Optimal Subcarrier Allocation Scheme for Physical-Layer Key Generation in an OFDMA Network

Qingjiang Xiao, Guyue Li, *Member, IEEE,* Zilong Liu, *Senior Member, IEEE,* Aiqun Hu, *Senior Member, IEEE*

***Abstract*—This paper studies enhanced physical-layer key generation (PKG) for multiuser orthogonal frequency division multiple access (OFDMA) networks. In practical OFDMA systems, our key observation is that there are frequency correlations between different subcarriers which potentially lead to compromised randomness of the generated keys as well as reduced sum secret key rate. Motivated by this, we show that subcarrier allocation plays a key role in enhancing the PKG performance in OFMDA networks. We prove that when a single user terminal selects a finite number of subcarriers for key generation, adopting uniformly spaced subcarriers is the optimal solution as it leads to higher secret key rates and better randomness. Moreover, we derive a closed-form expression for the sum secret key rate and introduce a low-complexity near-optimal algorithm that can achieve an appropriate subcarrier allocation policy in a timely manner. Simulation results show that our proposed near-optimal algorithm exhibits significant advantages in maximizing the sum secret key rate and improving key randomness compared with existing subcarrier allocation algorithms.**

***Index Terms*—Key generation, OFDMA, physical-layer security, sum rate maximization, multi-user.**

I. Introduction

THE next generation mobile communication systems must be not only reliable, fast, efficient, but also highly secure. However, the open nature of wireless networks [1] makes them susceptible to various malicious attacks like eavesdropping and impersonation attacks [2], [3]. Key distribution is a critical part of communication security. Traditionally, the key distribution is usually handled by the Diffie-Hellman protocol to set up shared secret keys [4]. PKG can be regarded as another type of key distribution scheme that is applicable in certain specific scenarios. For instance, PKG does not require modular exponentiation of large prime numbers, making it suitable for resource-constrained lightweight devices with limited computational resources [5], [6].

Physical-layer key generation (PKG) has emerged as a promising technology to share the symmetric key for cryptographic applications [7]. By exploiting the inherent characteristics of wireless channels [8], for example, PKG can take advantage of the channel reciprocity for symmetric key generation without complex computation, update the keys frequently in accordance with the nature of the time-varying channels [9], and protect the keys from eavesdropping through spatial decorrelation [10]. Moreover, PKG can achieve information-theoretic security [11], less affected by computational hardware advancements or more efficient algorithms. Nowadays, PKG has become an important security task of the integrated communication and security system (ICAS) [12]. With ICAS, one can achieve mutual benefits of communication and security functions by sharing spectrum, power and hardware resources, etc. Several studies [13], [14] have focused on the optimization problem of PKG within the ICAS.

This paper is concerned with efficient PKG design for orthogonal frequency division multiple access (OFDMA) which has attracted significant research attention owing to its efficient hardware implementation, resilience to frequency selective channels, and high spectrum efficiency. For decades, OFDMA has been widely applied in a number of application scenarios, such as the 3GPP long-term evolution (LTE), 5G New Radio (NR), and WiFi networks [15]–[18]. In view of its dominance in modern communication systems, it is urgent to find an efficient and reliable way to secure OFDMA-based networks. Secondly, considering the proliferation of the devices in OFDMA-based networks and the constraints in computation & battery life, PKG is more attractive compared to the cryptography-based methods. In addition, the secret key rate of the PKG scheme can be improved by leveraging the fine-grained channel state information (CSI) from individual subcarriers for enhanced security [19]–[22].

In the literature, PKG has been applied to various communication technologies such as multiple input multiple output (MIMO) [7], [23], [24], reconfigurable intelligent surface (RIS) [8], [25] and orthogonal frequency division multiplexing (OFDM) [9], [20]–[22], and has also been explored in OFDMA [19], [26]. In [19], Zhang *et al.* designed an OFDMA-based multi-user PKG protocol for efficient key generation with reduced channel probing overhead. In [26], Yaacoub investigated secret key generation using MIMO systems for single-user transmission in which the subcarriers in

Manuscript received 17 May 2024; revised 19 March 2025 and 17 April 2025; accepted 18 April 2025. This work was supported in part by the Frontier Technologies R&D Program of Jiangsu under Grant BF2024065; in part by the National Natural Science Foundation of China under Grant 62171121 and Grant U22A2001; in part by the Natural Science Foundation on Frontier Leading Technology Basic Research Project of Jiangsu under Grant BK20222001. (Corresponding authors: Guyue Li)

Qingjiang Xiao is with the School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China. (e-mail: qjxiao@seu.edu.cn)

Guyue Li is with the School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China, and also with the Purple Mountain Laboratories, Nanjing 210096, China (e-mail: guyuelee@seu.edu.cn).

Zilong Liu is with the School of Computer Science and Electronics Engineering, University of Essex, Colchester CO4 3SQ, U.K. (e-mail: zilong.liu@essex.ac.uk).

Aiqun Hu is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China, and also with the Purple Mountain Laboratories, Nanjing 210096, China (e-mail: aqhu@seu.edu.cn).

OFDMA were exploited to increase the key length. Although these methods provided feasible PKG procedures to generate keys for OFDMA networks, they overlooked the impact of frequency correlation among different subcarriers on the performance of PKG and did not explore how a subcarrier allocation scheme can help improve the secret key rate.

To fill this gap, we propose an optimal subcarrier allocation scheme for PKG in an OFDMA network aiming to maximize the sum secret key rate. The main contributions of this paper can be summarized as follows.

- We present an optimal subcarrier allocation scheme tailored for PKG in OFDMA and show that it is necessary to analyze the impact of subcarrier frequency correlation on key generation. We further investigate the mathematical characteristics of frequency correlation and prove that when a single user terminal (UT) occupies multiple subcarriers for key generation, adopting uniformly spaced subcarriers for key generation leads to higher secret key rates and better randomness as it can mitigate the effects of frequency correlation to the greatest extent. Additionally, we derive a closed-form expression for the sum secret key rate based on mutual information and [7], [9], and provide a novel observation on the secret key rate for UTs.
- Next, we optimize the subcarrier allocation policy in order to maximize the sum secret key rate while meeting the security requirements of all UTs. Since the optimization problem is NP-hard, we develop a low-complexity near-optimal algorithm with negligible increase of processing time and computational overhead.
- Simulation results demonstrate that our proposed scheme effectively improves the performance of PKG in an OFDMA network. Compared with the existing random and continuous subcarrier allocation algorithms, the obtained subcarrier allocation scheme arising from our proposed algorithm improves the sum secret key rate by 9.93% and 40.59%, respectively. When facing the same security requirements, the required number of subcarriers is reduced by more than 5.74% and 20.15%, respectively. Besides, our generated keys generally exhibit stronger randomness with higher pass ratios under the National Institute of Standards and Technology (NIST) random test suite [27].

Notations: Throughout the paper, scalars, vectors, and matrices are represented by lowercase letters, boldface lowercase letters, and boldface uppercase letters, respectively. $\mathbb{C}^{A\times B}$ denotes a complex matrix space with a size of $A\times B$. $(\cdot)^H$ refers to the Hermitian transpose. $O(\cdot)$ represents an asymptotic upper bound. $\Gamma(\cdot,\cdot)$, $\sigma(\cdot)$, and $\delta(\cdot)$ represent the covariance, standard deviation, and Dirac delta function, respectively. $\mathbb{E}\{\cdot\}$ represents statistical expectation. $x!$ denotes the factorial of a non-negative integer x. $|a|$ and $\det(\mathbf{A})$ represent the modulus of scalar a and the determinant of matrix $\mathbf{A}$. $I(X;Y)$ represents the mutual information between two random variables, and $I(X;Y|Z)$ represents the conditional mutual information between X and Y given that random variable Z is known. C_m^n denotes the combination number of choosing m elements from n distinct elements, and $\int_a^b f(x)dx$ represents the integration of the function $f(x)$ from a to b. $\lfloor\cdot\rfloor$ represents the floor function, which maps a real number to the largest integer less than or equal to that number.

The rest of this paper is organized as follows. Section II introduces related work on maximizing the sum secret key rate in multi-user scenarios and utilizing multiple subcarriers for key generation in OFDMA/OFDM systems. Section III presents the system and channel models, and briefly introduces the workflow of PKG with our subcarrier allocation scheme. In Section IV, we elucidate the necessity of an optimal subcarrier allocation scheme for improving the performance of PKG in OFDMA and formulate the subcarrier allocation problem as an optimization problem. Section V analyzes the optimization problem and provides a detailed description of the algorithm design which can solve the problem in a timely manner. In Section VI, the performance of the proposed algorithm is evaluated through simulations. Finally, conclusions are drawn in Section VII.

II. Related Works

To the best of our knowledge, none of the existing PKG solutions have explored the secret key rate maximization by optimizing the subcarrier allocation scheme. In general, there are two main streams of research on PKG:

PKG in OFDMA/OFDM: In [19], Zhang *et al.* designed an efficient key generation protocol based on the known subcarrier allocation results to reduce the channel probing overhead. However, their focus was not on subcarrier allocation, and neither they studied such a problem. Yaacoub [26] explored using the large number of subcarriers in OFDMA to generate large keys in single-user massive MIMO scenarios. However, subcarrier allocation was not explored in [26], as the single UT can use all subcarriers without multi-user allocation issues. In [28], Wang *et al.* formulated a power and subcarrier allocation problem with the objective of maximizing the sum secrecy rate of an OFDMA-based broadband network. The problem was solved in an asymptotically optimal manner using dual decomposition. Nevertheless, their algorithm relies on channel probing results from all users on all subcarriers, leading to excessive overhead for channel probing. This significantly increases the time overhead and poses a challenge in the limited coherence time. Moreover, the algorithm does not account for frequency correlations between subcarriers. In [20] and [21], Li *et al.* have shown that the CSI data collected from OFDM systems suffer from high frequency correlations, thus leading to a low-entropy key. They then proposed a preprocessing approach based on principal component analysis (PCA) to address this problem, but they did not analyze the essential reason for the frequency correlation and their solution relied on the values measured by channel probing. Zhang *et al.* [22] mathematically modeled the OFDM system and expressed time and frequency correlation analytically. Nonetheless, they did not analyze the relations among frequency correlation, the randomness of the generated keys, and the secret key rate. Besides, none of the previous works in [20]–[22] have studied multi-user scenarios and taken into account the subcarrier allocation problem.

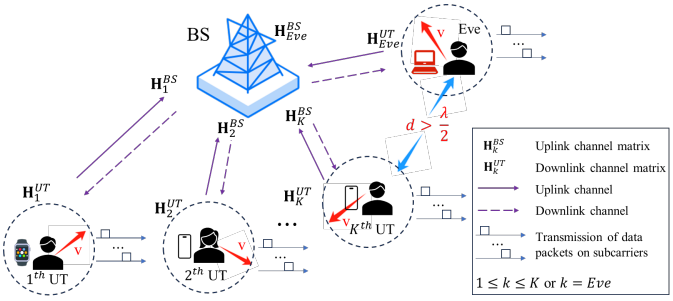

Fig. 1. A system model for multi-user key generation in OFDMA.

