Precoding Design for Key Generation in Extremely Large-Scale MIMO Near-Field Multi-User Systems

Tianyu Lu, *Member, IEEE,* Liquan Chen, *Senior Member, IEEE,* Junqing Zhang, *Senior Member, IEEE,* Chen Chen, *Member, IEEE,* Trung Q. Duong, *Fellow, IEEE*, and Michail Matthaiou, *Fellow, IEEE*

***Abstract*—This paper develops a physical layer key generation (PLKG) scheme that utilizes artificial randomness in extremely large-scale multiple-input multiple-output (XL-MIMO) near-field multi-user communications to produce shared secret keys for legitimate users. Unlike traditional PLKG schemes, which rely on the variation of wireless channels, this approach introduces noise power via the precoding vectors to create dynamic fluctuations in the line-of-sight (LoS) channels, emulating the rapid changes typically observed in fast-fading channels. This artificial randomness ensures that the user equipment (UEs) can generate secret keys while effectively preventing potential eavesdropping from malicious eavesdroppers. In particular, a novel channel probing protocol is designed, enabling multiple UEs to simultaneously agree on secret keys with the base station (BS) using non-orthogonal pilots, which exploits the difference in the distances and spatial angles of UEs in near-field communications. Secondly, to maximize the secret key rate, an alternating optimization algorithm is proposed, solving two sub-optimization problems. The first sub-problem employs the singular value decomposition (SVD) method to identify the legitimate space and its orthogonal subspace for generating secret keys and preventing eavesdropping attacks, respectively. Subsequently, a Dinkelbach method-based power allocation algorithm is developed to allocate noise power to these two spaces. The second sub-problem uses a water-filling algorithm to implement power allocation among multiple UEs. Finally, to address the issue of precoding noise not being considered in the alternating optimization problem, a deep learning-based method is introduced, which further improves the performance of the scheme. Simulations demonstrate the efficiency of the proposed PLKG scheme over existing schemes.**

***Index Terms*—Deep learning, extremely large-scale MIMO, near-field communications, physical layer key generation.**

This research was supported by the National Natural Science Foundation of China (No. U22B2026, 62572121). The work of J. Zhang and C. Chen was also supported by the UK EPSRC under grant ID EP/V027697/1. The work of T. Q. Duong was supported in part by the Canada Excellence Research Chair (CERC) Program CERC-2022-00109, in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant Program RGPIN-2025-04941. This work was supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 101001331) and by a research grant from the Department for the Economy Northern Ireland under the US-Ireland R&D Partnership Programme. For the purpose of open access, the authors have applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising. Parts of this paper were presented at the 2023 IEEE GLOBECOM conference [1]. (*Corresponding author: L. Chen*)

T. Lu and M. Matthaiou are with the Centre for Wireless Innovation (CWI), Queen's University Belfast, Belfast, BT3 9DT, U. K. (e-mail: t.lu@qub.ac.uk; m.matthaiou@qub.ac.uk).

L. Chen is with the School of Cyber Science and Engineering, Southeast University, Nanjing, 210096, China. L. Chen is also with the Purple Mountain Laboratories for Network and Communication Security, Nanjing, 211111, China. (e-mail: lqchen@seu.edu.cn).

J. Zhang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, U. K. (email: junqing.zhang@liverpool.ac.uk).

C. Chen is with the College of Astronautics, Nanjing University of Aeronautics and Astronautics, Nanjing, 211106, China. (e-mail: chenchen8079@nuaa.edu.cn).

T. Q. Duong is with the Faculty of Engineering and Applied Science, Memorial University, St. John's, NL A1C 5S7, Canada, and with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast, U.K. (e-mail: tduong@mun.ca).

I. Introduction

SIGNIFICANT research has been dedicated to developing advanced technologies, such as millimeter-wave (mmWave)/terahertz (THz) networks as well as extremely large-scale multiple-input multiple-output (XL-MIMO) [2], [3], also known as extra large-scale MIMO [4], to meet the increasing requirements for widespread connectivity in the sixth generation (6G) wireless communications [5]. Ensuring secure communication services is crucial for 6G. Compared with public key cryptography (PKC) based on computational security, physical layer key generation (PLKG) leverages channel randomness, channel reciprocity, and spatial decorrelation properties to achieve information-theoretical security [6]. Furthermore, the design of PLKG is less complicated compared to PKC, making it well-suited for resource-constrained devices [7]. Equally importantly, PLKG schemes are ideal for device-to-device communications as they eliminate the need for third-party involvement or expensive infrastructure to handle key management challenges [8].

The advent of XL-MIMO systems has led to a significant increase in the number of antennas operating within the mmWave and THz frequency bands, which fundamentally alters the structure of the electromagnetic (EM) radiation field [9]–[12]. The EM field can be categorized into two regions: the far-field and the radiating near-field regions [13]. The Rayleigh distance is the boundary that separates these two distinct regions [14]. Beyond the Rayleigh distance, also called as Fraunhofer distance, the far-field channel model is based on planar waves. In contrast, within the Rayleigh distance, the spherical waves channel model is more suitable [3], [4], [15]. Consequently, this transition towards near-field communications introduces unique characteristics to PLKG.

Current PLKG research concentrates mainly on sub-6GHz systems with a focus on far-field scenarios. However, PLKG experiences significant challenges in sub-6GHz scenarios characterized by poor channel conditions. Conventional key generation schemes depend on the inherent randomness of wireless channels to generate secret keys, typically assuming a certain degree of user mobility or environmental changes [16], [17].

In such schemes, the non-line-of-sight (NLoS) components provide the necessary channel variations for key generation. In static environments, where the channel variations are slow, the inherent randomness of wireless channels is insufficient for generating secret keys. More specifically, the line-of-sight (LoS) component is determined by the transceiver distance and varies little over time, thus offering limited key randomness. To address this, random beamforming in MIMO systems is introduced to mimic "fast fading" variations by randomly configuring the antenna coefficients. This allows Alice and Bob to leverage the artificial randomness from the static channel combined with random beamforming, thereby increasing the secret key rate (SKR) in scenarios with slow channel variations [18]. In [19], the precoding matrix indices from a MIMO-based transmitter along with rotated reference signals were applied to enhance the SKR, where a bi-directional channel in one band was constructed for exchanging the rotated reference signals. Furthermore, to address the multiply-divide attack in the loop-back key generation scheme proposed therein, two separate bands for rotated pilot transmission and echo reception were leveraged in [20]. However, a limitation of random beamforming arises when the direct channel is blocked or exhibits poor quality. In response, a reconfigurable intelligent surface (RIS) has been utilized as a passive technique to address the low-entropy problem in PLKG [21]. Matching-based secret key generation is a potential solution for solving low-entropy problems [22]. This technique enables the master node to apply a random permutation to a shared sequence obtained from channel measurements, while the follower node can identify this random permutation using matching algorithms. Nevertheless, in the above-mentioned works, there is no information-theoretical security analysis.

To address the issue of static channels, it is typically assumed that there exists a disparity in the spatial angles between Bob and the eavesdropper in far-field key generation systems. More specifically, Alice leverages spatial angles as a spatial degree of freedom (DoF) to introduce artificial randomness. For example, exploiting the variance in the spatial angles between a receiver and an eavesdropper in MIMO systems offers an opportunity to introduce randomness into the transmitter, thereby generating secret keys [23]. With the increase in the number of antennas in massive MIMO systems, perturbed beamforming weights can be utilized to introduce artificial randomness [24]. The high directionality provided by massive MIMO-based beamforming is harnessed to safeguard legitimate users from potential eavesdroppers in close proximity in mmWave channels. However, it is challenging for traditional secret beam schemes [24] to ensure a positive SKR in situations where Eve occupies the same spatial angle as Bob, for example, when Bob is obstructed by Eve, and Eve is closer to Alice than Bob.

Recently, several works have explored the potential of machine learning techniques in enhancing the security aspects of communication systems. For instance, the deep learning-based secure precoding optimization problem within the context of artificial noise (AN), applied to multiple-input single-output (MISO) wiretap channels, was studied in [25]. Later in [26], a deep neural network (DNN)-based precoder was designed for MIMO systems, aiming to enhance the physical layer security. These works focused on keyless secure transmission. Regarding secret key generation, machine learning is effective in tackling non-convex optimization problems that are challenging to solve using traditional mathematical methods [27]. A machine learning-based joint precoding and phase shift matrices design in a RIS-aided system was proposed to increase the SKR in [27]. To the best of our knowledge, the utilization of machine learning for designing optimal precoders in AN schemes for secret key generation in near-field communications remains unexplored.

To tackle the aforementioned challenges, this paper studies the near-field XL-MIMO key generation problem to utilize distance as a new spatial DoF to induce artificial randomness to solve the low-SKR problem in high-frequency bands. Furthermore, by exploiting the distinctions in spatial angles and distances among users, this approach facilitates multi-user key generation, effectively minimizing the pilot overhead. Our main contributions are summarized as follows:

- We design a PLKG framework through a multi-user channel probing protocol with non-orthogonal pilots, which leverages the difference in the distances and spatial angles of user equipment (UEs) in near-field communications. The proposed protocol reduces the pilot overhead and prevents eavesdroppers from eavesdropping. Furthermore, we derive an analytical expression for the SKR.
- We propose an alternating optimization algorithm to maximize the SKR, where two sub-problems are solved. In the first sub-problem, we use a singular value decomposition (SVD) to find the legitimate and orthogonal subspaces. A Dinkelbach-based power allocation method is proposed to implement power allocation for UEs to generate secret keys and to prevent Eves from eavesdropping. In the second sub-problem, a water-filling algorithm is proposed to allocate power among the UEs.
- Since the alternating optimization algorithm does not consider the influence of precoding on the noise, we design a deep-learning network to solve a more complex problem. To maximize the SKR, we introduce an unsupervised DNN to learn the relationship between the distance of UEs and Eves, the spatial angles of UEs and Eves and the power range.
- We validate the SKRs of the proposed PLKG schemes in terms of transmit power, the distance of UEs and Eves and the spatial angles of UEs and Eves. The proposed schemes surpass the performance of existing schemes.

Note that our previous conference work in [1] designed precoding vectors of BS in a single-user XL-MIMO near-field system. In this paper, we considerably extend the work of [1] to a more general scenario with multiple users. The precoding vectors for inducing artificial randomness to UEs are jointly designed to maximize the SKR when the Eves eavesdrop on legitimate channels. Furthermore, a deep learning-based precoding design algorithm is proposed to optimize the SKR when the precoding noise is considered in the objective function.

The rest of this paper is organized as follows: Section II

elaborates on the system model of near-field key generation. In Section III, a multi-user channel probing protocol is proposed. We further derive the analytical expression for the SKR. Section IV presents an optimization problem formulation followed by the introduction of a power allocation method based on the water-filling algorithm. In Section V, we extend the deep-learning-based method to address the general case. Section VI provides simulation results. Sections VII and VIII present this paper's discussion and conclusion, respectively.

Notations: Italic letters, boldface lower-case letters, boldface upper-case letters and calligraphic letters denote scalars, vectors, matrices and sets, respectively; diag$(\cdot)$ forms a diagonal matrix out of its vector argument; vec$(\cdot)$ is the vectorization of a matrix argument; $(\cdot)^T$, $(\cdot)^H$, $(\cdot)^{-1}$ and $(\cdot)^*$ denote the transpose, conjugate transpose, inverse, and conjugate, respectively; $\mathbb{C}^{m\times n}$ is the complex space of a $m \times n$ matrix; $\mathbf{I}_N$ denotes the $N \times N$ identity matrix; $\mathcal{CN}(\mu, \sigma^2)$ denotes the circularly symmetric complex Gaussian distribution with mean μ and variance σ^2; $\mathbb{E}\{\cdot\}$ is the statistical expectation; $I(\cdot)$ denotes mutual information; The matrix with all elements equal to zero is denoted as $\mathbf{0}$; $\|\cdot\|_2$ is the Euclidean norm; Tr$(\cdot)$ denotes the trace of a matrix; For a complex vector $\mathbf{x} \in \mathbb{C}^n$, $\Re\{\mathbf{x}\}$ and $\Im\{\mathbf{x}\}$ denote its real and imaginary parts, respectively; $\mathbb{R}^{m\times n}$ denotes the space of real-valued $m \times n$ matrices.

II. System Model

A. Overview

Figure 1 presents the setup for an XL-MIMO-assisted key generation system, comprising a base station (BS), K UEs, and K eavesdroppers (Eves). The BS is equipped with N antennas, while the UEs and Eves are equipped with a single antenna. The Eves are assumed to be passive, as they do not actively transmit signals to interfere with the key generation process. In addition, we assume that the Eves are curious users within the same network who are interested in the information exchanged between legitimate parties. Since these curious users communicate with the BS, their channel state information (CSI) can be acquired during the transmission process [28], [29]. Given the known CSI, the BS designs precoding vectors that inject artificial randomness into the legitimate channels for secret key generation, as detailed in Sections IV and V. In near-field communications, the channel correlation between an Eve and a UE increases significantly with proximity, leading to a higher risk of key leakage. Hence, we assume that the k-th user is targeted by a nearby k-th Eve attempting to eavesdrop on the secret keys.

