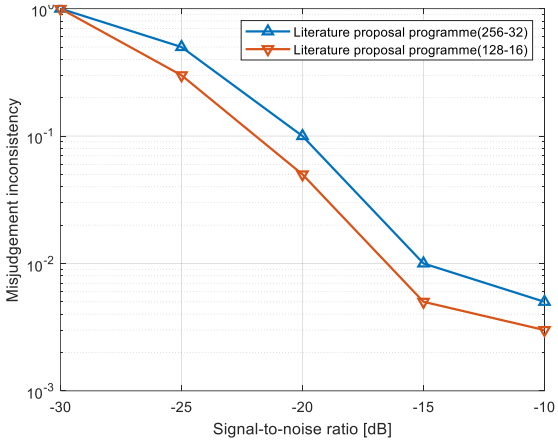


Figure 15. Key generation rate under different SNR and antenna configurations

Figure 15 compares the number of bits of the binary key obtained from the quantisation of the sequential number information of the best and alternate beam pairs obtained after completing a coarse beam search for two antenna configurations, using the angle of arrival and departure as random sources for comparison with the scheme, and it can be seen that increasing the number of antennas is effective in increasing the number of bits of the key generated.

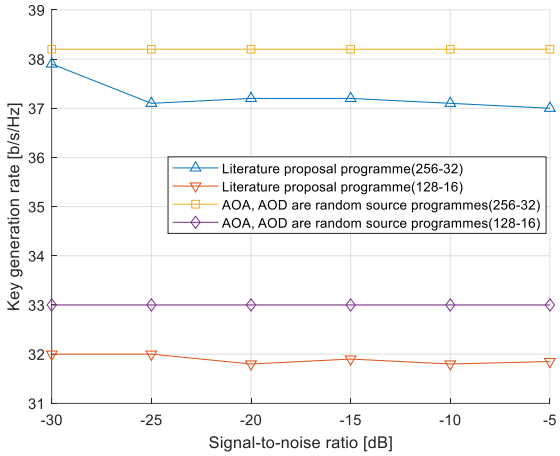


Figure 16. key inconsistency rate for the two antenna configurations

Figure 16 shows the key inconsistency rate for the two antenna configurations, from which it can be seen that the key inconsistency rate is more at low SNR; when the SNR is increased, the key inconsistency rate decreases significantly.

4. Comparative analysis of solution performance

This chapter presents a comprehensive performance analysis comparing the solutions studied in the paper in terms of key generation rate, key inconsistency rate, randomness of generated keys and communication cost as shown in the following Table 3.

Table 3. Comparison of five options for solving problems

Programme / Problems / Scenarios	signal interference	quasi-stationary environment	channel estimation error
DCT-LMS-PP+ Improved Quantification Programme	√	×	√
A key generation scheme based on private derivative and singular value decomposition	√	√	×
RIS-assisted Wireless Physical Layer Key Generation Based Scheme	×	√	×
Key generation method based on channel obfuscation	√	√	×

The three kinds of difficulties and challenges of wireless channel key generation mentioned above, in terms of signal interference, there are various aspects and types of interference, and the solution proposed now can not eliminate all the interference, but only some specific known interference; in terms of quasi-static channel, the impact it brings to the channel key generation is better solved, but solving the quasi-static channel problem requires some artificial factors of interference, which will Finally, in the elimination of channel estimation error, if the estimated channel error exists between the two legitimate communication parties, then the consistency of the channel feature information obtained by both parties will be poor, which will lead to a high rate of inconsistency in the initial key bits quantified by the two parties, resulting in the need for more negotiation information to rectify the inconsistent bits, which not only increases the communication overhead but also leaks a large amount of information to the eavesdropper. This not only increases the communication overhead, but also leaks a lot of communication information to eavesdroppers, and seriously leads to the failure of key negotiation.

To address these problems, we can combine the DCT-LMS-PP+ improved quantisation scheme with the RIS-assisted wireless physical layer key generation scheme to combat signal interference and improve the consistency of key generation while expanding its application scenarios. It is also possible to combine the channel obfuscation-based key generation method with the beam-based physical layer key generation scheme to compensate for the low key generation rate and reduce the inconsistency of the generated keys. We still need to explore the research to further improve the performance of wireless channel key generation (Table 4).

Table 4. Comparison of scenarios applicable to the five options

Applicable Scenarios / Programme	mobile scenario	still scene	Complex communications environment
DCT-LMS-PP+ Improved Quantification Programme	×	×	√
A key generation scheme based on private derivative and singular value decomposition	×	√	√
RIS-assisted Wireless Physical Layer Key Generation Based Scheme	×	√	×
Key generation method based on channel obfuscation	×	√	×
Beam-based physical layer key generation scheme	×	√	×

DCT-LMS-PP+ improved quantisation scheme, key generation scheme based on private guide and singular value decomposition need some complex algorithms and hardware resources support by themselves in solving the corresponding problems; RIS-assisted wireless physical layer key generation scheme needs to increase RIS; channel obfuscation-based key generation method, and physical layer key generation scheme based on beams need to use multi-antenna system,. All these will increase the communication cost.

In the existing technical solutions can only have complex algorithms, hardware resource support and other equipment configuration to solve the problems mentioned in the paper, when faced with a low configuration of equipment or even no hardware resource support, how do we solve the problems faced by the wireless key generation, with the development of 6G technology, the Internet of Things Internet of Things has become a mainstream point-to-point communication communication link equipment, we can combine the two to solve the problems we face when there is no device configuration. We can combine the two to solve the problem of key generation in the absence of device configuration.