Sum secret key rate maximization: The sum secret key rate is a critical metric to evaluate the security of communication systems, which is defined as the sum of the lengths of generated keys from all UTs in bits per channel use. To maximize the sum secret key rate, various solutions have been devised [7], [23], [25]. Li *et al.* [7] analyzed the secret key rate and derived a closed-form expression for a massive MIMO system with multiple users, and further provided an optimization algorithm to achieve the maximal sum secret key rate. [25] has shown that the secret key rate without RISs may be low due to the inter-cell interference and this motivates them to propose an innovative RIS-aided multi-cell PKG framework. In addition, they also formulated a weighted sum key rate maximization problem which is non-convex and solved it through an alternating optimization algorithm. In [23], a sum secret key rate maximization problem was formulated for multi-user massive MIMO systems. A novel PKG scheme was developed to achieve the maximal sum secret key rate with reasonable power allocation and beam scheduling.

III. Models and Workflow Overview

In this section, we establish the system and channel models based on a multi-user OFDMA network (as shown in Fig. 1). Then, based on the above models, we illustrate how the optimal subcarrier allocation scheme can improve PKG in an OFDMA network by providing a workflow overview of PKG with our subcarrier allocation scheme.

A. System Model

Our paper considers an OFDMA system that comprises a base station (BS), an eavesdropper (Eve), and K mobile UTs with a relatively small speed v and unpredictable direction. This system can be viewed as block fading, with stable channel characteristics over a certain period of time. For the sake of problem formulation, the BS and K UTs are equipped with one antenna. We assume that the messages between UTs are forwarded through the BS rather than direct communications. Because of this, the keys should be generated between the BS and UTs to ensure communication security. During communications between the BS and UTs, each sender encrypts the information with the generated key before sending it to the receiver. Upon receiving the information, the receiver decrypts it using the same key to obtain the message. Moreover, different security devices may have varying requirements. For example, devices used in diplomatic or military contexts require significantly higher security than those used within a corporate intranet. Therefore, similar to [28], we require that the k^{th} UT being served with a nonzero secret key rate higher than $\Re_k$, which is called the security requirement of the k^{th} UT. Let $\{\Re_k | 1 \le k \le K\}$ denote the set of all security requirements.

We assume that Eve has the same equipment as the UTs, and she can perform passive eavesdropping to obtain the generated keys between the BS and UTs through her channel measurement by performing the same PKG process (see Subsection III-C). However, according to the spatial decorrelation [10], in rich-scattering environment, when Eve is located more than half a wavelength away from the legitimate UTs, the channel Eve experienced will be independent of that of legitimate UTs. It is worth noting that spatial decorrelation is a common situation that is easy to satisfy, because the center frequencies of mobile communication systems are generally in the GHz level and their half-wavelength is only a few centimeters [7], [9]. In addition, each UT is moving in an unknown direction at a speed v, and Eve can hardly follow any UT and keep the distance within half a wavelength. For this reason, Eve will not be taken into account in our subsequent analysis, but Eve's eavesdropping ability will be verified in Section VI.

B. Channel Model

In OFDMA, UTs transmit information over multiple subcarriers, whereby each subcarrier can only be occupied by one UT at most. The channel impulse response (CIR) of the multipath channel between BS and the k^{th} UT can be written as [19], [22]:

$$h_k^{\text{side}}(\tau, t) = \sum_{l=1}^{L} h_k^{\text{side}}(\tau_l, t)\delta(\tau - \tau_l), \tag{1}$$

where side $\in \{BS, UT\}$, represents where the CIR is obtained from, L is the number of the channel taps, τ_l is the delay of the l^{th} tap, and $h_k^{\text{side}}(\tau_l, t)$ is the corresponding attenuation.

To analyze the correlation between different subcarriers, we convert the CIR into channel frequency response (CFR) through the fast Fourier transform (FFT). Let N and $\mathbf{\Phi} = \{1, 2, \cdots, N\}$ denote the total number of subcarriers and the subcarrier set of the OFDMA system respectively, and all of the subcarriers are indexed as $n = 1, \cdots, N$. In our paper, let B denote the total bandwidth of the OFDMA system, and the total bandwidth is evenly divided into N subcarriers. The CFR of the n^{th} subcarrier that is allocated to the k^{th} UT can be expressed as

$$H_{k,n}^{\text{side}}(t) = \sum_{l=1}^{L} h_k^{\text{side}}(\tau_l, t) e^{-j2\pi f_n \tau_l}, \tag{2}$$

where $f_n = n \cdot \frac{B}{N}$ is the frequency value of the n^{th} subcarrier.

Let the matrix $\mathbf{H}_k^{\text{side}} = [\mathbf{h}_{k,n_1}^{\text{side}}, \mathbf{h}_{k,n_2}^{\text{side}}, \cdots, \mathbf{h}_{k,n_{N_k}}^{\text{side}}]^H \in \mathbb{C}^{N_k \times T}$ represent the channel matrix between the BS and the k^{th} UT, where N_k and $n_1, \cdots, n_{N_k}$ are the total number and

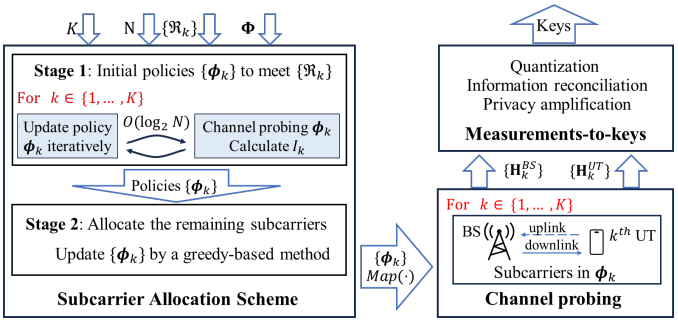

Fig. 2. Workflow of PKG with optimal subcarrier allocation scheme.

the indices of the subcarriers occupied by the k^{th} UT respectively, and $\mathbf{h}^{\text{side}}_{k,n_i} \in \mathbb{C}^{T\times 1}, i = 1, \cdots, N_k$ represent the CFR complex values of T samples. We assume that the multipath channel is rich scattering and hence the attenuation of different channel taps $h^{\text{side}}_k(\tau_i, t)$ and $h^{\text{side}}_k(\tau_j, t)$ are uncorrelated and the attenuation of each channel tap can be regarded as a random process [22].

C. Workflow of PKG with Subcarrier Allocation Scheme

In this paper, we propose an optimal subcarrier allocation scheme for PKG in an OFDMA network based on the models mentioned above, aiming to maximize the sum secret key rate and improve the randomness of generated keys while meeting the security requirements of all UTs. Compared to the conventional PKG framework, we introduce a novel subcarrier allocation scheme before channel probing. Such a scheme does not affect the strategy of subsequent steps and can be easily integrated into legacy PKG frameworks. The workflow of PKG with subcarrier allocation is shown in Fig. 2.

1) Subcarrier allocation: In this step, the subcarriers are allocated to UTs for data transmission and key generation. The output contains an allocation policy and a mapping function: i) Let $\{\phi_k | 1 \le k \le K\}$ denote the subcarrier allocation policy, where the set ϕ_k stores the subcarriers allocated to the k^{th} UT. ii) The mapping function $Map(\cdot)$ denotes the mapping function that stores the correspondence between subcarriers and UTs, and we can get the index k_n of the UT that occupies the n^{th} subcarrier by $Map(n)$. To utilize the subcarriers sufficiently and generate keys with improved randomness at a higher secret key rate, the general considerations for the optimal allocation method are: i) **Security requirement satisfaction.** When the k^{th} UT utilizes the subcarriers in ϕ_k for key generation, the secret key rate should be greater than its security requirement $\Re_k$. ii) **Sum rate maximization.** On the basis of satisfying the security requirements of all UTs, the sum secret key rate of the entire OFDMA system should be maximized. iii) **Secret key effectiveness.** The randomness of generated keys through allocated subcarriers must be guaranteed, meaning that the keys should be able to pass the tests in the NIST random test suite [27], which is a common tool used to evaluate randomness.

As shown in Fig. 2, the subcarrier allocation scheme achieves the initial allocation policy with the minimum number of subcarriers satisfying $\{\Re_k\}$ through iterative implementation in Stage 1, and then allocates the remaining subcarriers in Stage 2 to obtain the final allocation policy (details are provided in Subsection V-C). The scheme incurs only a small amount of additional time and computational overhead (as discussed in Subsection V-D), yet effectively mitigates the negative effects of subcarrier frequency correlation on PKG, resulting in improved sum secret key rate and better key randomness.

2) Channel probing: In this step, both UTs and BS obtain the channel information of each subcarrier via sending orthogonal pilots to each other. Each channel probing round should be completed within the channel coherence time. For example, given the coherence time $T_c = 9c/16\pi v f_n$ [9], where c is the speed of light, when the moving speed $v = 1.25$ m/s and the frequency $f_n = 3.5$ GHz, the coherence time is approximately 12 ms. Therefore, the channel probing rate should be set to 1 round/12 ms.

In the uplink, the k^{th} UT transmits the orthogonal pilot signal matrix $\mathbf{X}^{BS}_k \in \mathbb{C}^{T\times T}$ through subcarriers in ϕ_k, i.e., $\mathbf{X}^{BS}_k(\mathbf{X}^{BS}_k)^H = \mathbf{I}_T$, and the received signal at the BS is given by:

$$\mathbf{Y}^{BS}_k = \mathbf{H}^{BS}_k \mathbf{X}^{BS}_k + \mathbf{W}^{BS}_k, \tag{3}$$

where $\mathbf{W}^{BS}_k$ is the complex Gaussian noise at the BS with zero mean and variance σ^2. By using the least squares (LS) estimation, the BS can obtain the estimation of $\mathbf{H}^{BS}_k$ by

$$\hat{\mathbf{H}}^{BS}_k = \mathbf{H}^{BS}_k + \mathbf{W}^{BS}_k(\mathbf{X}^{BS}_k)^H. \tag{4}$$

Similarly, in the downlink, the BS transmits the orthogonal pilot signal matrix $\mathbf{X}^{UT}_k \in \mathbb{C}^{T\times T}$ through subcarriers in ϕ_k, and the received signal at the k^{th} UT is given by:

$$\mathbf{Y}^{UT}_k = \mathbf{H}^{UT}_k \mathbf{X}^{UT}_k + \mathbf{W}^{UT}_k, \tag{5}$$

where $\mathbf{W}^{UT}_k$ is the complex Gaussian noise at the k^{th} UT with zero mean and variance σ^2_k. By using the LS estimation, the UT can obtain the estimation of $\mathbf{H}^{UT}_k$ as

$$\hat{\mathbf{H}}^{UT}_k = \mathbf{H}^{UT}_k + \mathbf{W}^{UT}_k(\mathbf{X}^{UT}_k)^H. \tag{6}$$

After traversing all UTs, we can obtain the channel matrices $\hat{\mathbf{H}}^{BS}_k$ and $\hat{\mathbf{H}}^{UT}_k$ between the BS and all K UTs. For the matrix $\hat{\mathbf{H}}^{\text{side}}_k \in \mathbb{C}^{N_k\times T}$, where side $\in \{BS, UT\}$, each row in the matrix is the measured values of the channel state of a subcarrier occupied by the k^{th} UT in T samples and is obtained from uplink/downlink channel probing.

3) Measurements-to-keys processing: Following subcarrier allocation and channel probing, the procedures of quantization, information reconciliation, and privacy amplification should be carried out to acquire the final secret keys. Similar methods are adopted in most PKG frameworks. In this paper, we mainly focus on the design of subcarrier allocation and channel probing, targeting improving the utilization efficiency of subcarriers as well as the security of the OFDMA system.

So far, the PKG scheme outputs the final secret keys, which can be utilized for applications such as encrypted transmission.

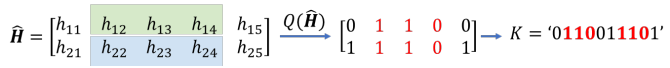

Fig. 3. Example of raw key generated by quantization.