As shown in Fig. 2, a key generation protocol comprises four steps, namely channel probing, quantization, information reconciliation and privacy amplification. In the channel probing step, the k-th UE (BS) transmits uplink (downlink) pilots to each other using a time division duplexing (TDD) mode. Accordingly, the k-th UE measures the downlink near-field channel while the BS measures the uplink channels. Particularly, we assume that the uplink and downlink channels are reciprocal. In the quantization step, these channel measurements are converted into binary sequences using quantization

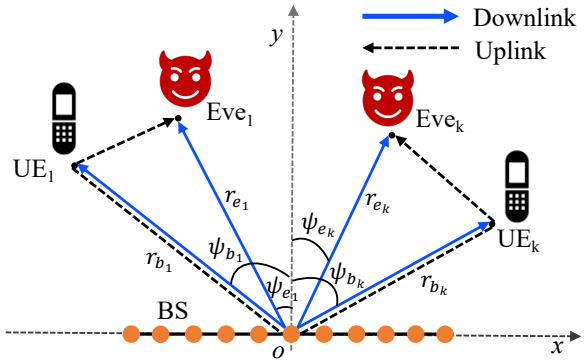

Fig. 1. System model.

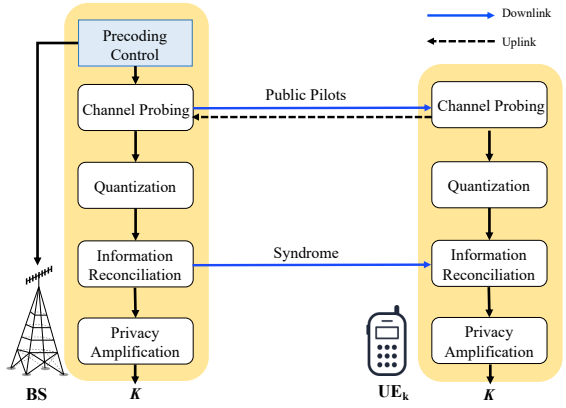

Fig. 2. Key generation protocol.

algorithms. Due to the presence of noise, discrepancies may arise between the quantized sequences, which can be rectified during the subsequent information reconciliation step. Finally, privacy amplification algorithms are employed to eliminate any potential information leakage from the preceding stages. The BS and the k-th UE agree on a unique secret key sequence $\boldsymbol{k}_c$. This paper focuses on the design of channel probing, which will be explained in Section III. The quantization is presented in Section VI.

B. Device Configuration

As shown in Fig. 1, we consider a two-dimensional coordinate system consisting of BS (Alice), UEs (Bobs) and Eves, with the BS deployed along x-axis. The coordinate of the central antenna of the BS equipped with a N-antenna uniform linear array (ULA) is situated at $(0, 0)$. The coordinate of the n-th antenna is $(\delta_n d, 0)$ with $\delta_n = \frac{2n-N+1}{2}$, $n = 0, \ldots, N-1$, where d is the antenna spacing. The coordinates of u, $u \in \{b_k, e_k\}$, are $(r_u\theta_u, r_u\sqrt{1-\theta_u^2})$, where $\theta_u = \sin\psi_u \in [-1, 1]$, r_u is the distance from u to the centre of BS and ψ_u is the azimuth angle. Notably, b_k denotes the b_k-th UE and e_k denotes the e_k-th Eve.

C. Near-Field Channel Model

Depending on the distance from the antenna, the EM field can be classified into reactive field and radiative field [30]. The reactive near-field region, which lies close to the antenna, is

characterized by energy stored in capacitive and inductive reactance rather than being radiated into free space. By contrast, in the radiative field, the electric and magnetic fields begin to become radiative. Typically, the boundary for separating the reactive and radiative field is defined as $d_F = 0.62\sqrt{\frac{D^3}{\lambda}}$, where D represents the array aperture and λ corresponds to the wavelength [13].

The radiative field itself is further split into the radiative near-field and the far-field [31]. A commonly utilized demarcation between these regions is defined by the Rayleigh distance, which is given by $d_R = \frac{2D^2}{\lambda}$ [32]. For a ULA, the array aperture is $D = (N-1)d$. Thus, the Rayleigh distance of a ULA is $d_R = \frac{1}{2}(N-1)^2\lambda$ with $d = \lambda/2$. For example, with a 100-element ULA operating at 28 GHz, the d_R is approximately 52.5 m and the d_F is around 2.3 m. Therefore, the radiative near-field region spans from 2.3 m to 52.5 m. Notably, in this paper, when we use the term "near-field", we are specifically referring to the radiative near-field. The radiative near-field is defined within the distance range from d_F to d_R. For those interested in the key generation within the reactive near-field region, the study conducted in [33] provides relevant insights.

When the distance between the BS and the user is less than the Rayleigh distance, the EM field enters the radiative near-field region. The planar wavefront approximation no longer holds, and a spherical wavefront representation is adopted following [13], [31], [32]. Taking into account the curvature of the spherical wavefront, we model both the nonlinear phase variations and non-uniform amplitude gains across the array elements. Firstly, when the incident wavefront is spherical, the wave arrives at each antenna element with a different propagation angle, resulting in varying distances from the user to each antenna. Let $r_u^{(n)} = \sqrt{r_u^2 + d^2\delta_n^2 - 2r_u\theta_u d\delta_n}$ denote the distance from the user to the n-th antenna. The relative distance difference is defined as $(r_u^{(n)} - r_u)$, which leads to a nonlinear phase shift of $k_c(r_u^{(n)} - r_u)$ across the array, where $k_c = \frac{2\pi}{\lambda}$ is the wavenumber. Secondly, to further account for the effect of wavefront curvature, we model the non-uniform channel amplitude across the array. Due to distance variations across antenna elements, the channel amplitude $\sqrt{\beta_u^{(n)}}$ from user u to the n-th antenna element varies with n. Accordingly, the near-field array response vector is modeled as:

$$\mathbf{c}(\psi_u, r_u) = \frac{1}{\sqrt{N}}\left[\sqrt{\beta_u^{(0)}}e^{-jk_c(r_u^{(0)}-r_u)}, \ldots, \sqrt{\beta_u^{(N-1)}}e^{-jk_c(r_u^{(N-1)}-r_u)}\right]^T, \quad (1)$$

where $\mathbf{c}(\psi_u, r_u) \in \mathbb{C}^{N\times 1}$.

Based on (1), the near-field LoS channel from the k-th UE to the BS is modeled as

$$\mathbf{f}_k = \sqrt{N}\mathbf{c}(\psi_{b_k}, r_{b_k}), \quad (2)$$

where $\mathbf{f}_k \in \mathbb{C}^{N\times 1}$. Similarly, we model the near-field channel from the k-th Eve to the BS as

$$\mathbf{h}_k = \sqrt{N}\mathbf{c}(\psi_{e_k}, r_{e_k}), \quad (3)$$

where $\mathbf{h}_k \in \mathbb{C}^{N\times 1}$. In near-field communications, the correlation between $\mathbf{f}_k$ and $\mathbf{h}_k$ is affected by both the angles and distances [13]. As the number of antennas increases, the correlation between two near-field channels with different angles or distances approaches zero [34].

For high-frequency bands, such as mmWave and THz frequency bands, non-line-of-sight (NLoS) components can be neglected due to relatively small power levels compared with the LoS counterparts [35], [36]. In non-stationary near-field channels, different regions of an XL-MIMO antenna array may be either visible or invisible to a UE, leading to a distinct channel model [13]. Our paper focuses on a stationary near-field channel, where all antenna arrays are visible to the UE, as also adopted in [31].

III. Multi-User Channel Probing in Near-Field Communications

The channel probing process consists of uplink and downlink phases, each spanning V time slots. In the uplink (downlink) phase, the UEs (BS) transmit uplink (downlink) pilots to the BS (UEs). In the uplink phase, each UE simultaneously transmits the same uplink pilot $\mathbf{s}_a \in \mathbb{C}^{V\times 1}$, where V denotes the pilot length over consecutive time slots. Here $\mathbf{s}_a^H\mathbf{s}_a = P_bV$, where P_b denotes the transmit power of each UE. After receiving the uplink pilots from all K UEs, the BS estimates the near-field channels from N antennas. The BS then uses the random precoding vector $\mathbf{w}_k \in \mathbb{C}^{N\times 1}$ to combine the estimated channel to extract the effective channel associated with the k-th UE.

In the downlink phase, the BS transmits the same downlink pilot $\mathbf{s}_d \in \mathbb{C}^{V\times 1}$ to all UEs over V consecutive time slots. The $\mathbf{s}_d$ satisfies $\mathbf{s}_d^H\mathbf{s}_d = V$ to ensure unit average power. Using user-specific precoding vectors $\{\mathbf{w}_k\}_{k=1}^K$, the BS transmits the aggregated pilot signal $\sum_{k=1}^K \mathbf{w}_k\mathbf{s}_d^H \in \mathbb{C}^{N\times V}$. Each UE receives a superposition of the precoded signals, and estimates its effective downlink channel. Note that since the LoS fading is static, the BS employs precoding vectors, $\{\mathbf{w}_k\}$, to create artificial randomness to mimic fast-fading characteristics for generating secret keys, as will be described in Section IV and Section V.

A. Channel Probing for Secret LoS Channels

1) Downlink Channel Probing: The BS transmits a non-orthogonal pilot signal in the form of $\sum_{k=1}^K \mathbf{w}_k\mathbf{s}_d^H$. The received signal at the k-th UE is given by

$$\mathbf{y}_{b_k}^T = \mathbf{f}_k^H\sum\nolimits_{i=1}^K \mathbf{w}_i\mathbf{s}_d^H + \mathbf{n}_{b_k}^T, \quad (4)$$

where $\mathbf{y}_{b_k} \in \mathbb{C}^{V\times 1}$. The noise vector $\mathbf{n}_{b_k} \in \mathbb{C}^{V\times 1}$ represents temporally independent complex Gaussian noise over the V time slots, modeled as $\mathbf{n}_{b_k} \sim \mathcal{CN}(\mathbf{0}, \sigma_{b_k}^2\mathbf{I})$.

By the least square (LS) estimator, the k-th UE measures the near-field channel, $\mathbf{f}_k$, according to

$$\begin{aligned} z_{b_k} &= \mathbf{y}_{b_k}^T\frac{\mathbf{s}_d}{\|\mathbf{s}_d\|_2^2} = \mathbf{f}_k^H\sum\nolimits_{i=1}^K \mathbf{w}_i + \mathbf{n}_{b_k}^T\frac{\mathbf{s}_d}{\|\mathbf{s}_d\|_2^2} \\ &= \mathbf{f}_k^H\mathbf{w}_k + \underbrace{\mathbf{f}_k^H\sum\nolimits_{i\neq k}\mathbf{w}_i}_{\text{interference}} + \widehat{n}_{b_k}, \end{aligned} \quad (5)$$

where $\widehat{n}_{b_k} \sim \mathcal{CN}(0, \widehat{\sigma}^2_{b_k})$ is the LS estimation noise at the k-th UE, and $\widehat{\sigma}^2_{b_k} = \frac{\sigma^2_{b_k}}{V}$ is the estimation noise variance.

The k-th Eve also receives the downlink pilot, given by

$$\mathbf{y}^T_{ae_k} = \mathbf{h}^H_k \sum\nolimits_{i=1}^{K} \mathbf{w}_i \mathbf{s}^H_d + \mathbf{n}^T_{ae_k}, \tag{6}$$

where $\mathbf{y}_{ae_k} \in \mathbb{C}^{V\times 1}$, $\mathbf{n}_{ae_k} \in \mathbb{C}^{V\times 1} \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{ae_k}\mathbf{I})$ is the noise at the k-th Eve, while $\sigma^2_{ae_k}$ is the noise variance.

By the LS estimator, the k-th Eve measures the near-field channel, $\mathbf{h}_k$, which is given by

$$\begin{aligned} z_{ae_k} &= \mathbf{y}^T_{ae_k} \frac{\mathbf{s}_d}{\|\mathbf{s}_d\|^2_2} = \mathbf{h}^H_k \sum\nolimits_{i=1}^{K} \mathbf{w}_i + \mathbf{n}^T_{ae_k} \frac{\mathbf{s}_d}{\|\mathbf{s}_d\|^2_2} \\ &= \mathbf{h}^H_k \sum\nolimits_{i=1}^{K} \mathbf{w}_i + \widehat{n}_{ae_k}, \end{aligned} \tag{7}$$

where $\widehat{n}_{ae_k} \sim \mathcal{CN}(0, \widehat{\sigma}^2_{ae_k})$ is the estimation noise and $\widehat{\sigma}^2_{ae_k} = \frac{\sigma^2_{ae_k}}{V}$ is the estimation noise variance.