5. Summary

This paper analyses the difficulties and challenges faced in key generation for wireless channels, combs out the existing typical technical solutions, and makes a comprehensive analysis and comparison of their performances in four aspects, namely, key generation rate, key inconsistency rate, generated key randomness, and communication cost.

In the first two chapters, the first chapter describes the research background as well as the significance of physical layer wireless key generation, and colleagues give an overview of the current state of the art of physical layer key generation technology and present the current difficulties and challenges faced by channel key generation. In Chapter 2, a more comprehensive introduction to the traditional model of wireless channel key generation is given. In Chapter 3, the solutions to the proposed problem are systematically sorted out and their respective performances are analysed. In Chapter 4, the performance of the solutions studied in the paper is analysed in a comprehensive comparison and further research is proposed.

References

[1] Shannon C E. Communication theory of secrecy systems[J]. The Bell system technical journal, 1949, 28(4):656-715.

[2] Maurer U M. Secret key agreement by public discussion from common information[J]. IEEE transactions oninformation theory, 1993, 39(3): 733-742.

[3] Hershey J E, Hassan A A, Yarlagadda R. Unconventional cryptographic keying variable management[J]. IEEE Transactions on Communications, 1995, 43(1): 3-6.

[4] Premnath, Sriram, Nandha, et al. Secret key extraction from wireless signal strength in real environments [J]. IEEE Transactions on Mobile Computing,2013,12(5):917-930.

[5] Youssef E H S, Hogrefe D. An optimal guard-intervals based mechanism for key generation from multipath wireless channels[A]. IEEE International Conference on New Technologies, Mobility and Security[C], 2011:1-5.

[6] Ohira T. Secret key generation exploiting antenna beam steering and wave propagation reciprocity [A]. European Microwave Conference[C], Paris, France,2005:23-27.

[7] Wang Q,Xu K, Ren K. Cooperative secret key generation from phase estimation in narrowband fading channels [J]. IEEE Journal on Selected Areas in Communications, 2012, 30(9): 1666-1674.

[8] S. Jana, S. N. Premnath, M. Clark, et al. On the effectiveness of secret key extraction from wireless signal strength in real environments[C]. Proceedings of the 15th annual international conference on Mobile computing and networking. ACM, Beijing, China, 2009, 321-332.

[9] Long Jiao, Tang Jie, Zeng Kai. Physical Layer Key Generation Using Virtual AoA and AoD of mmWave MassiveMIMOChannel[A]. IEEE Conference on Communications and Network Security[C],2018:1-9.

[10] C. E. Shannon.Communication Theory of Secrecy Systems*[J].Bell System Technical Journal,1949(4).

[11] LI Gu Yue,HU Ai Qun. Wireless channel key extraction method based on K-L transform[J]. Journal of Southeast University: natural science edition, 2017, 47(2):6

[12] Margelis G, Fafoutis X, Oikonomou G, et al. Physical layer secret-key generation with discreet cosinetransform for the Internet of Things[C]2017 IEEE international conference on communications (ICC). IEEE,2017: 1-6.

[13] Youssef E H S, Hogrefe D. An optimal guard-intervals based mechanism for key generation from multipath wireless channels[C]2011 4th IFIP International Conference on New Technologies,Mobility and Security. IEEE, 2011:1-5.

[14] Cai, W.-B. Research on the theoretical limit and quantitative method of generating keys based on wireless channel characteristics[D]. Henan:PLA Information Engineering University,2013.

[15] Yasukawa S, Iwai H, and Sasaoka H. A secret key agreement scheme with multi-level quantization and parity check using fluctuation of radio channel property [A]. IEEE International Symposium on Information Theory[C], Toronto, Canada, 2008:732-736.

[16] Dai Peak, Jin Liang, Huang Kaizhi. Design of adaptive key generation scheme based on channel feature quantisation[J]. Journal of Communication,2014,35(1):191-197.

[17] Liu Jingmei, Han Qingqing, Shen Zhiwei,et al. Physical layer key generation scheme using k-mean clustering[J]. Journal of Xi'an Electronic Science and Technology University,2019,46(1):6.

[18] Zhu X, Xu F, Novak E, et al. Extracting secret key from wireless link dynamics in vehicular environments[C]IEEE INFOCOM. ieee, 2013:2283-2291.

[19] Bai E, Jiang X, Wu Y. Memory-Saving and High-Speed Privacy Amplification Algorithm UsingLFSR-Based Hash Function for Key Generation[J]. Electronics, 2022, 11(3):377.

[20] Yasukawa S,Iwai H,Sasaoka H.Adaptive key generation in secret key agreement scheme basedon the channel characteristics in OFDM[C]2008 International Symposium on InformationTheory and Its Applications.IEEE,2008:1-6.

[21] Huang Y,Zhou S,Shie Z,et al.Channel frequency response-based secret key generation inunderwater acoustic systems[J].IEEE Transactions on Wireless Communications,2016,15(9):5875-5888.

[22] Longwang Cheng,Wei Li and Dongtang Ma.Secret Key Generation via Random Beamforming in Stationary Environment [C].International Conference on Wireless Communications & Signal Processing (WCSP),2015:1-5.

[23] Tang W,Chen X,Chen M Z,et al.On channel reciprocity in reconfigurable intelligent surface assistedwireless networks[J].IEEE Wireless Communications,2021,28(6):94-101.