IV. Necessity Analysis and Problem Formulation

In this section, we first answer the question of why an optimal subcarrier allocation scheme is needed from both practical and theoretical perspectives. Subsequently, we extend the model defined in Section III and formulate the subcarrier allocation problem as an optimization problem, which will be solved in Section V.

A. Why an Optimal Subcarrier Allocation Scheme Is Needed

In practical OFDMA systems, there are correlations between adjacent frequencies [22]. For UTs that occupy multiple subcarriers for key generation, strong correlation between different subcarriers leads to negative impacts on the performance of PKG.

1) Impact on the secret key rate: We present a simplified example to introduce why the frequency correlation affects the secret key rate. As portrayed in Fig. 3, the matrix $\hat{\mathbf{H}} \in \mathbb{C}^{2\times 5}$ is obtained by a UT with two subcarriers, the first and second rows are the CFR values of the two subcarriers at five time slots. When the frequencies of two subcarriers are close, the CFR values obtained by the two subcarriers at the same time have a high probability of being in the same quantization area. In other words, when the difference between h_{12} and h_{22} is small (though unequal), it is more likely that they fall into the same quantization area. Values within the same area mean they will be mapped to the same bit (0 or 1) after quantization. When this situation occurs in h_{12} and h_{22}, the quantized bit of h_{22} can be inferred from that of h_{12}. When this is not an isolated instance, it significantly reduces the randomness of the bit sequence. For example, in Fig. 3, if h_{12} and h_{22}, h_{13} and h_{23}, and h_{14} and h_{24} all have small differences and fall into the same quantization area, the key space of the quantized bit sequence reduces from 2^{10} to 2^7. It is worth noting that the purpose of information reconciliation and privacy amplification is to ensure the symmetry of the keys generated between communication parties and avoid information leakage. It will not have a significant impact on the characteristics of the raw key. Therefore, the correlation among the bits in the raw key will be retained in the final key, thereby compromising its randomness. If batches of final keys fail the NIST tests, they will be discarded and regenerated, leading to degraded secret key rate.

From the information theory perspective [29], the effective length of the binary bits (i.e., the raw key) extracted from a matrix is constrained by the entropy of the matrix. Many algorithms quantize matrix elements into fixed-length binary bits, yielding a raw key length strictly related to the matrix size. However, extracting a raw key from a low-entropy matrix results in additional length due to redundant information, thereby compromising randomness. Consequently, the randomness compromise in the raw key cascades to the final key, impairing its randomness as well.

2) Impact on randomness of generated keys: Randomness is an important property to ensure the unpredictability of keys. The NIST random test suite provides 15 tests, each of which evaluates randomness by returning a p-value based on its specific mathematical calculation and the sequence under test. When the p-value is larger than 0.01, the test can be considered passed. As analyzed above, the higher the correlation between subcarriers, the higher similarity the sequences obtained by their channel probing will be, i.e., the values between the corresponding rows in the matrix $\hat{\mathbf{H}}_k^{BS}$ will be closer. By analyzing the calculation process of all tests in the test suite, it can be found that several tests will be affected by frequency correlation, including: 1) Binary Matrix Rank Test. 2) Discrete Fourier Transform Test. 3) Serial Test. 4) Approximate Entropy Test. This observation will be verified in Subsection VI-B.

B. Problem Formulation

Considering the negative impact of frequency correlation on PKG, we formulate the subcarrier allocation problem as an optimization problem aiming to maximize the overall sum secret key rate of all UTs. The secret key rate is defined as an indicator that represents the length of effective keys and can be extracted from the common channel information obtained by channel probing. For the BS and the k^{th} UT, the secret key rate between them can be given by the conditional mutual information between $\hat{\mathbf{H}}_k^{BS}$, $\hat{\mathbf{H}}_k^{UT}$ and $\hat{\mathbf{H}}_e^{UT}$ as follows [7], [9], i.e.,

$$I_k = I(\hat{\mathbf{H}}_k^{BS}; \hat{\mathbf{H}}_k^{UT} | \hat{\mathbf{H}}_e^{UT}), \tag{7}$$

where $\hat{\mathbf{H}}_e^{UT}$ is an estimated channel matrix between the BS and Eve. Since Eve is not considered in our scheme (see Subsection III-A), the secret key rate degrades to

$$I_k = I(\hat{\mathbf{H}}_k^{BS}; \hat{\mathbf{H}}_k^{UT}). \tag{8}$$

By extending (8) in the same way as in [7], [8], [24], we obtain:

$$I_k = \log_2 \frac{\det(\hat{\mathbf{R}}_k^{BS}) \det(\hat{\mathbf{R}}_k^{UT})}{\det(\hat{\mathcal{R}}_k^{BU})}, \tag{9}$$

where $\hat{\mathbf{R}}_k^{BS}$ and $\hat{\mathbf{R}}_k^{UT}$ represent the covariance matrices of $\hat{\mathbf{H}}_k^{BS}$ and $\hat{\mathbf{H}}_k^{UT}$ respectively, and $\hat{\mathcal{R}}_k^{BU}$ represents the covariance of $\hat{\mathbf{H}}_k^{BS}$ and $\hat{\mathbf{H}}_k^{UT}$. In this paper, we assume the uplink and downlink channels have high reciprocity. Therefore, the relevant covariance matrices are then constructed using

$$\hat{\mathbf{R}}_k^{BS} = \mathbb{E}\{\hat{\mathbf{H}}_k^{BS}(\hat{\mathbf{H}}_k^{BS})^H\} = \mathbf{R}_k + \sigma^2\mathbf{I}, \tag{10}$$

$$\hat{\mathbf{R}}_k^{UT} = \mathbb{E}\{\hat{\mathbf{H}}_k^{UT}(\hat{\mathbf{H}}_k^{UT})^H\} = \mathbf{R}_k + \sigma_k^2\mathbf{I}, \tag{11}$$

$$\begin{aligned} \hat{\mathcal{R}}_k^{BU} &= \mathbb{E}\left\{ \begin{bmatrix} \hat{\mathbf{H}}_k^{BS} \\ \hat{\mathbf{H}}_k^{UT} \end{bmatrix} \begin{bmatrix} (\hat{\mathbf{H}}_k^{BS})^H & (\hat{\mathbf{H}}_k^{UT})^H \end{bmatrix} \right\} \\ &= \begin{bmatrix} \hat{\mathbf{R}}_k^{BS} & \mathbf{R}_k \\ \mathbf{R}_k & \hat{\mathbf{R}}_k^{UT} \end{bmatrix}, \end{aligned} \tag{12}$$

where

$$\mathbf{R}_k = \mathbb{E}\{\mathbf{H}_k(\mathbf{H}_k)^H\}, \tag{13}$$

$$\mathbf{H}_k = \mathbf{H}_k^{BS} = \mathbf{H}_k^{UT}. \tag{14}$$

To this end, substituting (10)-(14) into (9) results in the following expression:

$$I_k = \log_2 \frac{\det(\mathbf{R}_k + \sigma_k^2 \mathbf{I})}{\det(\mathbf{R}_k + \sigma_k^2 \mathbf{I} - \mathbf{R}_k(\mathbf{R}_k + \sigma^2 \mathbf{I})^{-1}\mathbf{R}_k)}. \quad (15)$$

Since matrix $\mathbf{R}_k$ is symmetric, we perform an eigenvalue decomposition on this matrix and obtain

$$\mathbf{R}_k = \mathbf{Q}_k \mathbf{\Lambda}_k (\mathbf{Q}_k)^H, \quad (16)$$

where $\mathbf{Q}_k$ is a unitary matrix, i.e., $\mathbf{Q}_k(\mathbf{Q}_k)^H = \mathbf{I}$, and each column vector in $\mathbf{Q}_k$ is an eigenvector of $\mathbf{R}_k$. $\mathbf{\Lambda}_k$ is a diagonal matrix, with each element on the diagonal being an eigenvalue of $\mathbf{R}_k$ and corresponding one-to-one with the column vectors in $\mathbf{Q}_k$. The elements on the diagonal of $\mathbf{\Lambda}_k$ are defined as λ_{ki} ($\lambda_{k1} \geq \lambda_{k2} \geq \cdots \geq \lambda_{kN_k}$). Then (15) can be recalculated as:

$$\begin{aligned} I_k &= \log_2 \frac{\det(\mathbf{\Lambda}_k + \sigma_k^2 \mathbf{I})}{\det(\mathbf{\Lambda}_k + \sigma_k^2 \mathbf{I} - \mathbf{\Lambda}_k(\mathbf{\Lambda}_k + \sigma^2 \mathbf{I})^{-1}\mathbf{\Lambda}_k)} \\ &= \log_2 \prod_{i=1}^{N_k} \left(\frac{\lambda_{ki} + \sigma_k^2}{\lambda_{ki} + \sigma_k^2 - \lambda_{ki}(\lambda_{ki} + \sigma^2)^{-1}\lambda_{ki}} \right) \\ &= \sum_{i=1}^{N_k} \log_2 \frac{\lambda_{ki} + \sigma_k^2}{\lambda_{ki} + \sigma_k^2 - \frac{\lambda_{ki}^2}{\lambda_{ki} + \sigma^2}} \\ &= \sum_{i=1}^{N_k} \log_2 \left(1 + \frac{\lambda_{ki}^2}{(\sigma_k^2 + \sigma^2)\lambda_{ki} + \sigma_k^2 \sigma^2} \right). \end{aligned} \quad (17)$$

Remark 1. *From* (17)*, it is seen that I_k is related to $\{\lambda_{ki} | 1 \leq i \leq N_k\}$, i.e., the eigenvalues of $\mathbf{R}_k$. We can further analyze* (17) *as*

$$I_k = \log_2 \prod_{i=1}^{N_k} (1 + u(\lambda_{ki})), \quad (18)$$

where

$$u(\lambda_{ki}) = \frac{\lambda_{ki}^2}{(\sigma_k^2 + \sigma^2)\lambda_{ki} + \sigma_k^2 \sigma^2}. \quad (19)$$

One can see that I_k increases for larger $\prod_{i=1}^{N_k}(1 + u(\lambda_{ki}))$. When the sum of the eigenvalues of $\mathbf{R}_k$ is finite, i.e.,

$$\sum_{i=1}^{N_k} \lambda_{ki} \leq C, \quad (20)$$

where C can be any constant. One can see that a more uniform distribution of the eigenvalues contributes to a larger $u(\lambda_{k1}, \cdots, \lambda_{kN_k})$. Next, we explain this using the Lagrange multiplier method. First, we construct the Lagrange function using (18)-(20) *as follows:*

$$L(\lambda_{k1}, \cdots, \lambda_{kN_k}, \lambda) = \prod_{i=1}^{N_k} (1 + u(\lambda_{ki})) + \lambda(C - \sum_{i=1}^{N_k} \lambda_{ki}), \quad (21)$$

where λ is the Lagrange multiplier. Taking the partial derivative of the Lagrange function with respect to $\lambda_{k1}, \cdots, \lambda_{kN_k}$ and equating it to zero, we have the following optimality condition:

$$u^{'}(\lambda_{ki}) \prod_{j \neq i}^{N_k} (1 + u(\lambda_{kj})) = \lambda, \forall i, \quad (22)$$

where $u^{'}(\lambda_{ki})$ is the first-order derivative of $u(\lambda_{ki})$. We can obtain the first-order and second-order derivatives as follows:

$$u^{'}(\lambda_{ki}) = \frac{(\sigma_k^2 + \sigma^2)\lambda_{ki}^2 + 2\sigma_k^2 \sigma^2 \lambda_{ki}}{((\sigma_k^2 + \sigma^2)\lambda_{ki} + \sigma_k^2 \sigma^2)^2} \geq 0, \quad (23)$$

$$u^{''}(\lambda_{ki}) = \frac{2(\sigma_k^2 \sigma^2)^2}{((\sigma_k^2 + \sigma^2)\lambda_{ki} + \sigma_k^2 \sigma^2)^3} \geq 0. \quad (24)$$