2) Uplink Channel Probing: The UEs simultaneously send the same uplink pilot $\mathbf{s}_a$ to the BS, and the received signal at the BS is given by

$$\mathbf{Y}_a = \sum\nolimits_{i=1}^{K} \mathbf{f}_i \mathbf{s}^H_a + \mathbf{N}_a, \tag{8}$$

where $\mathbf{N}_a \in \mathbb{C}^{N\times V}$ is the noise matrix at the BS. The i-th row and the j-th column element of $\mathbf{N}_a$ corresponds to the noise observed at the i-th receive antenna during the j-th time slot, and is modeled as an independent and identically distributed complex Gaussian variable, i.e., $n_{i,j} \sim \mathcal{CN}(0, \sigma^2_a)$, where σ^2_a is the noise variance at the BS.

The BS gets the measurement of the k-th UE as

$$\mathbf{z}_{a_k} = \mathbf{Y}_a \frac{\mathbf{s}_a}{\|\mathbf{s}_a\|^2_2} = \sum\nolimits_{i=1}^{K} \mathbf{f}_i + \widehat{\mathbf{n}}_a, \tag{9}$$

where $\mathbf{z}_{a_k} \in \mathbb{C}^{N\times 1}$, $\widehat{\mathbf{n}}_a = \mathbf{N}_a \frac{\mathbf{s}_a}{\|\mathbf{s}_a\|^2_2} \in \mathbb{C}^{N\times 1} \sim \mathcal{CN}(0, \bar{\sigma}^2_a \mathbf{I})$ is the LS estimation noise and $\bar{\sigma}^2_a = \frac{\sigma^2_a}{VP_b}$.

The BS applies the random precoding vector, $\mathbf{w}_k$, to the measurement of the k-th UE in (9) and obtains

$$\bar{z}_{a_k} = \mathbf{w}^H_k \mathbf{z}_{a_k} = \mathbf{w}^H_k \sum\nolimits_{i=1}^{K} \mathbf{f}_i + \mathbf{w}^H_k \widehat{\mathbf{n}}_a. \tag{10}$$

The BS obtains the conjugate transpose of $\bar{z}_{a_k}$ as follows:

$$z_{a_k} = \bar{z}^H_{a_k} = \left(\sum\nolimits_{i=1}^{K} \mathbf{f}^H_i \right) \mathbf{w}_k + \widehat{n}_{a_k}, \tag{11}$$

where $\widehat{n}_{a_k} = \widehat{\mathbf{n}}^H_a \mathbf{w}_k$ is the estimation noise after precoding, $\widehat{n}_{a_k} \sim \mathcal{CN}(0, \widehat{\sigma}^2_{a_k})$, and $\widehat{\sigma}^2_{a_k} = \frac{P_{a_k}\sigma^2_a}{VP_b}$ is the estimation noise variance at the BS. When the input signal has unit power, the value of $\|\mathbf{w}_k\|^2_2$ equals the transmit power for the k-UE, i.e., $\|\mathbf{w}_k\|^2_2 = P_{a_k}$.

Accordingly, the k-th Eve gets the measurement from the uplink pilot as

$$z_{be_k} = \sum\nolimits_{i=1}^{K} h_{b_i e_k} + \widehat{n}_{be_k}, \tag{12}$$

where $\widehat{n}_{be_k} \sim \mathcal{CN}(0, \widehat{\sigma}^2_{be_k})$ is the LS estimation noise, $\widehat{\sigma}^2_{be_k}$ is the estimation noise variance at the k-th Eve, and $h_{b_i e_k}$ is the channel from the i-th UE to the k-th Eve.

To reduce the pilot overhead, K UEs share the same uplink and downlink pilot in the multi-user key generation process. However, this approach introduces interference from the precoding vectors of other UEs, causing the measurements to become correlated. To address this issue, we propose an SVD-based precoding scheme that mitigates the interference from other UEs, ensuring the measurements of the K UEs remain uncorrelated.

B. Singular Value Decomposition

To ensure that the artificial noise induced for other UEs does not affect the k-th UE, we carefully construct the precoding vector $\mathbf{w}_k$ for the k-th UE to lie in the null space of other UEs. This approach effectively mitigates interference among UEs. Moreover, to prevent the leakage of information to unintended Eves, the design of the precoding vector $\mathbf{w}_k$ must also be confined within the null space of all Eves, except for the k-th Eve. This ensures that the secret keys are safeguarded and remain private to the intended UE while avoiding potential eavesdropping risks.

We define

$$\begin{aligned} \widetilde{\mathbf{R}}_k = &[\mathbf{f}_1, \ldots, \mathbf{f}_{(k-1)}, \mathbf{f}_{(k+1)}, \ldots, \mathbf{f}_K, \\ &\mathbf{h}_1, \ldots, \mathbf{h}_{(k-1)}, \mathbf{h}_{(k+1)}, \ldots, \mathbf{h}_K], \end{aligned} \tag{13}$$

where $\widetilde{\mathbf{R}}_k \in \mathbb{C}^{N\times(2K-2)}$, $\mathbf{f}_k$ is the channel of the k-th UE, while $\mathbf{h}_k$ is the channel of the k-th Eve. We apply SVD to $\widetilde{\mathbf{R}}_k$ and decompose it as

$$\widetilde{\mathbf{R}}_k = [\bar{\mathbf{V}}^{(1)}_k \ \bar{\mathbf{V}}^{(0)}_k] \begin{bmatrix} \bar{\mathbf{\Lambda}}_k & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \bar{\mathbf{U}}^H_k, \tag{14}$$

where $\bar{\mathbf{\Lambda}}_k \in \mathbb{C}^{r_k\times r_k}$ is a rank-r_k diagonal matrix with non-negative singular values, $\bar{\mathbf{V}}^{(1)}_k \in \mathbb{C}^{N\times r_k}$ and $\bar{\mathbf{V}}^{(0)}_k \in \mathbb{C}^{N\times(N-r_k)}$ are complex unitary matrices containing the vectors corresponding to the non-zero and zero singular values, respectively, and $\bar{\mathbf{U}}_k \in \mathbb{C}^{(2K-2)\times(2K-2)}$ is a complex unitary matrix.

Note that $\bar{\mathbf{V}}^{(0)}_k$ constitutes an orthogonal basis for the null space of $\widetilde{\mathbf{R}}_k$. The dimension of the null space must be greater than 0, which implies that $N - r_k \geq 0$, where r_k represents the rank of $\widetilde{\mathbf{R}}_k$. This leads to the requirement $N \geq r_k$. With K UEs needing to perform SVD on their respective $\widetilde{\mathbf{R}}_k$ matrices while meeting the specified requirements, it follows that $N \geq \max(r_1, \ldots, r_K)$. In extreme cases, if $\widetilde{\mathbf{R}}_k$ has full column rank, then rank ($\widetilde{\mathbf{R}}_k$) = $2K-2$. Therefore, N must satisfy the condition $N \geq (2K-2)$. Since our paper focuses on XL-MIMO systems with a large number of antennas, this condition is likely to be satisfied. To let the k-th UE generate secret keys, the BS injects artificial randomness in the direction of $\mathbf{R}_k = \bar{\mathbf{V}}^{(0)}_k \mathbf{\Sigma}_k (\bar{\mathbf{V}}^{(0)}_k)^H \in \mathbb{C}^{N\times N}$, where $\mathbf{\Sigma}_k \in \mathbb{C}^{(N-r_k)\times(N-r_k)}$ is a diagonal matrix with identical diagonal elements $1/(N-r_k)$.

We define

$$\widetilde{\mathbf{R}}_{ek} = [\mathbf{f}_1, \ldots, \mathbf{f}_K, \mathbf{h}_1, \ldots, \mathbf{h}_{(k-1)}, \mathbf{h}_{(k+1)}, \ldots, \mathbf{h}_K], \tag{15}$$

where $\widetilde{\mathbf{R}}_{ek} \in \mathbb{C}^{N\times(2K-1)}$. To prevent the k-th Eve from eavesdropping, the BS injects noise through $\widetilde{\mathbf{R}}_{ek}$. We apply SVD to $\widetilde{\mathbf{R}}_{ek}$ and express it as

$$\bar{\mathbf{R}}_{ek} = [\bar{\mathbf{V}}^{(1)}_{ek} \ \bar{\mathbf{V}}^{(0)}_{ek}] \begin{bmatrix} \bar{\mathbf{\Lambda}}_{ek} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \bar{\mathbf{U}}^H_{ek}, \tag{16}$$

where $\bar{\mathbf{\Lambda}}_{ek} \in \mathbb{C}^{r_{ek}\times r_{ek}}$ is a rank-r_{ek} diagonal matrix with non-negative singular values, $\bar{\mathbf{V}}_{ek}^{(1)} \in \mathbb{C}^{N\times r_{ek}}$ and $\bar{\mathbf{V}}_{ek}^{(0)} \in \mathbb{C}^{N\times(N-r_{ek})}$ are complex unitary matrices containing the vectors corresponding to the non-zero and zero singulars, respectively, and $\bar{\mathbf{U}}_{ek} \in \mathbb{C}^{(2K-1)\times(2K-1)}$ is a complex unitary matrix. Specially, $\bar{\mathbf{V}}_{ek}^{(0)}$ constitutes an orthogonal basis for the null space of $\bar{\mathbf{R}}_{ek}$. To prevent the k-th Eve from eavesdropping, the BS injects artificial randomness to the direction of $\mathbf{R}_{ek} = \bar{\mathbf{V}}_{ek}^{(0)}\mathbf{\Sigma}_{ek}(\bar{\mathbf{V}}_{ek}^{(0)})^H \in \mathbb{C}^{N\times N}$, where $\mathbf{\Sigma}_{ek} \in \mathbb{C}^{(N-r_{ek})\times(N-r_{ek})}$ is a diagonal matrix with identical diagonal element $1/(N-r_{ek})$.

Notably, we assume that the eavesdroppers are passive but act as curious users within the same network, whose CSI is known at the BS. Given the knowledge of all non-target UEs and eavesdroppers' channels, i.e., $\mathbf{f}_{k'}$ and $\mathbf{h}_{k'}$ for $k' \neq k$, the BS constructs a composite matrix $\widetilde{\mathbf{R}}_k$ and finds its nullspace $\bar{\mathbf{V}}_k^{(0)}$, which is used to design the precoder $\mathbf{w}_{S,k}$ for injecting artificial randomness into the k-th UE's channel. Similarly, based on the channel knowledge of $\mathbf{f}_k$ and $\mathbf{h}_{k'}$ for $k' \neq k$, the BS constructs another matrix $\widetilde{\mathbf{R}}_{ek}$ and computes its nullspace $\bar{\mathbf{V}}_{ek}^{(0)}$ to design the precoder $\mathbf{w}_{N,k}$ that suppresses eavesdropping at the k-th Eve. The near-field channels required for precoding can be obtained at the BS through uplink pilot-based channel estimation. To reduce the pilot overhead in extremely large-scale arrays, compressed sensing techniques, such as orthogonal matching pursuit are adopted, as discussed in [37] and [31].

Define $\mathbf{W}_k = \mathbb{E}\{\mathbf{w}_k\mathbf{w}_k^H\} \in \mathbb{C}^{N\times N}$ as the pilot covariance matrix for the k-th UE. Based on (14) and (16), we decompose the pilot covariance matrix as $\mathbf{W}_k = P_{S,k}\mathbf{R}_k + P_{N,k}\mathbf{R}_{ek}$, where $P_{S,k}$ is the transmit power for the k-th UE to generate secret keys and $P_{N,k}$ is the transmit power to prevent the k-th Eve from eavesdropping. Note that $\mathbf{R}_k$ is the covariance matrix for injecting secret keys, while $\mathbf{R}_{ek}$ is the covariance matrix for suppressing eavesdropping.

In near-field communications, the UEs have distinct spatial angles or distances, enabling the BS to distinguish them. The proposed SVD-based precoding method utilizes this by identifying the null space corresponding to other UEs. Specifically, when the precoding vector of UE i (where $i \neq k$) lies in the null space of the k-th UE, the following condition holds:

$$\mathbf{f}_k^H\mathbf{w}_i = 0. \tag{17}$$

The interference from the k-th UE's precoding vector does not impact the measurements of other UEs. This approach mitigates the interference when the UEs share the same uplink and downlink pilots, thereby reducing the pilot overhead.

C. Secret Key Rate

Passive eavesdropping is a threat to key generation, in which listeners intercept the signals in an effort to guess the secret keys. According to [23], under the passive eavesdropping attack, the SKR is $I(z_{a_k}; z_{b_k}|z_{ae_k}, z_{be_k})$.

We assume that the k-th Eve is able to 1) receive the uplink pilot and downlink pilot from the k-th UE and BS, respectively; 2) be in close proximity to the k-th UE for experiencing correlated channels as the k-th UE. The correlation between the k-th UE's and the k-th Eve's near-field LoS channel combined with random precoding vector is $\rho = \mathbf{f}_k^H\mathbf{W}_k\mathbf{h}_k / \left(\sqrt{\mathbf{f}_k^H\mathbf{W}_k\mathbf{f}_k}\sqrt{\mathbf{h}_k^H\mathbf{W}_k\mathbf{h}_k}\right)$. Due to the differences in angles and distances between the k-th UE and the k-th Eve, the eavesdropper cannot estimate the same channel as the UE, thereby facilitating the key generation. Therefore, the SKR is simplified as

$$I(z_{a_k}; z_{b_k}|z_{ae_k}) = \log_2\left(\frac{|\mathbf{K}_{z_{a_k}z_{ae_k}}||\mathbf{K}_{z_{b_k}z_{ae_k}}|}{\sigma_{EE,k}^2|\mathbf{K}_{z_{a_k}z_{b_k}z_{ae_k}}|}\right). \tag{18}$$

The channel variances of the measurements are derived as

$$\begin{aligned}
\sigma_{AA,k}^2 &= \left(\sum\nolimits_{i=1}^K \mathbf{f}_i^H\right)\mathbb{E}\left\{\mathbf{w}_k\mathbf{w}_k^H\right\}\left(\sum\nolimits_{i=1}^K \mathbf{f}_i\right) + \widehat{\sigma}_{a_k}^2 \\
&\overset{(a)}{=} \mathbf{f}_k^H\mathbf{W}_k\mathbf{f}_k + \widehat{\sigma}_{a_k}^2, \\
\sigma_{BB,k}^2 &= \mathbf{f}_k^H\left(\sum\nolimits_{i=1}^K \mathbf{W}_i\right)\mathbf{f}_k + \widehat{\sigma}_{b_k}^2 = \mathbf{f}_k^H\mathbf{W}_k\mathbf{f}_k + \widehat{\sigma}_{b_k}^2, \\
\sigma_{EE,k}^2 &= \mathbf{h}_k^H\left(\sum\nolimits_{i=1}^K \mathbf{W}_i\right)\mathbf{h}_k + \widehat{\sigma}_{ae_k}^2 = \mathbf{h}_k^H\mathbf{W}_k\mathbf{h}_k + \widehat{\sigma}_{ae_k}^2, \\
\sigma_{AE,k}^2 &= \sigma_{BE,k}^2 = \mathbf{f}_k^H\mathbf{W}_k\mathbf{h}_k,
\end{aligned} \tag{19}$$

where (a) holds due to the SVD in Section III-B. We define $\sigma_{B,k}^2 \triangleq \mathbf{f}_k^H\mathbf{W}_k\mathbf{f}_k$ and $\sigma_{E,k}^2 \triangleq \mathbf{s}_k^H\mathbf{W}_k\mathbf{s}_k$.

Based on (19), the covariance matrices of the measurements in (18) are calculated as follows:

$$\begin{aligned}
\mathbf{K}_{z_{a_k}z_{ae_k}} &= \begin{bmatrix} \sigma_{AA,k}^2 & \sigma_{AE,k}^2 \\ (\sigma_{AE,k}^2)^* & \sigma_{EE,k}^2 \end{bmatrix}, \\
\mathbf{K}_{z_{b_k},z_{ae_k}} &= \begin{bmatrix} \sigma_{BB,k}^2 & \sigma_{BE,k}^2 \\ (\sigma_{BE,k}^2)^* & \sigma_{EE,k}^2 \end{bmatrix}, \\
\mathbf{K}_{z_{a_k}z_{b_k}z_{ae_k}} &= \begin{bmatrix} \sigma_{AA,k}^2 & \sigma_{B,k}^2 & \sigma_{AE,k}^2 \\ \sigma_{B,k}^2 & \sigma_{BB,k}^2 & \sigma_{BE,k}^2 \\ (\sigma_{AE,k}^2)^* & (\sigma_{BE,k}^2)^* & \sigma_{EE,k}^2 \end{bmatrix}.
\end{aligned} \tag{20}$$

The determinants of these three covariance matrices in (20) are calculated as follows:

$$\begin{aligned}
|\mathbf{K}_{z_{a_k}z_{ae_k}}| &= (\sigma_{B,k}^2 + \widehat{\sigma}_{a_k}^2)(\sigma_{E,k}^2 + \widehat{\sigma}_{ae_k}^2) - |\sigma_{AE,k}^2|^2, \\
|\mathbf{K}_{z_{b_k}z_{ae_k}}| &= (\sigma_{B,k}^2 + \widehat{\sigma}_{b_k}^2)(\sigma_{E,k}^2 + \widehat{\sigma}_{ae_k}^2) - |\sigma_{BE,k}^2|^2, \\
|\mathbf{K}_{z_{a_k}z_{b_k}z_{ae_k}}| &= (\sigma_{B,k}^2 + \widehat{\sigma}_{a_k}^2)(\sigma_{B,k}^2 + \widehat{\sigma}_{b_k}^2)(\sigma_{E,k}^2 + \widehat{\sigma}_{ae_k}^2) \\
&\quad - |\sigma_{AE,k}^2|^2(\widehat{\sigma}_{a_k}^2 + \widehat{\sigma}_{b_k}^2) - \sigma_{B,k}^4(\sigma_{E,k}^2 + \widehat{\sigma}_{ae_k}^2).
\end{aligned} \tag{21}$$

Substituting (21) into (18), the objective function is simplified as (22), which is shown at the top of the next page.

D. The Monotonicity of Secret Key Rate

Substituting $\alpha_k = \sigma_{B,k}^2 - \frac{\sigma_{AE,k}^4}{\sigma_{E,k}^2 + \widehat{\sigma}_{ae_k}^2}$ into (22), the argument X of the $\log_2(X)$ function in (22) is simplified as the function $f(\alpha_k)$ in terms of α_k, which is expressed as

$$f(\alpha_k) = 1 + \frac{\alpha_k^2}{(\widehat{\sigma}_{a_k}^2 + \widehat{\sigma}_{b_k}^2)\alpha_k + \widehat{\sigma}_{a_k}^2\widehat{\sigma}_{b_k}^2}. \tag{23}$$

$$I(z_{a_k};z_{b_k}|z_{ae_k})=\log_2\left(1+\frac{(\sigma_{B,k}^2-\frac{\sigma_{AE,k}^4}{\sigma_{E,k}^2+\widehat{\sigma}_{ae_k}^2})^2}{(\widehat{\sigma}_{a_k}^2+\widehat{\sigma}_{b_k}^2)(\sigma_{B,k}^2-\frac{\sigma_{AE,k}^4}{\sigma_{E,k}^2+\widehat{\sigma}_{ae_k}^2})+\widehat{\sigma}_{a_k}^2\widehat{\sigma}_{b_k}^2}\right). \tag{22}$$

We derive the first-order derivative of the objective function (23) in terms of α, which is given by

$$\frac{\partial f}{\partial \alpha_k}=\frac{(\widehat{\sigma}_{a_k}^2+\widehat{\sigma}_{b_k}^2)\alpha_k^2+2\widehat{\sigma}_{a_k}^2\widehat{\sigma}_{b_k}^2\alpha_k}{\left((\widehat{\sigma}_{a_k}^2+\widehat{\sigma}_{b_k}^2)\alpha_k+\widehat{\sigma}_{a_k}^2\widehat{\sigma}_{b_k}^2\right)^2}. \tag{24}$$

From (24), we find that $\frac{\partial f}{\partial \alpha_k}>0$ for $\alpha_k>0$. Therefore, the objective function in (22) increases monotonically with α_k. Next, we only have to maximize α_k. Notably, $\widehat{\sigma}_{b_k}^2$ is a constant value while $\widehat{\sigma}_{a_k}^2$ is influenced by $P_{a,k}$. Here, for simplicity, we consider the worst case that $\widehat{\sigma}_{a_k}^2=\frac{P_a\sigma_{a_k}^2}{VP_b}$. In Section V, we design a deep learning-based algorithm to optimize the actual objective function (22).

IV. SVD-Based Precoding Vector Design for SKR Optimization

The formulated optimization problem aims to maximize the SKR by jointly designing the phase shift vectors $\mathbf{w}_k$, given that the BS possesses information about the LoS channel. Under the assumption of equal noise powers for both the UE and the BS, denoted as $\sigma_b^2=\sigma_{b_1}^2=\cdots=\sigma_{b_K}^2$ and $\sigma_a^2=\sigma_{a_1}^2=\cdots=\sigma_{a_K}^2$, respectively, the optimization problem can be written as follows:

$$\begin{aligned}\text{(P1):}\ \max_{\{\mathbf{W}_k\},\{P_{a,k}\}}\ & \sum_{k=1}^{K}\log_2\left(1+\frac{\alpha_k^2}{(\widehat{\sigma}_a^2+\widehat{\sigma}_b^2)\alpha_k+\widehat{\sigma}_a^2\widehat{\sigma}_b^2}\right)\\ \text{s.t.}\ & \sum_{k=1}^{K}P_{a,k}\le P_{\max},\\ & \text{Tr}(\mathbf{W}_k)\le P_{a,k},\end{aligned} \tag{25}$$

where $\widehat{\sigma}_a^2=\frac{\sigma_a^2}{VP_b}$ and $\widehat{\sigma}_b^2=\frac{\sigma_b^2}{V}$. The first constraint ensures that the total power allocated to K UEs cannot exceed the maximum power limit $P_{\max}$. The second constraint ensures that the power allocated for the k-th UE to generate secret keys cannot surpass the limit $P_{a,k}$. Next, we design an alternating optimization algorithm to maximize the SKR of (P1).

A. Optimize $\mathbf{W}_k$

Considering the observations from Section III-D, where it was established that the SKR of the k-th UE monotonically increases with α_k, we proceed to design $\mathbf{W}_k$ to optimize α_k, while keeping $P_{a,k}$ fixed. When $P_{a,k}$ is determined, we formulate the optimization problem as follows:

$$\begin{aligned}\text{(P2):}\ \max_{\mathbf{W}_k}\ & \sigma_{B,k}^2-\frac{|\sigma_{AE,k}^2|^2}{\sigma_{E,k}^2+\widehat{\sigma}_{ae}^2}\\ \text{s.t.}\ & \text{Tr}(\mathbf{W}_k)\le P_{a,k},\end{aligned} \tag{26}$$

where $\widehat{\sigma}_{ae}^2=\frac{\sigma_{ae}^2}{V}$. Notably, we assume that the noise variances of Eves are equal, i.e., $\sigma_{ae}^2=\sigma_{ae_1}^2=\cdots=\sigma_{ae_K}^2$. Since the objective function of (P2) is non-concave, we introduce an SVD-based method in Section III-B to convert (P2) as follows:

$$\begin{aligned}\text{(P3):}\ \min_{\mathbf{W}_k}\ & \frac{\text{Tr}(\mathbf{W}_k\mathbf{A}_k\mathbf{W}_k\mathbf{B}_k)}{\text{Tr}(\mathbf{W}_k\mathbf{A}_k)+\widehat{\sigma}_{ae}^2}-\text{Tr}(\mathbf{W}_k\mathbf{B}_k)\\ \text{s.t.}\ & \text{Tr}(\mathbf{W}_k)\le P_{a,k},\\ & \mathbf{W}_k=\mathbf{W}_{S,k}+\mathbf{W}_{N,k},\end{aligned} \tag{27}$$

where $\mathbf{B}_k=\mathbf{f}_k\mathbf{f}_k^H\in\mathbb{C}^{N\times N}$, $\mathbf{A}_k=\mathbf{s}_k\mathbf{s}_k^H\in\mathbb{C}^{N\times N}$, $\mathbf{W}_k=\mathbf{W}_{S,k}+\mathbf{W}_{N,k}$, $\mathbf{W}_{S,k}=P_{S,k}\mathbf{R}_k\in\mathbb{C}^{N\times N}$, and $\mathbf{W}_{N,k}=P_{N,k}\mathbf{R}_{ek}\in\mathbb{C}^{N\times N}$. Therefore, $\text{Tr}(\mathbf{W}_k\mathbf{B}_k)=\text{Tr}(\mathbf{W}_{S,k}\mathbf{B}_k)=P_{S,k}\text{Tr}(\mathbf{R}_k\mathbf{B}_k)$.

Through mathematical steps, we can simplify the objective function of the optimization problem (P3) as shown in (28), which is presented at the top of the following page. The coefficients in (28) are presented as follows:

$$\begin{aligned}m_{1,k}&=\text{Tr}(\mathbf{R}_k\mathbf{A}_k\mathbf{R}_k\mathbf{B}_k)-\text{Tr}(\mathbf{R}_k\mathbf{A}_k)\text{Tr}(\mathbf{R}_k\mathbf{B}_k)\\&\quad+\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k)\text{Tr}(\mathbf{R}_k\mathbf{B}_k)-\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k\mathbf{R}_k\mathbf{B}_k),\\ m_{2,k}&=P_{a,k}\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k\mathbf{R}_k\mathbf{B}_k)-P_{a,k}\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k)\text{Tr}(\mathbf{R}_k\mathbf{B}_k)\\&\quad-\widehat{\sigma}_{ae}^2\text{Tr}(\mathbf{R}_k\mathbf{B}_k),\\ m_{3,k}&=\text{Tr}(\mathbf{R}_k\mathbf{A}_k)-\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k),\\ m_{4,k}&=P_{a,k}\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k)+\widehat{\sigma}_{ae}^2.\end{aligned} \tag{29}$$

By exploiting the simplicity of the objective function, we transform the objective function of the optimization problem (P3) into a function with respect to the power allocated for generating secret keys, $P_{S,k}$. The resulting optimization problem is expressed as follows:

$$\begin{aligned}\text{(P4):}\ \min_{P_{S,k}}\ & \frac{m_{1,k}P_{S,k}^2+m_{2,k}P_{S,k}}{m_{3,k}P_{S,k}+m_{4,k}}\\ \text{s.t.}\ & 0\le P_{S,k}\le P_{a,k}.\end{aligned} \tag{30}$$

To make the problem (P4) tractable, we can use the Dinkelbach method to rewrite the objective function of (P4) as follows:

$$\begin{aligned}\text{(P5):}\ \min_{P_{S,k}}\ & y(P_{S,k})\\ \text{s.t.}\ & 0\le P_{S,k}\le P_{a,k},\end{aligned} \tag{31}$$

where $y(P_{S,k})=m_{1,k}P_{S,k}^2+m_{2,k}P_{S,k}+\beta_k(m_{3,k}P_{S,k}+m_{4,k})$ and β_k is the slope parameter.