Therefore, when $\lambda_{ki} \neq \lambda_{kj}$, then $u(\lambda_{ki}) \neq u(\lambda_{kj})$, and the optimality condition of $L(\lambda_{k1}, \cdots, \lambda_{kN_k}, \lambda)$ simplifies to

$$\lambda_{k1} = \cdots = \lambda_{kN_k}. \quad (25)$$

Recall from Subsection III-C that an optimal subcarrier allocation requires security requirement satisfaction, sum rate maximization, and secret key effectiveness. To this end, we adopt the secret key rate to quantify the length of effective keys and formulate the problem with the objective of maximizing the sum secret key rate whilst satisfying the security constraints of all UTs. The optimization problem is formulated as

$$\begin{aligned} \textbf{(\#P1)}: \max_{\mathbf{\Phi}} \quad & \sum_{k=1}^{K} \sum_{i=1}^{N_k} p(\lambda_{ki}) && \text{(26a)} \\ \text{subject to} \quad & \\ & \boldsymbol{\phi}_k \cap \boldsymbol{\phi}_{k'} = \emptyset,\ 1 \leq k, k' \leq K,\ k \neq k' && \text{(26b)} \\ & \boldsymbol{\phi}_1 \cup \boldsymbol{\phi}_2 \cdots \cup \boldsymbol{\phi}_K \subseteq \mathbf{\Phi} && \text{(26c)} \\ & I_k \geq \Re_k, 1 \leq k \leq K, && \text{(26d)} \end{aligned}$$

where

$$p(\lambda_{ki}) = \log_2 \left(1 + \frac{\lambda_{ki}^2}{(\sigma_k^2 + \sigma^2)\lambda_{ki} + \sigma_k^2 \sigma^2} \right). \quad (27)$$

V. Problem Analysis and Algorithm Design

In this section, we first analyze the challenges in solving the problem **(#P1)** and show that it is NP-hard, meaning that it cannot be solved in polynomial time. Next, we design a low-complexity algorithm that can efficiently solve **(#P1)**, at the price of providing only a near-optimal solution.

A. The Challenge of Solving Problem *(#P1)*

First, we prove the problem **(#P1)** is NP-hard.

Theorem 1. *The problem (#P1) is NP-hard.*

Proof. We can prove that **(#P1)** is NP-Hard by showing that it can be reduced from a known NP-complete problem.

Transform problem **(#P1)** into an equivalent form as follows:

$$\textbf{(\#P2)}: \max \quad \sum_{k=1}^{K}\sum_{n=1}^{N} x_{kn} p(\lambda_{kn}) \tag{28a}$$

subject to

$$\sum_{k=1}^{K} x_{kn} \le 1,\ 1 \le n \le N \tag{28b}$$

$$\sum_{n=1}^{N} x_{kn} \le N,\ 1 \le k \le K \tag{28c}$$

$$x_{kn} \in \{0,1\},\ 1 \le k \le K,\ 1 \le n \le N \tag{28d}$$

$$\sum_{n=1}^{N} x_{kn} p(\lambda_{kn}) \ge \Re_k,\ 1 \le k \le K, \tag{28e}$$

where $x_{kn} = 1$ if the n^{th} subcarrier is allocated to the k^{th} UT and zero otherwise.

When we set all the $\Re_k$ values in constraint (28e) to zero, one can see that problem **(#P2)** is transformed into a form of multiple knapsack problems (MKP) [30], implying that MKP is reducible to **(#P2)**. In addition, MKP is also one of Karp's 21 NP-complete problems [31]. Thus, this completes the proof. □

If we attempt all possible allocation policies, perform channel probing for each policy, and calculate the corresponding sum secret key rate, it may result in prohibitively high computational overhead. More precisely, assuming that all subcarriers are identical and indistinguishable, the number of policies for allocating N subcarriers to K UTs can be computed using the "stars and bars" method in combinatorics, yielding:

$$\mathrm{C}_{N-1}^{K-1} = \frac{(N-1)!}{(K-1)!(N-K)!} = \frac{\prod_{i=1}^{N-1} i}{\left(\prod_{j=1}^{K-1} j\right)\left(\prod_{k=1}^{N-K} k\right)}. \tag{29}$$

Next, consider the distinctiveness among subcarriers and calculate the number of allocation policies given the number of subcarriers assigned to each UT. That is, assuming in the i^{th} case, the number of subcarriers allocated to K UTs is known as $\{N_{i,k}, \forall k\}$, and the calculation result can be obtained as $\mathrm{C}_{N}^{N_{i,1}} \cdot \mathrm{C}_{N-N_{i,1}}^{N_{i,2}} \cdots \mathrm{C}_{N-\sum_{j=1}^{K-1} N_{i,j}}^{N_{i,K}}$. Therefore, the number of all possible allocation policies can be calculated as

$$\begin{aligned}\mathrm{Num}_{\mathrm{all}} &= \sum_{i=1}^{\mathrm{C}_{N-1}^{K-1}} \mathrm{C}_{N}^{N_{i,1}} \cdot \mathrm{C}_{N-N_{i,1}}^{N_{i,2}} \cdots \mathrm{C}_{N-\sum_{j=1}^{K-1} N_{i,j}}^{N_{i,K}} \\ &= \sum_{i=1}^{\frac{(N-1)!}{(K-1)!(N-K)!}} \frac{N!}{N_{i,1}! \cdots N_{i,K}! (N-\sum_{j=1}^{K} N_{i,j})!}.\end{aligned} \tag{30}$$

Since the calculation of combinations involves factorial operations, $\mathrm{Num}_{\mathrm{all}}$ grows super-exponentially with N. In addition, UTs need to perform channel probing according to each policy, calculate and compare the sum secret key rates of different policies, which resulting in unacceptable time and computational overhead. Therefore, it is not feasible to traverse all potential allocation policies to find the optimal solution of **(#P1)**.

B. Analysis of Frequency Correlation

In order to design an efficient algorithm with low complexity for problem solving, let us start with the mathematical characteristics of frequency correlation first.

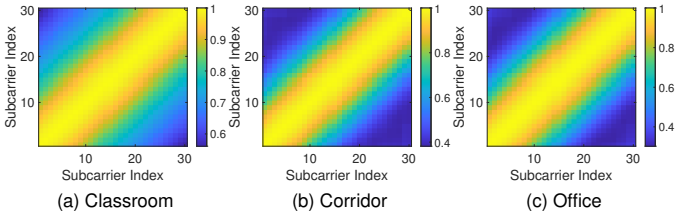

Fig. 4. Correlation matrix calculated based on Widar2.0 data set.

Let matrix $\mathbf{P}_k \in \mathbb{C}^{N_k \times N_k}$ record the correlation coefficients between subcarriers occupied by the k^{th} UT. The element in the i^{th} row and j^{th} column of $\mathbf{P}_k$ represent the correlation coefficient of channel information between subcarriers $\phi_k(i)$ and $\phi_k(j)$, which is quantified by the modulus of Pearson correlation coefficient[1]. The form of matrix $\mathbf{P}_k$ can be given as (31), as shown at the bottom of the next page. Since the matrix $\mathbf{P}_k$ is symmetric, we next analyze the situation where $j > i$.

The Pearson correlation coefficient between the i^{th} and j^{th} subcarriers occupied by the k^{th} UT can be calculated as:

$$\rho(\mathbf{h}_{k,n_i}^{\mathrm{side}}, \mathbf{h}_{k,n_j}^{\mathrm{side}}) = \frac{\Gamma(\mathbf{h}_{k,n_i}^{\mathrm{side}}, \mathbf{h}_{k,n_j}^{\mathrm{side}})}{\sigma(\mathbf{h}_{k,n_i}^{\mathrm{side}})\sigma(\mathbf{h}_{k,n_j}^{\mathrm{side}})}, \tag{32}$$

where side $\in \{BS, UT\}$. According to the definitions of covariance and standard deviation, substitute (2) we can get

$$\Gamma(\mathbf{h}_{k,n_i}^{\mathrm{side}}, \mathbf{h}_{k,n_j}^{\mathrm{side}}) = \mathbb{E}\{(\mathbf{h}_{k,n_i}^{\mathrm{side}})^H \mathbf{h}_{k,n_j}^{\mathrm{side}}\} - \mathbb{E}\{\mathbf{h}_{k,n_i}^{\mathrm{side}}\}^H \mathbb{E}\{\mathbf{h}_{k,n_j}^{\mathrm{side}}\}, \tag{33}$$

$$\sigma(\mathbf{h}_{k,n_i}^{\mathrm{side}}) = \sqrt{\frac{\sum_{t=1}^{T}(\sum_{l=1}^{L} h_k^{\mathrm{side}}(\tau_l, t) e^{-j2\pi f_{n_i}\tau_l} - \mathbb{E}\{\mathbf{h}_{k,n_i}^{\mathrm{side}}\})^2}{T-1}}, \tag{34}$$

$$\sigma(\mathbf{h}_{k,n_j}^{\mathrm{side}}) = \sqrt{\frac{\sum_{t=1}^{T}(\sum_{l=1}^{L} h_k^{\mathrm{side}}(\tau_l, t) e^{-j2\pi f_{n_j}\tau_l} - \mathbb{E}\{\mathbf{h}_{k,n_j}^{\mathrm{side}}\})^2}{T-1}}, \tag{35}$$

$$\mathbb{E}\{(\mathbf{h}_{k,n_i}^{\mathrm{side}})^H \mathbf{h}_{k,n_j}^{\mathrm{side}}\} = \frac{1}{T}\sum_{t=1}^{T}\sum_{l=1}^{L} (h_k^{\mathrm{side}}(\tau_l, t))^2 e^{-j2\pi\Delta f \tau_l}, \tag{36}$$

$$\mathbb{E}\{\mathbf{h}_{k,n_i}^{\mathrm{side}}\} = \frac{1}{T}\sum_{t=1}^{T}\sum_{l=1}^{L} h_k^{\mathrm{side}}(\tau_l, t) e^{-j2\pi f_{n_i}\tau_l}, \tag{37}$$

$$\mathbb{E}\{\mathbf{h}_{k,n_j}^{\mathrm{side}}\} = \frac{1}{T}\sum_{t=1}^{T}\sum_{l=1}^{L} h_k^{\mathrm{side}}(\tau_l, t) e^{-j2\pi f_{n_j}\tau_l}, \tag{38}$$

$$\Delta f = f_{n_j} - f_{n_i} = (n_j - n_i)\cdot\frac{B}{N}, j > i. \tag{39}$$

[1]Generally, the Pearson coefficient is used to measure the correlation between two variables. Considering that the Pearson coefficient of channel information between subcarriers is a complex number, we take its modulus to measure the similarity more intuitively.

Considering that the expression of $|\rho(\mathbf{h}_{k,n_i}^{\text{side}}, \mathbf{h}_{k,n_j}^{\text{side}})|$ is too complex, it is difficult for us to analyze the influence of the frequency spacing by deriving the first-order derivative and the second-order derivative of the expression with respect to the frequency spacing. To this end, we perform an analysis of actual channel data instead of theoretical derivation.

We use the open source Widar2.0 [32] data set for analysis, which provides CSI data received by a WiFi device with three antennas in three scenarios: a large empty classroom, a narrow corridor and a small office room with various furniture [32]. The data set provides the CSI of the receiving device on 30 subcarriers. We first obtain the corresponding correlation matrix based on the correlation of different subcarriers according to (31)-(39), which is plotted in Fig. 4. Comparing the correlation coefficient values in Fig. 4a-4c at the same subcarrier frequency spacing, calculated by (32), we can find that the coefficients of the classroom are the largest. This is because in a more empty environment, the multipath effect is less significant, the delay spread is smaller, and the coherence bandwidth is larger, leading to a slower decrease in subcarrier correlation with increasing frequency spacing. Next, we take four sets of data[2] collected by different trajectories from the three scenarios and draw the variation curve of the correlation coefficient with the frequency spacing[3], as shown in Fig. 5. Through Fig. 4 and Fig. 5, we can get two empirical observations: i) The frequency correlation coefficient decreases as the frequency spacing between subcarriers increases; ii) The rate of decrease in coefficient diminishes as the frequency spacing between subcarriers increases. From a mathematical perspective, the first-order derivative of the frequency correlation coefficient with respect to the frequency spacing is negative, while the second-order derivative is positive, so the rate of coefficient reduction is constantly decreasing.

C. Problem Solving: A Near-Optimal Algorithm

Taking into account of the challenge of problem solving (as discussed in Subsection V-A) and the analysis of frequency correlation characteristics (as discussed in Subsection V-B), we design a low-complexity algorithm for efficient near-optimal problem solving.

From **Remark** 1, we observe that I_k can be maximized when $\{\lambda_{ki}\}$ is uniformly distributed. Since $\{\lambda_{ki}\}$ represents the eigenvalues of matrix $\mathbf{R}_k$, this implies that I_k is maximized when the condition number of $\mathbf{R}_k$ is smallest. The condition number of $\mathbf{R}_k$ is defined as the ratio of its maximum singular value to its minimum singular value. Given that $\mathbf{R}_k = \mathbb{E}\{\mathbf{H}_k(\mathbf{H}_k)^H\}$, the singular values of $\mathbf{R}_k$ are the eigenvalues of $\mathbf{H}_k$. Therefore, when the condition number of matrix $\mathbf{H}_k$ is smaller, I_k can achieve a larger value. From a linear algebra perspective, if the row vectors of $\mathbf{H}_k$ have high similarity (i.e., stronger correlation among the subcarriers occupied by the k^{th} UT), it will result in an uneven distribution of the eigenvalues, leading to a larger condition number for $\mathbf{R}_k$. To this end, to maximize I_k, it is desirable to minimize the correlation among the subcarriers occupied by each UT. In other words, for each UT, the sum of correlation coefficients among subcarriers should be minimized. Next, we prove that the policy of uniformly allocating subcarriers can minimize the sum of correlation coefficients.

Theorem 2. *When selecting N_k subcarriers from N subcarriers to allocate to the k^{th} UT, choosing the N_k subcarriers with a maximized uniformly distributed frequency spacing is the optimal solution.*

Proof. Reviewing the two empirical conjectures mentioned in Subsection V-B, we can abstract a function $\text{Coef}(\Delta f)$ to characterize the relationship between correlation coefficients and subcarrier frequency spacing, where $\Delta f = f_{n_j} - f_{n_i} = (n_j - n_i) \cdot \frac{B}{N}, j > i$, and n_i and n_j represent the indices of the subcarriers occupied by the UT. As $\frac{B}{N}$ is a constant, we use $\text{Coef}(\Delta n)$ instead of $\text{Coef}(\Delta f)$ for analysis, where $\Delta n = (n_j - n_i)$. Furthermore, the first-order derivative $\text{Coef}^{'}(\Delta n)$ is always less than 0, and the second-order derivative $\text{Coef}^{''}(\Delta n)$ is always greater than 0. Our goal is to minimize the sum of correlation coefficients, i.e.

$$\min \sum_{i=1}^{N_k-1} \text{Coef}(n_{i+1} - n_i). \tag{40}$$

As $\text{Coef}(\Delta n)$ is monotonically decreasing, maximizing the frequency spacing is a necessary choice, and therefore, assigning the first and last subcarriers is required. Moreover, we can easily observe that $(n_2 - n_1), \cdots, (n_{N_k} - n_{N_k-1})$ have a complementary relationship, i.e., an increase in one term will inevitably lead to a decrease in the sum of all other terms, because

$$\begin{aligned} \sum_{i=1}^{N_k-1} n_{i+1} - n_i &= (n_2 - n_1) + \cdots + (n_{N_k} - n_{N_k-1}) \\ &= n_{N_k} - n_1 \leq N - 1, \end{aligned} \tag{41}$$

[2]Each scene in the Widar data set contains multiple sets of data, where different sets of data are obtained under different motion trajectories. Considering the space limit of the paper, we only draw the results of four sets of data processing for each scenario. However, the main characteristics of different sets of data are similar and do not affect the analysis results of this article.

[3]According to (39), the frequency spacing is proportional to the difference in subcarrier index. For ease of expression, the label on the horizontal axis in Fig. 5 uses the difference in subcarrier index to replace the indices.

$$\mathbf{P}_k = \begin{bmatrix} 1 & |\rho(\mathbf{h}_{k,n_1}^{\text{side}}, \mathbf{h}_{k,n_2}^{\text{side}})| & \cdots & |\rho(\mathbf{h}_{k,n_1}^{\text{side}}, \mathbf{h}_{k,n_{N_k}}^{\text{side}})| \\ |\rho(\mathbf{h}_{k,n_2}^{\text{side}}, \mathbf{h}_{k,n_1}^{\text{side}})| & 1 & \cdots & |\rho(\mathbf{h}_{k,n_2}^{\text{side}}, \mathbf{h}_{k,n_{N_k}}^{\text{side}})| \\ \vdots & \vdots & \ddots & \vdots \\ |\rho(\mathbf{h}_{k,n_{N_k}}^{\text{side}}, \mathbf{h}_{k,n_1}^{\text{side}})| & |\rho(\mathbf{h}_{k,n_{N_k}}^{\text{side}}, \mathbf{h}_{k,n_2}^{\text{side}})| & \cdots & 1 \end{bmatrix}. \tag{31}$$

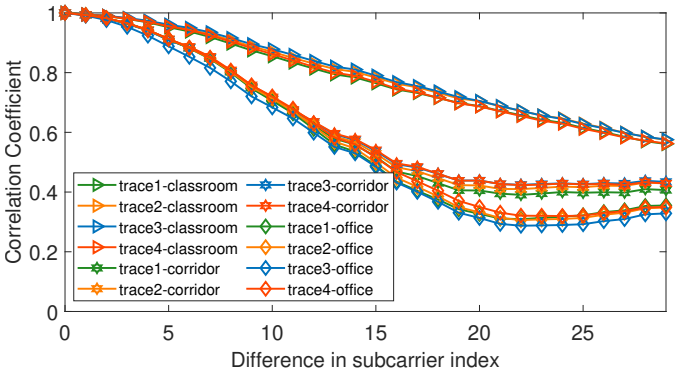

Fig. 5. Frequency correlation coefficient under different frequency spacing.

when choosing the first and last subcarriers, the inequality in (41) becomes an equality.

Therefore, in choosing the remaining N_k-2 subcarriers, we are faced with trade-offs. Let $\Delta a_i = (n_{i+1} - n_i) - \overline{n}$, where $\overline{n} = \frac{N-1}{N_k-1}$ is the average interval of subcarrier indices, and the sum of the correlation coefficients is

$$\begin{aligned}\sum_{i=1}^{N_k-1} \mathrm{Coef}(n_{i+1}-n_i) &= \sum_{i=1}^{N_k-1} \mathrm{Coef}(\overline{n}+\Delta a_i) \\ &= (N_k-1)\mathrm{Coef}(\overline{n}) + \sum_{i=1}^{N_k-1}\int_{\overline{n}}^{\overline{n}+\Delta a_i} \mathrm{Coef}^{'}(x)dx,\end{aligned} \tag{42}$$

when $\Delta a_i > 0$, $\mathrm{Coef}^{'}(\overline{n}) < \mathrm{Coef}^{'}(\overline{n}+\Delta a_i) < 0$; when $\Delta a_i < 0$, $\mathrm{Coef}^{'}(\overline{n}+\Delta a_i) < \mathrm{Coef}^{'}(\overline{n}) < 0$. In addition, according to (41), $\sum_{i=1}^{N_k-1}(\overline{n}+\Delta a_i) \le N-1$, i.e., $\sum_{i=1}^{N_k-1}\Delta a_i \le 0$, hence

$$\sum_{i=1}^{N_k-1}\int_{\overline{n}}^{\overline{n}+\Delta a_i} \mathrm{Coef}^{'}(x)dx \ge 0. \tag{43}$$

Therefore,

$$\sum_{i=1}^{N_k-1} \mathrm{Coef}(n_{i+1}-n_i) \ge (N_k-1)\mathrm{Coef}(\overline{n}), \tag{44}$$

the equality holds only when $\Delta a_1 = \cdots = \Delta a_{N_k-1} = 0$.

Thus, this completes the proof, and **Theorem** 2 follows. □

Our algorithm can be divided into two stages: i) According to **Theorem** 2 and the security requirement $\{\Re_k\}$, determine how many subcarriers are needed for each UT to satisfy Constraint (26d). ii) After satisfying the security requirements of all UTs, allocate the remaining subcarriers by means of a greedy-based policy to maximize the secret key rate.

Stage 1: Before the algorithm starts, set $\boldsymbol{\phi}_k$ as an empty set and N_k as zero for $k = 1, \cdots, K$. For ease of algorithm description, denote $\boldsymbol{\phi}_0$ as an empty set and N_0 as zero. For the k^{th} UT, let $begin = 0$ and $end = N - \sum_{i=0}^{k-1} N_i$, and perform the following steps.

- **Step 1:** Update N_k with the value $\lfloor \frac{(begin+end)}{2} \rfloor$, and based on **Theorem** 2, select N_k subcarriers uniformly from $\boldsymbol{\Phi}\backslash(\cup_{i=1}^{k-1}\boldsymbol{\phi}_i)$ to construct $\boldsymbol{\phi}_k$.
- **Step 2:** Perform channel probing on the subcarriers in $\boldsymbol{\phi}_k$ by both the BS and the k^{th} UT to obtain $\hat{\mathbf{H}}_k^{BS}$ and $\hat{\mathbf{H}}_k^{UT}$.
- **Step 3:** Calculate I_k using (10)-(17) and compare the relationship between I_k and $\Re_k$. If $I_k > \Re_k$, then $end = N_k - 1$; else if $I_k < \Re_k$, then $begin = N_k + 1$.
- **Step 4:** Return to **Step 1** until $begin > end$ or $I_k = \Re_k$.

All K UTs perform the above four steps to obtain preliminary results of N_k and $\boldsymbol{\phi}_k$ that can satisfy Constraint (26d). Recalculate I_k for all UTs. If $\exists k, I_k < \Re_k$, it indicates that the system resources are insufficient to meet the security requirements of all UTs. In this case, the algorithm terminates. Otherwise, proceed to **Stage 2**.