The algorithm for solving the problem (P5) is presented in **Algorithm 1**. In line 1, we set the initial power for generating secret keys as $P_{S,k}(0)=P_{a,k}$. From lines 2 to 5, for the t-th loop, we calculate the slope parameter $\beta_k(t)$. Given $\beta_k(t)$, we then find the optimized transmit power $P_{S,k}(t)$. Upon reaching the stopping criterion $|m_{1,k}P_{S,k}^2(t)+m_{2,k}P_{S,k}(t)-\beta_k(t)(m_{3,k}P_{S,k}(t)+m_{4,k})|\le\epsilon$, we designate $\beta_k(t)$ as the optimized value, where ϵ is an arbitrarily small error.

Consequently, following the aforementioned algorithm, we acquire the optimized values of $P_{S,k}$ for $k=1,\ldots,K$.

$$-\alpha_k = \frac{\text{Tr}(\mathbf{W}_k\mathbf{A}_k\mathbf{W}_k\mathbf{B}_k)}{\text{Tr}(\mathbf{W}_k\mathbf{A}_k)+\widehat{\sigma}_{ae}^2} - \text{Tr}(\mathbf{W}_k\mathbf{B}_k) = \frac{P_{S,k}^2\text{Tr}(\mathbf{R}_k\mathbf{A}_k\mathbf{R}_k\mathbf{B}_k)+P_{S,k}(P_{a,k}-P_{S,k})\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k\mathbf{R}_k\mathbf{B}_k)}{P_{S,k}\text{Tr}(\mathbf{R}_k\mathbf{A}_k)+(P_{a,k}-P_{S,k})\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k)+\widehat{\sigma}_{ae}^2} - P_{S,k}\text{Tr}(\mathbf{R}_k\mathbf{B}_k)$$
$$= \frac{m_{1,k}P_{S,k}^2+m_{2,k}P_{S,k}}{m_{3,k}P_{S,k}+m_{4,k}}. \tag{28}$$

Algorithm 1 Dinkelbach Algorithm

Input: $m_{1,k}$, $m_{2,k}$, $m_{3,k}$, $m_{4,k}$, $P_{a,k}$, ϵ;
Output: $P_{S,k}$, β_k, t.
1: Set $P_{S,k}(0)=P_{a,k}$, Set $t=1$;
2: **while** $|m_{1,k}P_{S,k}^2(t)+m_{2,k}P_{S,k}(t)-\beta_k(m_{3,k}P_{S,k}(t)+m_{4,k})|>\epsilon$ **do**
3: The slope parameter, $\beta_k(t)$, is calculated as follows: $\beta_k(t)=\frac{m_{1,k}P_{S,k}^2(t-1)+m_{2,k}P_{S,k}(t-1)}{m_{3,k}P_{S,k}(t-1)+m_{4,k}}$;
4: $P_{S,k}(t)=\arg\min\left\{y(0),y(P_{a,k}),y\left(\frac{\beta_k(t)m_{3,k}-m_{2,k}}{2m_{1,k}}\right)\right\}$, Set $t=t+1$;
5: **end while**

Moreover, we can express the pilot covariance matrix $\mathbf{W}_k$ as $\mathbf{W}_k=P_{S,k}\mathbf{R}_k+P_{N,k}\mathbf{R}_{ek}=P_{S,k}\mathbf{R}_k+(P_{a,k}-P_{S,k})\mathbf{R}_{ek}$.

B. Optimize $P_{a,k}$

With the pilot covariance matrices $\mathbf{W}_k$ for $k=1,\ldots,K$ determined, we now formulate α_k as follows:

$$-\alpha_k = \frac{\text{Tr}(\mathbf{W}_k\mathbf{A}_k\mathbf{W}_k\mathbf{B}_k)}{\text{Tr}(\mathbf{W}_k\mathbf{A}_k)+\widehat{\sigma}_e^2} - \text{Tr}(\mathbf{W}_k\mathbf{B}_k) = \frac{y_{1,k}P_{a,k}+y_{2,k}}{y_{3,k}P_{a,k}+y_{4,k}}, \tag{32}$$

where

$$\begin{aligned}
y_{1,k} &= P_{S,k}(\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k\mathbf{R}_k\mathbf{B}_k)-\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k)\text{Tr}(\mathbf{R}_k\mathbf{B}_k)),\\
y_{2,k} &= P_{S,k}^2(\text{Tr}(\mathbf{R}_k\mathbf{A}_k\mathbf{R}_k\mathbf{B}_k)-\text{Tr}(\mathbf{R}_k\mathbf{A}_k)\text{Tr}(\mathbf{R}_k\mathbf{B}_k)\\
&\quad+\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k)\text{Tr}(\mathbf{R}_k\mathbf{B}_k)-\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k\mathbf{R}_k\mathbf{B}_k))\\
&\quad-P_{S,k}\widehat{\sigma}_{ae}^2\text{Tr}(\mathbf{R}_k\mathbf{B}_k),\\
y_{3,k} &= \text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k),\\
y_{4,k} &= P_{S,k}(\text{Tr}(\mathbf{R}_k\mathbf{A}_k)-\text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k))+\widehat{\sigma}_{ae}^2.
\end{aligned} \tag{33}$$

Based on the coefficients given in (33), the objective function (34) expressed in terms of $P_{a,k}$ is presented at the top of the following page, where

$$\begin{aligned}
z_{1,k} &= -(\widehat{\sigma}_a^2+\widehat{\sigma}_b^2)y_{1,k}y_{3,k}+\widehat{\sigma}_a^2\widehat{\sigma}_b^2y_{3,k}^2+y_{1,k}^2,\\
z_{2,k} &= -(\widehat{\sigma}_a^2+\widehat{\sigma}_b^2)(y_{1,k}y_{4,k}+y_{2,k}y_{3,k})+2\widehat{\sigma}_a^2\widehat{\sigma}_b^2y_{3,k}y_{4,k}\\
&\quad+2y_{1,k}y_{2,k},\\
z_{3,k} &= -(\widehat{\sigma}_a^2+\widehat{\sigma}_b^2)y_{2,k}y_{4,k}+\widehat{\sigma}_a^2\widehat{\sigma}_b^2y_{4,k}^2+y_{2,k}^2,\\
z_{4,k} &= -(\widehat{\sigma}_a^2+\widehat{\sigma}_b^2)y_{1,k}y_{3,k}+\widehat{\sigma}_a^2\widehat{\sigma}_b^2y_{3,k}^2,\\
z_{5,k} &= -(\widehat{\sigma}_a^2+\widehat{\sigma}_b^2)(y_{1,k}y_{4,k}+y_{2,k}y_{3,k})+2\widehat{\sigma}_a^2\widehat{\sigma}_b^2y_{3,k}y_{4,k},\\
z_{6,k} &= -(\widehat{\sigma}_a^2+\widehat{\sigma}_b^2)y_{2,k}y_{4,k}+\widehat{\sigma}_a^2\widehat{\sigma}_b^2y_{4,k}^2.
\end{aligned} \tag{35}$$

Given $\mathbf{W}_k$, we formulate the following optimization problem:

$$\text{(P6):}\ \max_{\{P_{a,k}\}}\ \sum\nolimits_{k=1}^{K} f_k(P_{a,k}) \quad \text{s.t.}\ \sum\nolimits_{k=1}^{K} P_{a,k}\le P_{\max}. \tag{36}$$

1) The Concavity of the Objective Function: We aim to find the optimized value of (P6) using the Lagrangian multiplier method. According to [38], the solution to a concave function over a convex solution set is guaranteed to be a global maximum. Thus, we first analyze the concavity of the objective function in (P6). We derive the first-order and second-order partial derivatives of $C_s=\sum_{k=1}^{K}C_k(P_{a,k})$ in (37) and (38), respectively, as shown at the top of the next page. The first-order partial derivative of C_s is greater than zero for $P_{a,k}\in[P_{S,k},+\infty]$, implying that the K functions are monotonically increasing. To check for concavity, the Hessian matrix should be semi-negative definite. As $\frac{\partial^2 C_s}{\partial P_{a,i}\partial P_{a,j}}=0$, the objective is concave if $\frac{\partial^2 C_s}{\partial P_{a,i}^2}\le 0$. The second-order partial derivative function is negative in the interval $P_{a,k}\in[P_{S,k},+\infty]$, indicating that each decomposed function is concave within this interval.

Therefore, by constraining the power within the concave interval, we can find the global maximum. We proceed to derive the Karush-Kuhn-Tucker (KKT) conditions for (P6). Based on the KKT conditions, we then propose a water-filling algorithm to obtain the optimized $P_{a,k}$ for $k=1,\ldots,K$.

2) Water-Filling Algorithm: We first derive the KKT condition of (P6). Moreover, we propose a water-filling algorithm to solve the problem with lower-bound constraints. The Lagrangian function with respect to $P_{a,k}$ is given by

$$f_{\text{Lag}}=C_s-\mu\left(\sum\nolimits_{k=1}^{K}P_{a,k}-P_{\max}\right), \tag{39}$$

where $\mu\ge 0$ is the water-filling level. The corresponding KKT conditions are

$$\begin{cases}\dfrac{\partial f_{\text{Lag}}}{\partial P_{a,k}}=y_k(P_{a,k})-\mu=0,\ \sum\nolimits_{k=1}^{K}P_{a,k}\le P_{\max},\\ \mu\left(\sum\nolimits_{k=1}^{K}P_{a,k}-P_{\max}\right)=0,\end{cases} \tag{40}$$

where $y_k(P_{a,k})$ is the increasing rate of the power allocated to the k-th UE. Define $g_k(\mu)$ as the inverse function of $y_k(P_{a,k})$. According to $y_k(P_{a,k})=\mu$, we get the relationship mapping from μ to $P_{a,k}$, i.e., $P_{a,k}=g_k(\mu)$.

Next, we transform the KKT conditions into the water-filling algorithm and find the solution. We use the water-filling algorithm to solve the problem (40), which is shown in **Algorithm 2**. Since it is hard to get a closed-form expression for $g_k(\mu)$, we introduce a two-dimensional bisection search

$$C_k(P_{a,k}) = \log_2\left(1 + \frac{(\frac{y_{1,k}P_{a,k}+y_{2,k}}{y_{3,k}P_{a,k}+y_{4,k}})^2}{-(\widehat{\sigma}_a^2+\widehat{\sigma}_b^2)(\frac{y_{1,k}P_{a,k}+y_{2,k}}{y_{3,k}P_{a,k}+y_{4,k}})+\widehat{\sigma}_a^2\widehat{\sigma}_b^2}\right) = \log_2\left(\frac{z_{1,k}P_{a,k}^2+z_{2,k}P_{a,k}+z_{3,k}}{z_{4,k}P_{a,k}^2+z_{5,k}P_{a,k}+z_{6,k}}\right). \tag{34}$$

$$\frac{\partial C_s}{\partial P_{a,k}} = \frac{2z_{1,k}P_{a,k}+z_{2,k}}{\ln 2(z_{1,k}P_{a,k}^2+z_{2,k}P_{a,k}+z_{3,k})} - \frac{2z_{4,k}P_{a,k}+z_{5,k}}{\ln 2(z_{4,k}P_{a,k}^2+z_{5,k}P_{a,k}+z_{6,k})}. \tag{37}$$

$$\frac{\partial^2 C_s}{\partial P_{a,k}^2} = \frac{-2z_{1,k}^2P_{a,k}^2-2z_{1,k}z_{2,k}P_{a,k}+2z_{1,k}z_{3,k}-z_{2,k}^2}{\ln 2(z_{1,k}P_{a,k}^2+z_{2,k}P_{a,k}+z_{3,k})^2} - \frac{-2z_{4,k}^2P_{a,k}^2-2z_{4,k}z_{5,k}P_{a,k}+2z_{4,k}z_{6,k}-z_{5,k}^2}{\ln 2(z_{4,k}P_{a,k}^2+z_{5,k}P_{a,k}+z_{6,k})^2}. \tag{38}$$

to calculate $P_{a,k}$ and μ, as shown in **Algorithm 2**. In line 1, we set the initial μ as $\mu = (\mu_{\min} + \mu_{\max})/2$. From lines 2 to 4, for all UEs, we apply the bisection search to find the initial $P_{a,k}$ to meet the requirement of $|y_k - \mu| \leq \epsilon_1$. From lines 6 to 14, we update $P_{a,k}$ and μ, and repeat it until $|\sum_{k=1}^{K} P_{a,k} - P_{\max}| \leq \epsilon_2$. When **Algorithm 2** is terminated, we get the final $P_{a,k}$ and μ. According to **Algorithm 2**, we obtain the optimized $P_{a,k}$, $k = 1, \ldots, K$.