Stage 2: Select allocation objects for the remaining subcarriers (i.e., the subcarriers in $\boldsymbol{\Phi}\backslash(\cup_{k=1}^{K}\boldsymbol{\phi}_k)$). We define the distance from a subcarrier to $\boldsymbol{\phi}_k$ as the distance between the subcarrier and the most adjacent subcarrier in $\boldsymbol{\phi}_k$, and it is represented by $d_{ik} = \min_{j\in\boldsymbol{\phi}_k} |i-j|$. Then, for each subcarrier $i \in \boldsymbol{\Phi}\backslash(\cup_{k=1}^{K}\boldsymbol{\phi}_k)$, calculate its distance d_{ik}, and the allocation object is given by

$$k_i^* = \arg\max_k d_{ik}, \quad \text{for } k = 1, \cdots, K. \tag{45}$$

Next, append subcarrier i to $\boldsymbol{\phi}_{k_i^*}$ and $N_{k_i^*} = N_{k_i^*} + 1$. So far, the final subcarrier allocation policy has been obtained.

The workflow introduced above can be summarized as **Algorithm** 1.

D. Algorithm Analysis

The near-optimal algorithm has made a small compromise in optimality in exchange for feasibility in terms of time efficiency. Next, we answer the following two questions: (1) Why such an algorithm can achieve near-optimal; (2) Does such an algorithm address the challenge mentioned in Subsection V-A and achieve acceptable time and computational overhead.

1) Why such an algorithm can achieve near-optimal: In Stage 1, we use **Theorem** 2 and binary search to approximate the minimum number of subcarriers that can meet the security requirement $\{\Re_k\}$. Due to the optimality of **Theorem** 2, we believe that Stage 1 can optimally achieve its objective. In Stage 2, since a greedy-based approach is adopted for reallocating the remaining subcarriers, it only guarantees local optimality without proving its global optimality. For this reason, the algorithm is called near-optimal.

2) Does such an algorithm address the challenge: The challenge mentioned in Subsection V-A is the potentially vast number of policies, which would lead to unacceptable time and computational overhead. Fortunately, our near-optimal algorithm effectively addresses this challenge. Specifically, in Stage 1, each UT matches the minimum number of subcarriers satisfying $\{\Re_k\}$ through binary search, and the number of potential policies that k^{th} UT needs to perform is $\log_2(N - \sum_{i=1}^{k-1} N_i)$. In Stage 2, the solution is uniquely determined. Therefore, the number of potential policies that the near-optimal algorithm needs to explore is

$$\mathrm{Num}_{\mathrm{our}} = \sum_{k=1}^{K} \log_2(N - \sum_{i=1}^{k-1} N_i) < K\log_2 N, \tag{46}$$

Algorithm 1: A Near-Optimal Algorithm for Solving Optimization Problem **(#P1)**

Data: K, N, $\{\Re_k\}$, $\mathbf{\Phi}$
Result: $\{N_k\}$, $\{\boldsymbol{\phi}_k\}$

$N_0 \leftarrow 0, \boldsymbol{\phi}_0 \leftarrow \emptyset$;
for $k \leftarrow 1$ **to** K **do**
  $begin \leftarrow 0, end \leftarrow N - \sum_{i=0}^{k-1} N_i$;
  $I_k \leftarrow 0$;
  while $begin \leq end$ && $I_k \neq \Re_k$ **do**
    $N_k \leftarrow \lfloor \frac{(begin+end)}{2} \rfloor$;
    // select_from_set($\boldsymbol{A}, n$) is to select n subcarriers from $\boldsymbol{A}$ uniformly.
    $\boldsymbol{\phi}_k \leftarrow$ select_from_set($\mathbf{\Phi} \backslash (\cup_{i=1}^{k-1} \boldsymbol{\phi}_i), N_k$);
    Perform channel probing to obtain $\hat{\mathbf{H}}_k^{BS}$, $\hat{\mathbf{H}}_k^{UT}$;
    Calculate I_k according to (10)-(17);
    if $I_k > \Re_k$ **then**
      $end \leftarrow N_k - 1$;
    else
      $begin \leftarrow N_k + 1$;
  for $k \leftarrow 1$ **to** K **do**
    if $I_k < C_k$ **then**
      return False;
for $i \in \mathbf{\Phi} \backslash (\cup_{k=1}^{K} \boldsymbol{\phi}_k)$ **do**
  for $k \leftarrow 1$ **to** K **do**
    $d_{ik} \leftarrow \min_{j \in \boldsymbol{\phi}_k} |i - j|$;
  $k_i^* \leftarrow \arg\max_k d_{ik}$;
  $\boldsymbol{\phi}_{k_i^*} \leftarrow \boldsymbol{\phi}_{k_i^*} \cup i$;
  $N_{k_i^*} \leftarrow N_{k_i^*} + 1$;
return True;

and can be limited to $O(K \log_2 N)$. Compared to $\mathrm{Num}_{\mathrm{all}}$ in (30), it is almost negligible. To this end, the near-optimal algorithm can obtain a suitable allocation policy in a short time and without excessive computational overhead.

VI. Performance Evaluation

In this section, we provide simulation results to illustrate the performance of the proposed optimal subcarrier allocation scheme.

A. Simulation Settings

We utilize QuaDRiGa [33], [34] to establish a simulation model of OFDMA, and the detailed configuration parameters are shown in Table I. Then, we implemented the PKG framework with our optimal subcarrier allocation scheme using MATLAB. We focus on the urban-macro and non line-of-sight (NLOS) scenario. It's worth noting that the optimal subcarrier allocation scheme proposed in this paper is applicable for key generation in all OFDMA networks, not limited to the scenario adopted in our experiments.

TABLE I
Configuration parameters

Parameter	Value
Scenario	Urban-macro NLoS
Path number	14
Number of UTs	16
Moving speed	1.25 m/s
Center frequency	3.5 GHz
Subcarrier number	624
Subcarrier spacing	15 kHz

To the extent of our knowledge, none of the existing works has proposed an effective solution on how to allocate subcarriers for PKG in OFDMA multi-user systems and did not present their subcarrier allocation schemes. Therefore, we employ the commonly used continuous subcarrier allocation algorithm and random subcarrier allocation algorithm as comparison methods to evaluate the performance of the proposed near-optimal algorithm in our scheme. Each algorithm can be divided into two stages. In Stage 1, subcarriers are allocated to the k^{th} UT until $I_k \geq \Re_k$. The former continuously allocates subcarriers, while the latter allocates them randomly. This process is repeated for the next UT until either the subcarriers are exhausted or all UTs have been processed. In Stage 2, the remaining subcarriers are allocated to the UTs. The former uniformly allocates the remaining subcarriers among all UTs, while the latter iteratively traverses and randomly allocates each of the remaining subcarriers to a certain UT. Their pseudo codes are shown in **Algorithm** 2 and **Algorithm** 3.

Algorithm 2: The Continuous Subcarrier Allocation Algorithm

Data: K, N, $\{\Re_k\}$, $\mathbf{\Phi}$
Result: $\{N_k\}$, $\{\boldsymbol{\phi}_k\}$

$i \leftarrow 1$;
for $k \leftarrow 1$ **to** K **do**
  while $I_k < \Re_k$ **do**
    if $i > N$ **then**
      return False;
    $\boldsymbol{\phi}_k \leftarrow \boldsymbol{\phi}_k \cup i$;
    $N_k \leftarrow N_k + 1$;
    Perform channel probing to obtain $\hat{\mathbf{H}}_k^{BS}$, $\hat{\mathbf{H}}_k^{UT}$;
    Calculate I_k according to (10)-(17);
    $i \leftarrow i + 1$;
$j \leftarrow \frac{N-(i-1)}{K}$;
for $k \leftarrow 1$ **to** K **do**
  $\boldsymbol{\phi}_k \leftarrow \boldsymbol{\phi}_k \cup \{i, \cdots, i + (j-1)\}$;
  $i \leftarrow i + j$;
return True;

Obtaining the optimal solution poses challenges in terms of extensive computational resources and time costs (as discussed in Subsection V-A). To this end, we establish an optimal upper bound to replace the optimal solution. This upper bound is the sum secret key rate derived using **Theorem** 2 when all $\{\Re_k\}$ are set to zero. In other words, it represents the optimal

Algorithm 3: The Random Subcarrier Allocation Algorithm

Data: K, N, $\{\Re_k\}$, $\mathbf{\Phi}$
Result: $\{N_k\}$, $\{\boldsymbol{\phi}_k\}$

$\boldsymbol{\phi}_0 \leftarrow \emptyset$;
for $k \leftarrow 1$ **to** K **do**
  while $I_k < \Re_k$ **do**
    if $\mathbf{\Phi} \backslash (\cup_{i=1}^{k-1} \boldsymbol{\phi}_i)$ *is* $\emptyset$ **then**
      return False;
    // random_from_set($\boldsymbol{A}$) is to select a subcarrier from set $\boldsymbol{A}$ randomly.
    $index = \text{random\_from\_set}(\mathbf{\Phi} \backslash (\cup_{i=1}^{k-1} \boldsymbol{\phi}_i))$;
    $\boldsymbol{\phi}_k \leftarrow \boldsymbol{\phi}_k \cup index$;
    $N_k \leftarrow N_k + 1$;
    Perform channel probing to obtain $\hat{\mathbf{H}}_k^{BS}$, $\hat{\mathbf{H}}_k^{UT}$;
    Calculate I_k according to (10)-(17);
for $j \in \mathbf{\Phi} \backslash (\cup_{k=1}^{K} \boldsymbol{\phi}_k)$ **do**
  $k_j^* \leftarrow \text{random\_from\_set}(\{1, \cdots, K\})$;
  $\boldsymbol{\phi}_{k_j^*} \leftarrow \boldsymbol{\phi}_{k_j^*} \cup j$;
  $N_{k_j^*} \leftarrow N_{k_j^*} + 1$;
return True;

solution obtained by uniformly allocating all subcarriers to all UTs, where the k^{th} UT is assigned subcarriers $\{k + K \cdot r | 0 \leq r \leq \frac{N}{K} - 1\}$. We denote the optimal upper bound as Total, and define multiple sets of $\{\Re_k\}$. The initialization method of each $\{\Re_k\}$ is as follows:

$$\text{sum}_{\Re} = \text{Total} \times X, \tag{47}$$

$$\Re_k = \text{Random}(\text{sum}_{\Re} - \sum_{i=1}^{k-1} \Re_i), \tag{48}$$

where $X \in [0, 1]$, and $\text{Random}(n_{\max})$ is a function to return a random number between 0 and $n_{\max}$.

B. Simulation Results

First, we evaluate the performance of different algorithms in maximizing the sum secret key rate when system resources are abundant (i.e., the situations where all algorithms can easily satisfy all security requirements and fully execute Stage 2). Fig. 6 compares the sum secret key rate of different algorithms for multiple groups of $\{\Re_k\}$. From the results, we can observe that when the system resources are abundant, each algorithm maintains stable performance in the face of different $\{\Re_k\}$ (i.e., the performance of each algorithm in Fig. 6a-6d is similar). Moreover, the performance of the near-optimal algorithm significantly outperforms the random subcarrier allocation algorithm and the continuous subcarrier allocation algorithm. For example, when $X = \{10\%, 20\%, 30\%, 40\%\}$ and SNR ranges from 0 to 30 dB, the sum secret key rate of the near-optimal algorithm is on average 9.93% and 43.9% higher than that of the continuous allocation algorithm and the random allocation algorithm respectively. It is noting that the random subcarrier allocation algorithm consistently outperforms the continuous subcarrier allocation algorithm. This is because the continuous subcarrier allocation algorithm utilizes continuous subcarriers for key generation, and its performance is most affected by frequency correlation.

To evaluate the eavesdropping ability of the eavesdropper in this simulation model, we assume that for each UT, any other UT is a potential eavesdropper. We use the same experimental configuration as Fig. 6 to generate keys for all UTs. For the k^{th} UT (where $k \in \{1, 2, \cdots, K\}$), calculate the key disagreement rates between its generated keys and the keys generated by its nearest UT. The results show that the key disagreement rates are distributed between 48.9% and 51.4%, which is almost the same as blind guessing. Therefore, the results are consistent with the analysis in Subsection III-A, and the fact that eavesdroppers do not affect the correctness of our design.

Next, we evaluate the subcarrier utilization efficiency of different algorithms by comparing the minimum number of subcarriers required to meet $\{\Re_k\}$ when system resources are tight (i.e., some algorithms exhaust all subcarriers in Stage 1 and cannot meet all security requirements). Fig. 7 illustrates the minimum number of subcarriers required to satisfy $\{\Re_k\}$ for three algorithms when SNR ranges from 12 to 30 dB and $X = \{50\%, 60\%, 70\%, 80\%, 90\%\}$. It can be observed that the near-optimal algorithm requires the fewest subcarriers, followed by the random allocation algorithm. It is worth noting that when SNR $= 12$ dB and $X \geq 90\%$, the contiguous allocation algorithm fails to satisfy $\{\Re_k\}$ and thus occupies all subcarriers (similarly when SNR $= 18$ dB and $X \geq 80\%$, SNR $= 24$ dB and $X \geq 60\%$, SNR $= 30$ dB and $X \geq 50\%$). When it is impossible to meet $\{\Re_k\}$, we set the minimum number of subcarriers to the total number of subcarriers $N = 624$. Therefore, when facing the same security requirements, compared to random and continuous subcarrier allocation algorithms, the minimum number of subcarriers required by the near-optimal algorithm is reduced by 5.74% and 20.15%.

In Fig. 8, we evaluated the performance of different algorithms in maximizing the sum key rate under various frequency intervals. We resampled the subcarriers based on the original channel simulation and proportionally scaled the user requirements $\{\Re_k\}$ to explore the relationship between algorithm performance and subcarrier frequency spacing. For example, in the channel we simulated (simulation settings are shown in Table I), the number of subcarriers $N = 624$ with a subcarrier spacing of 15 kHz. When resampled with a gap of 2, the number of subcarriers becomes $N = 624/2 = 312$, and the subcarrier spacing becomes $2 \times 15 = 30$ kHz. Considering the reduced available subcarriers, we also scaled down the user requirements proportionally, resulting in $X = 5\%$. Table II summarizes the experimental results from Fig. 8, showing the performance improvement ratio of the near-optimal algorithm compared to the random and contiguous subcarrier allocation algorithms. We can observe that the advantage of the near-optimal algorithm becomes more pronounced as the subcarrier spacing increases.

Finally, we apply the subcarrier allocation policies obtained

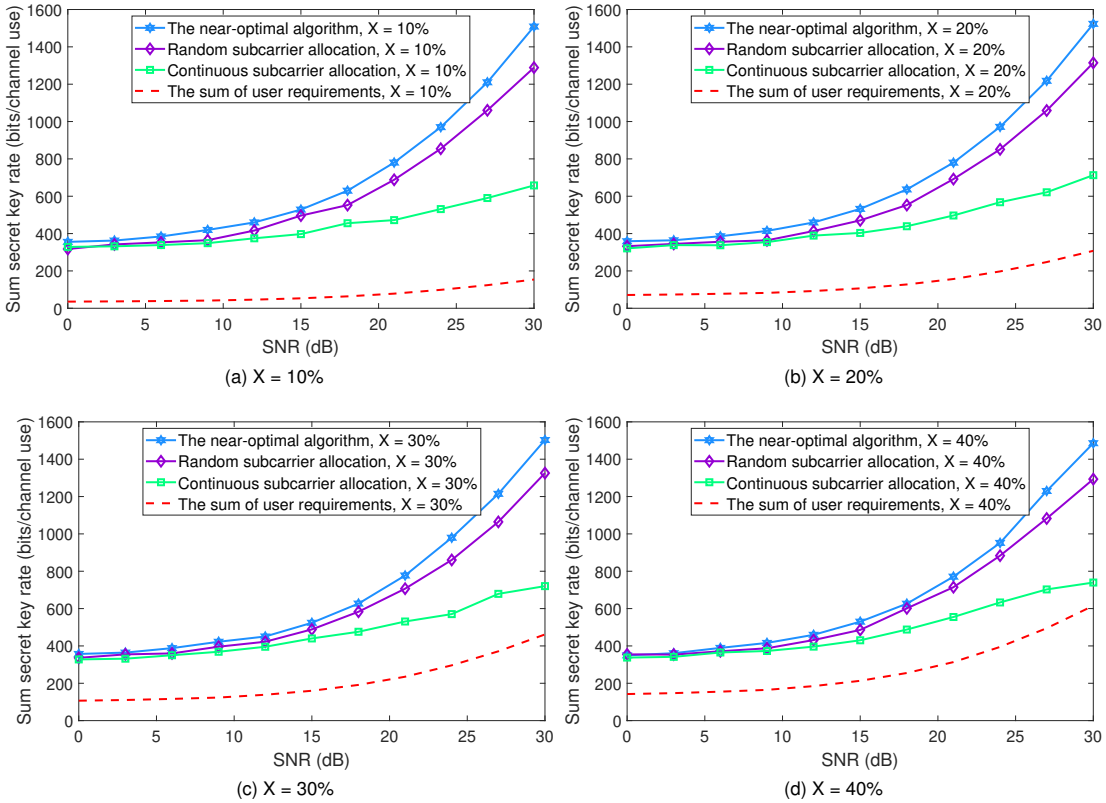

Fig. 6. The sum secret key rate comparison for different algorithms when system resources are abundant.

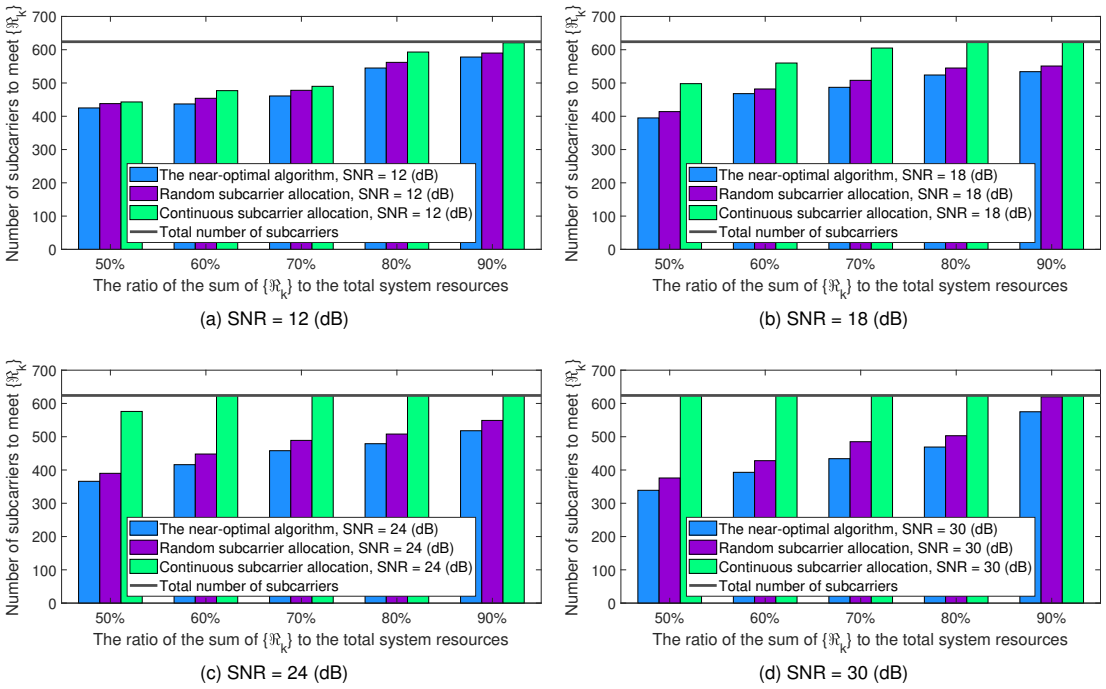

Fig. 7. The minimum number of subcarriers required to meet $\{\Re_k\}$ when system resources are tight.

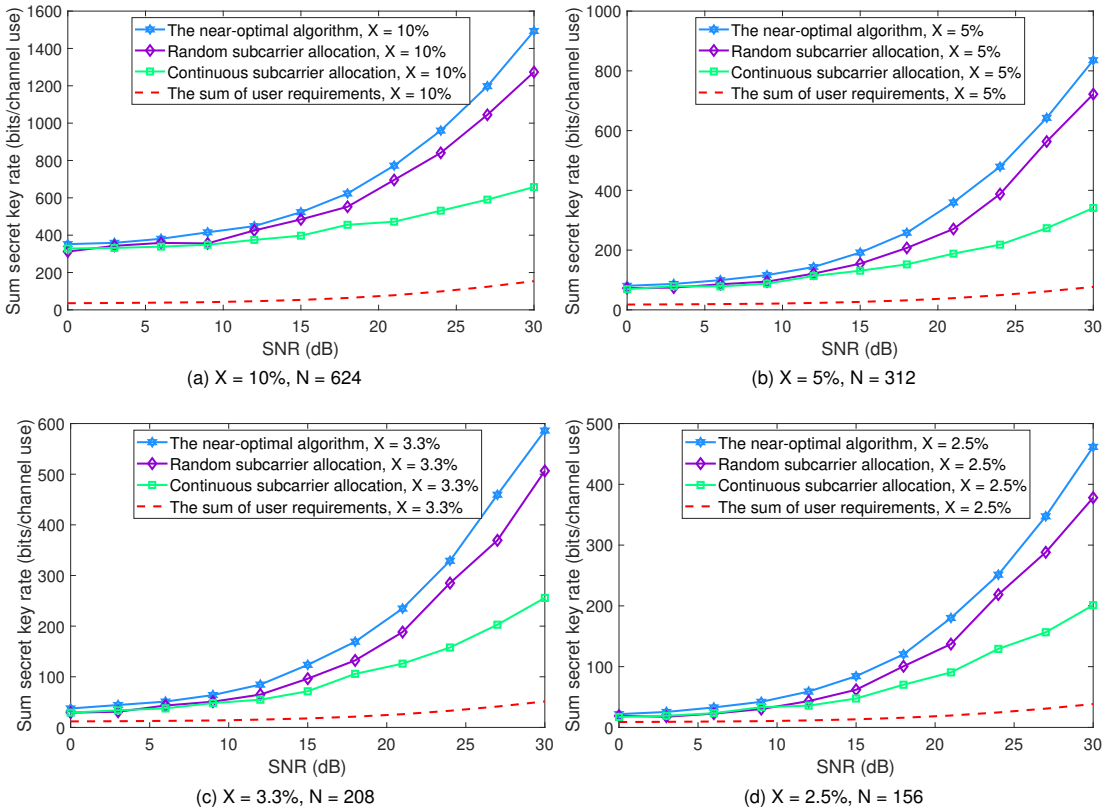

Fig. 8. The sum secret key rate comparison for different gaps.