Since $y_k(P_{a,k})$ monotonically decreases with respect to $P_{a,k}$, increasing μ leads to a smaller corresponding $P_{a,k}$, and vice versa. To determine the search interval for μ, we set $\mu_{\min} = 0$ so that the corresponding $P_{a,k}$ tends to infinity, and we choose a sufficiently large $\mu_{\max}$ such that the resulting $P_{a,k}$ becomes close to $P_{S,k}$ which is obtained from **Algorithm 1**. This ensures that the entire feasible power range $[P_{S,k}, P_{a,k}]$ is covered during the search.

The initialization of **Algorithm 2** requires setting several parameters, including the power constraint interval $[P_{S,k}, P_{\max}]$, the Lagrange multiplier interval $[0, \mu_{\max}]$, and the convergence tolerances ϵ_1 and ϵ_2 for the inner and outer loops, respectively. In our implementation, we set $\epsilon_1 = \epsilon_2 = 10^{-10}$. The parameter $y_k(P_{a,k})$ depends on a set of parameters $\{z_{1,k}, \ldots, z_{5,k}\}$, which are computed from the noise power and the near-field channels of both the legitimate UEs and the Eves.

We initiate the alternating optimization algorithm with $P_{a,1} = \cdots = P_{a,K}$. Subsequently, through alternate updates of the pilot covariance matrices $\mathbf{W}_k$ and transmit powers $P_{a,k}$, the objective function will be optimized.

Algorithm 2 Two-dimensional Bisection Algorithm

Input: $\{z_{i,k}\}$, $P_{\max}$, $\mu_{\max}$, $\mu_{\min}$, ϵ_1, ϵ_2;
Output: $\{P_{a,k}\}$, μ.
1: Set $\mu = (\mu_{\min} + \mu_{\max})/2$;
2: **for** $k = 1, \ldots, K$ **do**
3: Do bisection search of $P_{a,k}$ to satisfy $|y_k - \mu| \leq \epsilon_1$;
4: **end for**
5: **repeat**
6: **for** $k = 1, \ldots, K$ **do**
7: **if** $\sum_{k=1}^{K} P_{a,k} < P_{\max}$ **then**
8: $\mu_{\max} = \mu$;
9: **else**
10: $\mu_{\min} = \mu$;
11: **end if**
12: Set $\mu = (\mu_{\min} + \mu_{\max})/2$;
13: Do bisection search of $P_{a,k}$ to satisfy $|y_k - \mu| \leq \epsilon_1$;
14: **end for**
15: **until** $|\sum_{k=1}^{K} P_{a,k} - P_{\max}| \leq \epsilon_2$.

C. Obtaining precoding vectors

Based on $\mathbf{W}_k$, the precoding vector for key generation, $\mathbf{w}_{S,k}$, is expressed as $\mathbf{w}_{S,k} = \sum_{i=1}^{N-r_k} p_{k,i}\mathbf{u}_{k,i}$, where $p_{k,i}$ follows a complex Gaussian distribution with variance $P_{S,k}/(N-r_k)$ and $\mathbf{u}_{k,i}$ is the i-th column of $\bar{\mathbf{V}}_k^{(0)}$. Here, $\mathbf{u}_{k,i}$ denotes the beamforming weight vector to shape the transmitted signal's direction for key generation. The coefficient $p_{k,i}$, $i = 1, \ldots, N - r_k$, controls the amplitude of the signals to induce artificial randomness for generating secret keys.

Furthermore, the precoding vector for suppressing eavesdropping, $\mathbf{w}_{N,k}$, is defined as $\mathbf{w}_{N,k} = \sum_{i=1}^{N-r_{ek}} n_{k,i}\mathbf{v}_{k,i}$, where $n_{k,i}$ follows a complex Gaussian distribution with variance $P_{N,k}/(N - r_{ek})$ and $\mathbf{v}_{k,i}$ represents the i-th column of $\bar{\mathbf{V}}_{ek}^{(0)}$. Here, $\mathbf{v}_{k,i}$ signifies the beamforming weight vector tailored to direct the signal to prevent eavesdropping on secret keys by Eve. The coefficients $n_{k,i}$, $i = 1, \ldots, N - r_{ek}$, contribute to injecting random noise to prevent Eve from eavesdropping on secret keys.

Notably, our work aims to optimize the sum SKR in LoS near-field environments. The SKR is influenced by the artificial randomness observed at the legitimate user and the information leakage to the eavesdropper. To enhance key generation while mitigating information leakage, we adopt a two-stage precoding design. In the first stage, based on the SVD-based approach in Sec. III-B, we construct the $\mathbf{w}_k$ as a linear combination of two components: $\mathbf{w}_{S,k}$, which injects artificial randomness for the k-th UE, and $\mathbf{w}_{N,k}$, which generates interference to suppress eavesdropping by the k-th Eve. We further derive an analytical expression for the sum SKR. In the second stage, as detailed in Sec. IV, we aim to optimize the sum SKR by determining the total transmit power $P_{a,k}$ for each user and allocating it between the two components $\mathbf{w}_{S,k}$ and $\mathbf{w}_{N,k}$, denoted as $P_{S,k}$ and $P_{N,k} = P_{a,k} - P_{S,k}$, respectively. This

two-stage design enables both effective randomness injection and targeted eavesdropper suppression, thereby optimizing the overall sum SKR.

D. Complexity and Convergence

1) Complexity Analysis: The efficiency of the proposed algorithms is contingent upon two main factors: the number of iterations involved in the alternating maximization process, denoted as T_a, and the computational complexity associated with solving each sub-problem.

Algorithm 1 is designed to determine the optimized transmit power $P_{S,k}$ for the k-th UE to facilitate the generation of secret keys. According to [39], the complexity of the Dinkelbach algorithm depends on the iteration count and the complexity required to solve the convex problem in each iteration. In each iteration, a closed-form expression is given to find the optimized $P_{S,k}(t)$. Therefore, if the algorithm requires T_k iterations to get $P_{S,k}$, the complexity of the Dinkelbach algorithm is $\mathcal{O}(T_k)$. Considering there are K UEs, the total complexity of solving the first sub-optimization problem is $\mathcal{O}(KT_D)$, where $T_D = \max\{T_k\}$ is the maximum iteration count needed to find $P_{S,k}$ over K UEs. Based on [39], the Dinkelbach algorithm tends to converge rapidly toward the optimized solution and the rate of convergence may improve as the iterations proceed.

To solve the second sub-optimization problem, **Algorithm 1** is used to determine the optimized $P_{a,k}$. The complexity of **Algorithm 2** is determined by the precision parameters ϵ_1 and ϵ_2. In **Algorithm 2**, the inner bisection algorithm aims to find $P_{a,k}$ by solving the equation $y_k(P_{a,k}) = \mu$. The search interval is $[0, P_{a,k}]$. Thus, if the accuracy of the bisection search is ϵ_1, we have $\frac{P_{a,k}}{2^{T_{B,k}}} \leq \epsilon_1$, where $T_{B,k}$ is the iteration count. There are K equations to be solved, and as a result, the complexity becomes $\mathcal{O}(KT_B)$, where $T_B = \max\{T_{B,k}\}$. The outer bisection algorithm seeks to find μ to satisfy $\sum_{k=1}^{K} P_{a,k} = P_{\max}$. The search interval is $[\mu_{\min}, \mu_{\max}]$. If the accuracy of the bisection search is ϵ_2, then $\frac{\mu_{\max}-\mu_{\min}}{2^{T_P}} \leq \epsilon_2$, where T_P is the iteration count. The total complexity of **Algorithm 2** is $\mathcal{O}(KT_BT_P)$. According to the complexity of two sub-optimization problems, the total complexity of the alternative algorithm is $\mathcal{O}(T_aK(T_D + T_BT_P))$.

2) Convergence Analysis: According to [40], the max-ratio concave-convex Fractional Programming (FP) with Dinkelbach transform converges to the global optimum. Therefore, since the numerator of (P4) is convex and the denominator is concave, **Algorithm 1** seeks to minimize the objective function and make it converge to an optimized $P_{S,k}$. The convergence analysis of the bisection search is trivial. According to [41], if $y_k(P_{\min}) - \mu$ and $y_k(P_{\max}) - \mu$ have opposite signs, the inner bisection search can guarantee convergence to a solution from the interval $[P_{\min}, P_{\max}]$. For the outer bisection search, if $\sum_{k=1}^{K} g_k(\mu_{\min}) - P_{\max}$ and $\sum_{k=1}^{K} g_k(\mu_{\max}) - P_{\max}$ have different signs, the outer bisection search converges. Thus, the convergence of **Algorithm 2** hinges on the careful selection of the search interval.

According to [42] and [43], in each iteration, the alternating optimization algorithm seeks the optimized solution based on **Algorithm 1** and **Algorithm 2**, thereby ensuring a non-decreasing objective function. Furthermore, the algorithm guarantees convergence due to the upper bound constraint imposed by the power budget.

In this section, we divide the optimization problem into two sub-problems. By first optimizing the pilot covariance matrix $\mathbf{W}_k$ and then the transmit power for the k-th UE, $P_{a,k}$, we can iteratively solve these two sub-problems to improve the sum SKR. Given the non-convex nature of the problem, the SVD method decomposes $\mathbf{W}_k$ as $\mathbf{W}_k = P_{S,k}\mathbf{R}_k + P_{N,k}\mathbf{R}_{ek}$, where $P_{S,k}$ and $P_{N,k}$ are optimized in the first sub-problem. Consequently, this alternating optimization approach guarantees only a sub-optimal solution.

V. Deep Learning-Based Precoding Vector Design

The alternating optimization algorithm provides an optimized solution for (P1). However, the original objective function of (P1) fails to account for the influence of the precoding vectors $\{\mathbf{w}_k\}$, which directly affects the estimation noise. To accurately reflect the system's performance, it is necessary to modify the objective function to include the estimation noise caused by precoding. Thus, we define the actual objective function, taking into consideration the estimation noise after precoding, as follows:

$$f_p(\alpha_k) = \sum\nolimits_{k=1}^{K} \log_2\left(1 + \frac{\alpha_k^2}{(P_{a,k}\bar{\sigma}_a^2 + \widehat{\sigma}_b^2)\alpha_k + P_{a,k}\bar{\sigma}_a^2\widehat{\sigma}_b^2}\right). \tag{41}$$

The objective function (41) poses a challenge due to its complexity arising from the coupling of variables α_k and $P_{a,k}$. Notably, the determination of α_k relies on the precoding vector $\mathbf{w}_k$, further complicating the optimization problem. The interdependence between these variables necessitates a careful approach to address the coupled nature of $\mathbf{w}_k$ and $P_{a,k}$ and find an effective solution. Drawing inspiration from [27], we propose a novel deep-learning-based method to determine the optimized value of the SKR in near-field communications. The expression for α_k is provided in closed-form as shown in (28). However, it is worth noting that the multiplication of complex matrices $\mathbf{A}_k$, $\mathbf{B}_k$, and $\mathbf{W}_k$ presents a challenge for real-value deep learning networks to handle efficiently. We rewrite the analytical expression of α_k as

$$\alpha_k = P_{S,k}s_{5,k} - \frac{P_{S,k}^2 s_{1,k} + P_{S,k}P_{N,k}s_{3,k}}{P_{S,k}s_{2,k} + P_{N,k}s_{4,k} + \widehat{\sigma}_{ae}^2}, \tag{42}$$

where $s_{5,k} = \text{Tr}(\mathbf{R}_k\mathbf{B}_k)$, $s_{1,k} = \text{Tr}(\mathbf{R}_k\mathbf{A}_k\mathbf{R}_k\mathbf{B}_k)$, $s_{2,k} = \text{Tr}(\mathbf{R}_k\mathbf{A}_k)$, $s_{3,k} = \text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k\mathbf{R}_k\mathbf{B}_k)$, and $s_{4,k} = \text{Tr}(\mathbf{R}_{ek}\mathbf{A}_k)$. The power constraint is expressed as $\sum_{k=1}^{K}(P_{S,k} + P_{N,k}) = P_{\max}$.

To optimize (42), we introduce an unsupervised DNN-based power allocation algorithm, which we refer to as KGSVD-Net. The analytical expression for the sum SKR is determined by the coefficients $s_{n,k}$, which depend on the LoS near-field channels of the K UEs and Eves, as well as the transmit power. Through training, the DNN learns the complex relationships between these coefficients, the transmit power, and the values of $P_{S,k}$ and $P_{N,k}$. During the online inference phase, the

network directly outputs the optimized $P_{S,k}$ and $P_{N,k}$ once the coefficients $s_{n,k}$ and transmit power are provided. In contrast, the SVD precoding with a power allocation scheme depends on an iterative algorithm to maximize the sum SKR, requiring time to search for the optimized values and needing reoptimization whenever the parameters or transmit power change. The deep learning-based approach shifts the computational complexity to the training stage, thereby significantly reducing the workload during the online inference phase [27].

The KGSVD-Net architecture, illustrated in Fig. 3, is designed to take input tensors representing the BS's transmit power P_a (a 1×1 tensor) generated from the interval $[p_{\min}, p_{\max}]$ and coefficients $\{s_{1,k}, s_{2,k}, \ldots, s_{5,k}\}$ (a $5K \times 1$ tensor) generated from various intervals, such as $[r_{b_k,\min}, r_{b_k,\max}]$, $[r_{e_k,\min}, r_{e_k,\max}]$. The model leverages two fully connected (FC) layers as hidden layers for feature extraction, utilizing the ReLu activation function. The output layer consists of one $2K \times 1$ FC layer and one $2K \times 1$ normalization layer. The FC layer's output is denoted as $\mathbf{p}' = \left[P'_{S,1}, \ldots, P'_{S,K}, P'_{N,1}, \cdots, P'_{N,K}\right]^T$, where $P'_{S,1}$ to $P'_{S,K}$ represent the optimized values of the transmission powers for the UEs, and $P'_{N,1}$ to $P'_{N,K}$ represent the optimized values of the interference powers for the UEs. To satisfy the total power constraint, the normalization layer performs the necessary scaling of the output power values to ensure that the total allocated power across all UEs is within the specified range. By employing this architecture and leveraging the deep learning model, KGSVD-Net achieves effective power allocation, effectively optimizing the objective function (42) while respecting the constraints imposed on the total power. The normalization layer is given by

$$P_{N,k} = P_{\max} \frac{P'_{N,k}}{\sum_{k=1}^{K} P'_{S,k} + \sum_{k=1}^{K} P'_{N,k}}, \tag{43}$$

$$P_{S,k} = P_{\max} \frac{P'_{S,k}}{\sum_{k=1}^{K} P'_{S,k} + \sum_{k=1}^{K} P'_{N,k}}. \tag{44}$$

During the training phase, KGPA-Net updates its parameters through unsupervised learning with the aim of maximizing the SKR. This is accomplished by minimizing the loss function given by $Loss = -\frac{1}{N_m} \sum_{n=1}^{N_m} f_{p,n}(\alpha_k)$, where N_m is the number of training samples, α_k are the values calculated from (42) in the n-th training, and $f_{p,n}(\alpha_k)$ is the loss function calculated from (41) for the n-th sample. A smaller loss function corresponds to a higher average SKR. The DNN is updated using the stochastic gradient descent method (Adam optimizer) with a learning rate of 0.001. The training process is performed offline, resulting in lower computational complexity.

In the online inference phase, the BS allocates power directly to UEs based on the output of the trained neural network, as soon as it receives the power and $s_{n,k}$ calculated from the spatial angles and distances of UEs and Eves.

VI. Quantization

During the t-th channel probing, the BS applies a beamforming vector $\mathbf{w}_k$ to introduce randomness into the LoS channel by randomly configuring its amplitudes. Since $\mathbf{w}_k$ is reconfigured independently in each probing round, the resulting measurements become temporally random and statistically uncorrelated across different probings. This temporal randomness ensures that the quantized keys are sufficiently random for key generation. Specifically, the uplink and downlink measurements at the t-th probing, denoted by $z_{a_k}(t)$ and $z_{b_k}(t)$, follow the models in (11) and (5), respectively. After T_d probings, the BS and the k-th UE collect a sequence of random channel measurements $\mathbf{g}_{a_k} = [z_{a_k}(1), \ldots, z_{a_k}(T_d)]^T \in \mathbb{C}^{T_d \times 1}$ and $\mathbf{g}_{b_k} = [z_{b_k}(1), \ldots, z_{b_k}(T_d)]^T \in \mathbb{C}^{T_d \times 1}$.

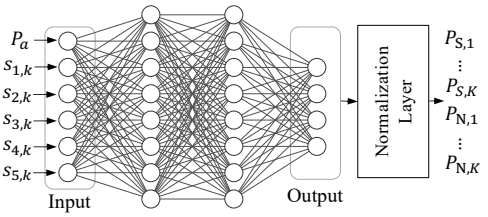

Fig. 3. KGSVD-Net architecture.

To verify the randomness of bit sequence after quantization, we construct the real-valued vectors $\bar{\mathbf{g}}_{a_k} = [\Re\{\mathbf{g}_{a_k}\}; \Im\{\mathbf{g}_{a_k}\}] \in \mathbb{R}^{2T_d \times 1}$ and $\bar{\mathbf{g}}_{b_k} = [\Re\{\mathbf{h}_{g_k}\}; \Im\{\mathbf{g}_{b_k}\}] \in \mathbb{R}^{2T_d \times 1}$. Following Algorithm 1 in [43], a one-bit quantizer is given by

$$k_{a_k}(i) = \begin{cases} 1, & \text{if } \bar{g}_{a_k}(i) > 0, \\ 0, & \text{if } \bar{g}_{a_k}(i) \leq 0, \end{cases} \tag{45}$$

where $\bar{g}_{a_k}(i)$ is the i-th element of $\bar{\mathbf{g}}_{a_k}$. The quantized bit sequence at the BS is denoted by $\mathbf{k}_{a_k} = [k_{a_k}(1), \ldots, k_{a_k}(2T_d)]^T$. The k-th UE applies the same quantization to obtain its own bit sequence $\mathbf{k}_{b_k}$.

Due to estimation errors, mismatches may occur between $\mathbf{k}_{a_k}$ and $\mathbf{k}_{b_k}$. We quantify the difference using the key disagreement rate (KDR) [6], defined as

$$\text{KDR} = \frac{1}{2T_d} \sum\nolimits_{i=1}^{2T_d} |k_{a_k}(i) - k_{b_k}(i)|, \tag{46}$$

where $k_{a_k}(i)$ and $k_{b_k}(i)$ denote the i-th bits in $\mathbf{k}_{a_k}$ and $\mathbf{k}_{b_k}$, respectively.

VII. Numerical Results

This section presents numerical results that demonstrate the efficiency of the proposed near-field key generation schemes.

A. Setup

The BS is equipped with a ULA comprising N antennas and positioned along the x-axis, with its central antenna located at the origin $(0, 0)$. The antennas are spaced at a distance of $d = \lambda/2$. The carrier frequency is set as $f_c = 30$ GHz. There are two UEs and the k-th UE, $k \in \{1, 2\}$, is situated at coordinates $\left(r_{b_k} \sin(\psi_{b_k}), r_{b_k} \sqrt{1 - \sin^2(\psi_{b_k})}\right)$, where r_{b_k} is the distance from the k-th UE to coordinate origin and ψ_{b_k} denotes the angle between the k-th BS-UE link and y-axis. There are two Eves and the k-th Eve eavesdrops on the k-th UE. The k-th Eve is situated at coordinates $\left(r_{e_k} \sin(\psi_{e_k}), r_{e_k} \sqrt{1 - \sin^2(\psi_{e_k})}\right)$, where r_{e_k} is the distance from the k-th Eve to coordinate

origin and ψ_{e_k} denotes the angle between the k-th BS-Eve link and y-axis. The transmit powers of the BS and the two UEs are configured to be equal, denoted as $P_t = P_a = P_b$ dBm.

The path-loss effect from $u \in \{b_1, b_2, e_1, e_2\}$ to the n-th antenna is $\beta_u^{(n)} = \beta_0 \left(\frac{d_0}{r_u^{(n)}}\right)^{\epsilon_u}$, where $\epsilon_u = 2$ is the path-loss exponent [36], [32], $\beta_0 = (\frac{\lambda}{4\pi})^2$ denotes the path-loss effect at $d_0 = 1$ m and $r_u^{(n)}$ is the distance from u to the n-th antenna.

The pilot length is set to $V = 1$. The noise powers for all components involved, namely $\sigma_0^2 = \sigma_a^2 = \sigma_b^2 = \sigma_e^2$, are identically set to -105 dBm [44]. Other parameters such as the transmnit power, the number of antennas, the angles and the distances of users and eavesdroppers vary with each scenario and are provided in the figure captions.

1) Considered Algorithms: The comparison and our proposed algorithms are described as follows:

(a) **Random Amplitude Scaling without Precoding (RAS w/o P):** The BS transmits pilot signals without any form of beamforming. To inject artificial randomness into the LoS channel, the pilot sequence of each user is scaled by a random coefficient p_k drawn from a zero-mean complex Gaussian distribution. Since no precoding is applied, this scheme cannot actively shape the transmission direction or suppress eavesdropping.

(b) **Maximal-Ratio Combining (MRC):** The BS applies MRC beamforming to let the precoding vector align the channel with the signal, $\mathbf{w}_k/\|\mathbf{w}_k\|_2 = \mathbf{f}_k/\|\mathbf{f}_k\|_2$ [35]. This process helps to enhance the signal-to-noise ratio (SNR) while mitigating the effects of noise.

(c) **SVD without Power Allocation (SVD w/o PA):** The design of the precoding vector is based on Section IV. The total transmit power $P_{\max}$ is equally allocated among K UEs, i.e., $P_{a,k} = P_{\max}/K$. For each UE, the $P_{a,k}$ is equally split between key generation and protection against eavesdropping, i.e., $P_{S,k} = P_{N,k} = P_{a,k}/2$.

(d) **SVD with Power Allocation (SVD w/ PA):** The design of precoding vector is based on Section IV. The transmit power allocated to generate secret keys and prevent Eve from eavesdropping is according to **Algorithms 1** and **2**. The transmit power to prevent Eve from eavesdropping is allocated to the orthogonal space that is perpendicular to the legitimate channel.

(e) **SVD with Deep-Learning-based Power Allocation (SVD w/ DLPA):** A deep learning network is designed to allocate power in the SVD-based precoding design, which was described in Section V.

B. Results of SKR

We evaluated the SKR against the spatial angles of Eves, the transmit power, the distances of Eves, and the number of transmit antennas.

Figure 4 illustrates the SKR versus the spatial angles of Eves. The spatial angles of Eves are defined as follows: $\psi_{e_1} = (\psi_{b_1} + \Delta\psi)$ radian, $\psi_{e_2} = (\psi_{b_2} + \Delta\psi)$ radian, where $\Delta\psi$ represents the variation along the y-axis. When Eve1 (Eve2) shares the same spatial angle with UE1 (UE2), the SKRs of all schemes are nearly 0. The spatial separation resulting from the differences in spatial angles causes the

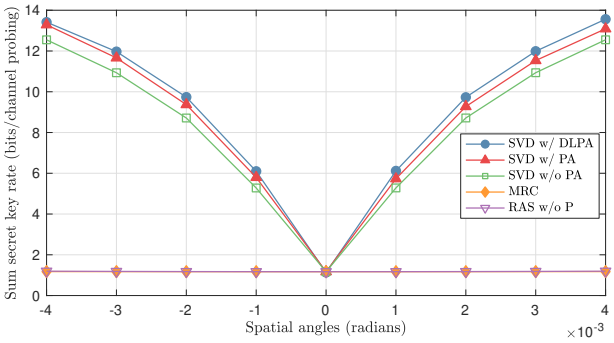

Fig. 4. Sum SKR versus the spatial angle of Eve. Here, $P_t = 20$ dBm, $N = 256$, $r_{b_1} = r_{e_1} = 12$ m, $r_{b_2} = r_{e_2} = 13$ m, $\psi_{b_1} = -1.5$ radians, and $\psi_{b_2} = 1.5$ radians.

near-field channels between Eves and UEs to become more uncorrelated. As a consequence, this enhanced uncorrelation in the near-field channels is the reason behind the improved performance of the SKR when $\Delta\psi$ deviates from 0. When there is a spatial angle between the UEs and Eves, the **SVD w/ PA** shows better performance than the **SVD w/o PA** scheme, which validates the performance of **Algorithms 1** and **2**. The difference in spatial angles enables the SVD-based precoding vector design to find sufficient legitimate and orthogonal spaces for **Algorithms 1** and **2** to allocate noise power. Compared to the **MRC** scheme, both the **SVD w/o PA**, **SVD w/ PA** and **SVD w/ DLPA** schemes demonstrate superior performance, indicating their ability to effectively utilize the differences in spatial angles to generate secret keys.