TABLE II
IMPROVEMENT RATIO OF ALGORITHM PERFORMANCE UNDER DIFFERENT FREQUENCY INTERVALS

Resample interval	1	2	3	4
Subcarrier spacing	15 kHz	30 kHz	45 kHz	60 kHz
Subcarrier number	624	312	208	156
X	10%	5%	3.3%	2.5%
Better than Random	**11.24%**	**19.93%**	**25.60%**	**29.45%**
Better than Continuous	**46.29%**	**65.35%**	**69.59%**	**71.27%**

from different algorithms to generate keys and verify the randomness of the keys before privacy amplification. We ran nine statistical tests in the NIST test suite [27]. Table III shows the p-values and the pass ratios of the keys generated by different subcarrier allocation algorithms. We can find that in the four tests mentioned in Subsection IV-A, the results of the keys generated by the near-optimal algorithm are better than those produced by the other two algorithms.

VII. CONCLUSION

In this paper, we have studied a multi-user OFDMA model to analyze the relationship between subcarrier frequency correlation and the performance of PKG. The importance of an optimal subcarrier allocation scheme for key generation has been identified for the first time in the literature. For the case where a single UT selects a finite number of subcarriers from a given set of subcarriers for key generation, the optimal policy has been provided to minimize the impact of frequency correlation. Meanwhile, we have designed an optimal subcarrier allocation scheme that considers the diverse security requirements of UTs and studied an optimization problem to maximize the sum secret key rate while meeting all UTs' security requirements. In addition, to tackle the NP-hardness of the optimization problem, our scheme has provided an efficient near-optimal algorithm to obtain suitable subcarrier allocation policies rapidly. Our simulation results have shown that, compared to other subcarrier allocation algorithms, the proposed method can effectively improve the sum secret key rate and enhance the randomness of generated keys, resulting in better security performance.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
[2] Y. Han, L. Duan, and R. Zhang, "Jamming-assisted eavesdropping over parallel fading channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 9, pp. 2486–2499, Sep. 2019.
[3] Y. Xu, M. Liu, L. Peng, J. Zhang, and Y. Zheng, "Colluding RF fingerprint impersonation attack based on generative adversarial network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May. 2022, pp. 3220–3225.
[4] J. Tang, H. Wen, K. Zeng, R.-f. Liao, F. Pan, and L. Hu, "Light-weight physical layer enhanced security schemes for 5G wireless networks," *IEEE Netw.*, vol. 33, no. 5, pp. 126–133, Sep. 2019.
[5] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138 406–138 446, Jul. 2020.
[6] Q. Xiao, J. Zhao, S. Feng, G. Li, and A. Hu, "Securing NextG networks with physical-layer key generation: A survey," *Secur. Saf.*, vol. 3, no. 2023021, Sep. 2024.

TABLE III
RANDOMNESS TEST RESULTS BEFORE PRIVACY AMPLIFICATION

Test	Near-optimal		Random		Continuous	
	p-value	Pass ratio	p-value	Pass ratio	p-value	Pass ratio
Frequency	0.4295	0.8341	0.4877	0.929	0.3932	0.7695
Block Frequency	0.5734	0.8936	0.5476	0.8138	0.6233	0.9179
Runs	0.5149	0.8268	0.4502	0.7764	0.6629	0.8374
Longest Run of Ones	0.4689	0.8152	0.5269	0.8935	0.4628	0.7919
Rank	0.5849	0.9354	0.5023	0.8469	0.3274	0.4099
DFT	0.5588	0.9408	0.5238	0.892	0.4479	0.6629
Serial	0.6435 0.6521	0.929	0.5233 0.5827	0.8102	0.3942 0.4531	0.7242
Approximate Entropy	0.674	0.9293	0.5269	0.8731	0.3211	0.5622
Cumulative Sums	0.5121	0.9543	0.4609	0.8922	0.4203	0.8335

[7] G. Li, C. Sun, E. A. Jorswieck, J. Zhang, A. Hu, and Y. Chen, "Sum secret key rate maximization for TDD multi-user massive MIMO wireless networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 968–982, Sep. 2021.

[8] L. Hu, G. Li, X. Qian, A. Hu, and D. W. K. Ng, "Reconfigurable intelligent surface-assisted secret key generation in spatially correlated channels," *IEEE Trans. Wireless Commun.*, vol. 23, no. 3, pp. 2153–2166, Mar. 2024.

[9] Z. Ji, Y. Zhang, Z. He, P. L. Yeoh, B. Li, H. Yin, Y. Li, and B. Vucetic, "Wireless secret key generation for distributed antenna systems: A joint space-time-frequency perspective," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 633–647, Jan. 2022.

[10] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[11] G. Li, H. Luo, J. Yu, A. Hu, and J. Wang, "Information-theoretic secure key sharing for wide-area mobile applications," *IEEE Wireless Commun.*, vol. 31, no. 1, pp. 118–124, Feb. 2024.

[12] N. Gao, Y. Han, N. Li, S. Jin, and M. Matthaiou, "When physical layer key generation meets RIS: Opportunities, challenges, and road ahead," *IEEE Wireless Commun.*, vol. 31, no. 3, pp. 355–361, Mar. 2024.

[13] N. Gao, Y. Yao, S. Jin, C. Li, and M. Matthaiou, "Integrated communications and security: RIS-assisted simultaneous transmission and generation of secret keys," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 7573–7587, Aug. 2024.

[14] Z. Wan, K. Huang, X. Xu, M. Yi, H.-M. Wang, Z. Zhu, and L. Jin, "RIS-assisted integration of communications and security: Protocol, prototyping, and field trials," *IEEE Internet Things J.*, vol. 11, no. 16, pp. 26 877–26 887, Apr. 2024.

[15] 3GPP, "NR; Physical channels and modulation," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.211, 6 2022, version 17.2.0. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3213

[16] 3GPP, "Study on channel model for frequencies from 0.5 to 100 GHz," 3rd Generation Partnership Project (3GPP), Technical Report (TR) 38.901, 3 2022, version 17.0.0. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3173

[17] "IEEE draft standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 8: Enhancements for extremely high throughput (EHT)," *IEEE P802.11be/D4.0*, pp. 1–1031, Jul. 2023.

[18] T. Wang, C. You, Z. He, and Y. Wang, "Distributed subcarrier assignment and discrete power allocation for multi-UAV millimeter-wave cooperative OFDMA networks with heterogeneous QoS consideration," *IEEE Access*, vol. 11, pp. 123 132–123 148, Oct. 2023.

[19] J. Zhang, M. Ding, D. López-Pérez, A. Marshall, and L. Hanzo, "Design of an efficient OFDMA-based multi-user key generation protocol," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8842–8852, Sep. 2019.

[20] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022–3034, Jul. 2018.

[21] G. Li, A. Hu, L. Peng, and C. Sun, "The optimal preprocessing approach for secret key generation from OFDM channel measurements," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–6.

[22] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, Jun. 2016.

[23] C. Sun and G. Li, "Power allocation and beam scheduling for multi-user massive MIMO secret key generation," *IEEE Access*, vol. 8, pp. 164 580–164 592, Jan. 2020.

[24] B. T. Quist and M. A. Jensen, "Maximization of the channel-based key establishment rate in MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5565–5573, Oct. 2015.

[25] L. Hu, C. Sun, G. Li, A. Hu, and D. W. K. Ng, "Reconfigurable intelligent surface-aided secret key generation in multi-cell systems," *IEEE Trans. Commun.*, vol. 71, no. 11, pp. 6499–6513, Aug. 2023.

[26] E. Yaacoub, "On secret key generation with massive MIMO antennas using time-frequency-space dimensions," in *Proc. IEEE Middle East Conf. Antennas Propag. (MECAP)*, Beirut, Lebanon, Sep. 2016, pp. 1–4.

[27] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert *et al.*, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. National Institute of Standards & Technology, 2001, vol. 22.

[28] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 693–702, Sep. 2011.

[29] F. Alajaji and P.-N. Chen, *An Introduction to Single-User Information Theory*. Singapore: Springer, 2018.

[30] H. Kellerer, U. Pferschy, and D. Pisinger, "Multiple knapsack problems," in *Knapsack Problems*. Berlin, Germany: Springer, 2004, pp. 285–316. [Online]. Available: https://doi.org/10.1007/978-3-540-24777-7_10

[31] R. M. Karp, "Reducibility among combinatorial problems," in *Complexity of Computer Computations*. Boston, MA: Springer US, 1972, pp. 85–103. [Online]. Available: https://doi.org/10.1007/978-1-4684-2001-2_9

[32] K. Qian, C. Wu, Y. Zhang, G. Zhang, Z. Yang, and Y. Liu, "Widar2.0: Passive human tracking with a single Wi-Fi link," in *Proc. ACM Int. Conf. Mobile Syst. Appl. Serv. (MobiSys)*, Jun. 2018, p. 350–361.

[33] S. Jaeckel, L. Raschkowski, K. Börner, and L. Thiele, "Quadriga: A 3-D multi-cell channel model with time evolution for enabling virtual field trials," *IEEE Trans. Antennas Propag.*, vol. 62, no. 6, pp. 3242–3256, Jun. 2014.

[34] S. Jaeckel, L. Raschkowski, K. Borner, L. Thiele, F. Burkhardt, and E. Eberlein, "Quadriga-quasi deterministic radio channel generator, user manual and documentation," Fraunhofer Heinrich Hertz Institute, Tech. Rep. v2.6.1, 2021.

Qingjiang Xiao received the B.Eng. degree from the College of Computer and Data Science, Fuzhou University. He is currently pursuing the M.Sc. degree with the School of Cyber Science and Engineering, Southeast University. His current research interests include physical layer security and secret key generation.

Guyue Li (Member, IEEE) received the B.S. degree in information science and technology and the Ph.D. degree in information security from Southeast University, Nanjing, China, in 2011 and 2017, respectively. From June 2014 to August 2014, she was a Visiting Student with the Department of Electrical Engineering, Tampere University of Technology, Tampere, Finland. She is currently an Associate Professor with the School of Cyber Science and Engineering, Southeast University, and a Visiting Scholar with Tampere University of Technology and Université Gustave Eiffel (ESIEE PARIS), Noisy-le-Grand, France. Her current research interests include wireless network attacks, physical-layer security solutions for 5G and 6G, secret key generation, radio frequency fingerprints, and reconfigurable intelligent surfaces. She is currently serving as an Editor for IEEE COMMUNICATION LETTERS and an Associate Editor for EURASIP Journal on Wireless Communications and Networking.

Zilong Liu (Senior Member, IEEE) received the Bachelor's degree in Electronics and Information Engineering from Huazhong University of Science and Technology (HUST), Wuhan, China, the Master's degree in Electronic Engineering from Tsinghua University, Beijing, China, and the Ph.D. degree in Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore, in 2004, 2007 and 2014, respectively. He was a Visiting PhD student in the University of Melbourne and the Hong Kong University of Science and Technology (HKUST). He is currently an Associate Professor and the 6G Lab Manager with the School of Computer Science and Electronic Engineering, University of Essex. His research lies in the interplay of coding, signal processing, and communications, with a major objective of bridging theory and practice. His recent research interests include advanced 6G V2X communication, sensing, and localization technologies for future connected autonomous vehicles as well as machine learning for enhanced communications and networking. Details of his research can be found at: https://sites.google.com/site/zilongliu2357.

Aiqun Hu (Senior Member, IEEE) received the B.Sc.(Eng.), M.Eng.Sc., and Ph.D. degrees from Southeast University, Nanjing, China, in 1987, 1990, and 1993, respectively. He was invited as a Postdoctoral Research Fellow with The University of Hong Kong, Hong Kong, from 1997 to 1998, and a TCT Fellow with Nanyang Technological University, Singapore, in 2006. He is currently a Professor with the School of Information Science and Engineering and the National Mobile Communications Research Laboratory, Southeast University. He has published two books and more than 100 technical articles in the wireless communications field. He is an IET Fellow. His research interests include data transmission and secure communication technology.