Figure 5 illustrates the SKR versus the transmit power when Eves and UEs share the same spatial angles but different distances. As the transmit power rises, the SNR also increases, consequently leading to a higher SKR. In scenarios where Eves share the same spatial angles with UEs, denoted by $\psi_{b_1} = \psi_{e_1} = -0.6$ and $\psi_{b_2} = \psi_{e_2} = 0.6$, it is still possible for the BS and UEs to extract secret keys from the LoS channel from the proposed schemes. This is feasible due to the disparity in distances between UEs and Eves in the near-field channel model, which provides sufficient space for the BS to achieve a better SNR in near-field communications, enabling successful key generation. The **MRC** scheme yields poor performance since it does not induce artificial noise to prevent Eve from eavesdropping. The k-th Eve is positioned very close to the k-th UE, resulting in a high correlation between $\mathbf{h}_k$ and $\mathbf{f}_k$. In the **MRC** scheme, the precoding vector $\mathbf{w}_k$ is aligned with $\mathbf{f}_k$. Consequently, the k-th Eve can eavesdrop on a significant portion of the secret keys, since its channel $\mathbf{h}_k$, when multiplied by the random precoding vector, is highly correlated with $\mathbf{f}_k$ multiplied by $\mathbf{w}_k$. This high correlation limits the secret key rate in the **MRC** scheme.

The **SVD w/o PA** scheme outperforms both the **MRC** and **RAS w/o PA** schemes, demonstrating the effectiveness of the proposed SVD-based precoding in shaping the transmit signal to enable key generation and to suppress eavesdropping. The **SVD w/ PA** scheme is slightly better than the **SVD w/o PA** scheme since the the alternating optimization algorithm in **Algorithms 1** and **2** enhances performance by jointly

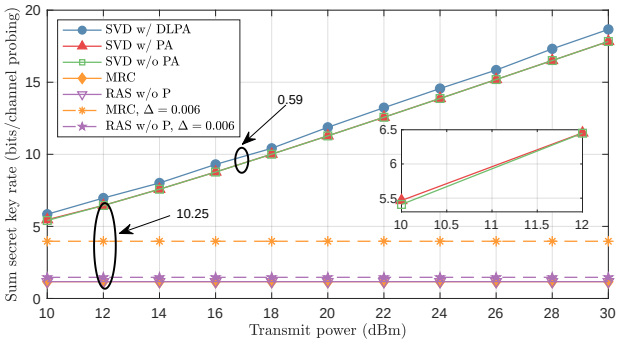

Fig. 5. Sum SKR versus the transmit power. Here, $N = 256$, $r_{b_1} = 12$ m, $r_{b_2} = 13$ m, $r_{e_1} = 11.98$ m, $r_{e_2} = 12.98$ m, $\psi_{b_1} = \psi_{e_1} = -0.6$ radians, and $\psi_{b_2} = \psi_{e_2} = 0.6$ radians.

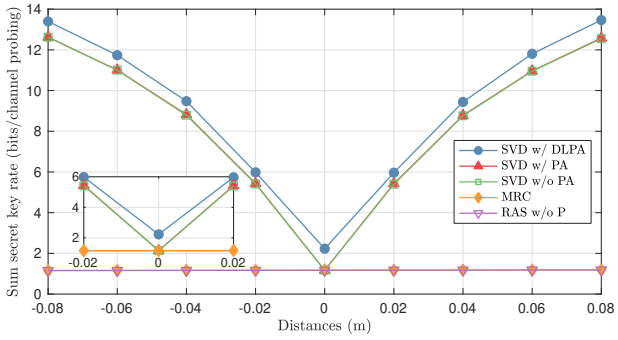

Fig. 6. Sum SKR versus the distance of Eve. Here, $P_t = 20$ dBm, $N = 256$, $r_{b_1} = 12$ m, $r_{b_1} = 13$ m, $\psi_{b_1} = \psi_{e_1} = -0.6$ radians and $\psi_{b_2} = \psi_{e_2} = 0.6$ radians.

optimizing the power allocation across UEs and dividing the transmit power between $P_{S,k}$ for key generation and $P_{N,k}$ for suppressing eavesdropping. However, the **SVD w/ PA** scheme does not show good performance since the difference in distances between Eve and the UE is not very large, so the SVD method cannot find sufficient legitimate and orthogonal spaces to conduct power allocation. Moreover, the objective function of the **SVD w/ PA** scheme is designed under a worst-case assumption, where the noise power is affected by the total transmit power $P_{\max}$. In contrast, the **SVD w/ DLPA** scheme improves the performance by directly optimizing the original non-convex objective, explicitly accounting for the impact of precoding on the noise at the BS. As a result, it provides a more effective power allocation for both key generation and preventing eavesdropping, compared to the **SVD w/ PA** scheme. Our simulation results show that the **SVD w/ DLPA** scheme achieves an average performance gain of 0.59 over the **SVD w/ PA** scheme.

In Fig. 5, compared to the **RAS w/o P** scheme, the proposed **SVD w/ PA** scheme achieves an average SKR gain of 10.25 over different transmit power levels. Since the **RAS w/o P** scheme applies no precoding and uses random coefficients, the SKR remains low, particularly when eavesdroppers are located close to the legitimate users with identical angles. Moreover, the sum SKR of the **RAS w/o P** scheme is close to that of the **MRC** scheme under these settings, as the legitimate UEs and their corresponding eavesdroppers have the same angles and only differ slightly in distance. To examine the impact of angular separation, we increase the angle of the k-th Eve by setting $\psi_{e_k} = \psi_{b_k} + \Delta$ with $\Delta = 0.006$. Under this setting, the gap between the **MRC** and **RAS w/o P** schemes becomes more significant. This is because **MRC** aligns with the near-field channels of legitimate users and injects artificial randomness into the LoS channel of the target UE, while the **RAS w/o P** scheme lacks a precoding mechanism to suppress eavesdropping or enhance randomness.

In Fig. 6, we illustrate the SKR when the distances of Eves vary. The distances of Eves are defined as follows: $r_{e_1} = (r_{b_1} + \Delta r)$ m, $r_{e_2} = (r_{b_2} + \Delta r)$ m, where Δr represents the variation with respect to the centre of antennas. When Eve1 (Eve2) and UE1 (UE2) have the same spatial angle of -0.6 (0.6) radians, the SKR of the **MRC** scheme exhibits an increasing trend with the growth of r_{e_1} and r_{e_2}. It is noteworthy that despite the increase in SKR as r_{e_1} and r_{e_2} rise, the overall SKR of the **MRC** scheme remains relatively low. In near-field communications, the distance difference can be used to help UEs have an advantage over Eves in generating secret keys. Other than Eve having the same distance and spatial angles as some UEs, the schemes in the near-field can generate secret keys. The SKR of the proposed schemes initially decrease, attaining their minimum values at $\Delta r = 0$ m and then increase as Δr varies. This behavior indicates that Eves' location is gradually shifting from being closer to the UEs to being farther away from UEs. The correlation between the near-field channels of UEs and Eves gets stronger when the Eves are gradually near the UEs. What is more, the proposed **SVD w/ DLPA** scheme shows better performance than the **SVD w/o PA** scheme.

In Fig. 7, we investigate the SKR versus the number of antennas. Increasing the number of antennas enhances the channel estimation accuracy, leading to an improved SKR in key generation systems. When the total number of antennas is not sufficiently large, the increase in the number of antennas does not significantly improve the SKR of the **MRC** scheme. While increasing the number of antennas can improve the resolution of spatial angles to distinguish potential Eves, the differences in spatial angles may not be obvious when the number of antennas is not large enough. However, the proposed **SVD w/o PA**, **SVD w/ PA** and **SVD w/ DLPA** schemes demonstrate improved performance, even in scenarios where Eves are in close proximity to UEs.

Figure 8 investigates the SKR versus the transmit power in the case of 4 UEs and 6 UEs. The dashed curves represent the SKR of the proposed and the comparison schemes for 6 UEs while the solid curves represent the SKR of the proposed and the comparison schemes for 4 UEs. The **SVD w/ PA** and the **SVD w/ DLPA** schemes can be applied to the scenario where the number of UEs is over 2. When the number of UEs increases, the total SKR of the system increases. The distance in the spatial angles and distances between UEs can be applied to generate secret keys simultaneously with the BS.

C. Results of KDR and Randomness

We investigate the KDR and the randomness of secret keys.

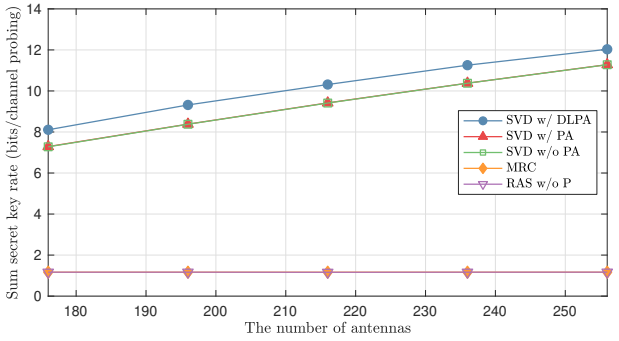

Fig. 7. Sum SKR versus the number of antennas. Here, $P_t = 20$ dBm, $r_{b_1} = 12$ m, $r_{b_2} = 13$ m, $r_{e_1} = 11.98$ m, $r_{e_2} = 12.98$ m, $\psi_{b_1} = \psi_{e_1} = -0.6$ radians, and $\psi_{b_2} = \psi_{e_2} = 0.6$ radians.

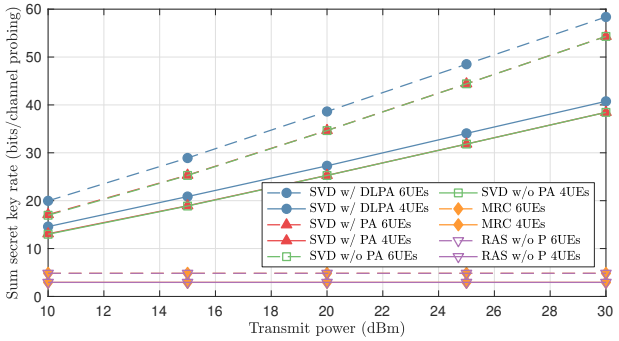

Fig. 8. Sum SKR versus the transmit power for the cases of 4 and 6 UEs. Here, $N = 256$, $r_{b_1} = 12$ m, $r_{b_2} = 13$ m, $r_{b_3} = 12$ m, $r_{b_4} = 13$ m, $r_{b_5} = 12$ m, $r_{b_6} = 13$ m, $r_{e_1} = 11.98$ m, $r_{e_2} = 12.98$ m, $r_{e_3} = 11.98$ m, $r_{e_4} = 12.98$ m, $r_{e_5} = 11.98$ m, $r_{e_6} = 12.98$ m, $\psi_{b_1} = \psi_{e_1} = -0.7$ radians, $\psi_{b_2} = \psi_{e_2} = -0.6$ radians, $\psi_{b_3} = \psi_{e_3} = -0.5$ radians, $\psi_{b_4} = \psi_{e_4} = 0.5$ radians, $\psi_{b_5} = \psi_{e_5} = 0.6$ radians, and $\psi_{b_6} = \psi_{e_6} = 0.7$ radians.

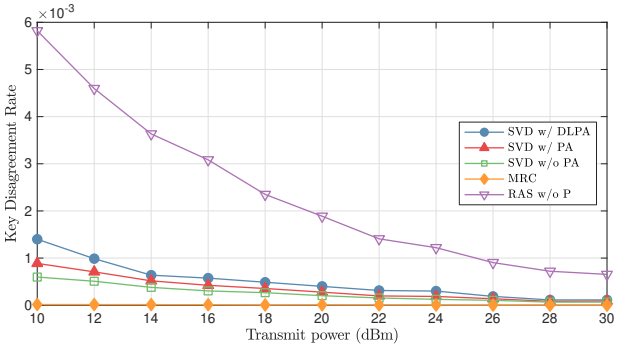

Fig. 9. Sum KDR versus the transmit power. Here, $N = 256$, $r_{b_1} = 12$ m, $r_{b_2} = 13$ m, $r_{e_1} = 11.98$ m, $r_{e_2} = 12.98$ m, $\psi_{b_1} = \psi_{e_1} = -0.6$ radians, and $\psi_{b_2} = \psi_{e_2} = 0.6$ radians.

Figure 9 evaluates the KDR performance as a function of the transmit power. A total of 10,000 channel probings are conducted, and the resulting quantized sequences are used to compute the KDR. It can be observed that the KDR decreases with increasing transmit power, as a higher SNR leads to fewer discrepancies between the channel measurements of Alice and Bob. The KDR of the **MRC** scheme is nearly zero and lower than that of the other schemes, since **MRC** precoding directly aligns with the channels of the UEs, resulting in the highest SNR for channel estimation. In contrast, the SVD-based precoding allocates power not only for key generation with UEs but also for interfering with Eves, which reduces the power allocated to legitimate UEs and thus degrades the SNR. The KDR of the **RAS w/o P** scheme is the highest, as no directional precoding is applied to focus energy toward the UEs, resulting in the lowest SNR. The **SVD w/ PA** scheme exhibits a higher KDR than the **SVD w/o PA** scheme. In the **SVD w/o PA** scheme, the transmit power is equally divided between $\mathbf{w}_{S,k}$ and $\mathbf{w}_{N,k}$ for each UE. In contrast, the **SVD w/ PA** scheme employs a power allocation algorithm that dynamically adjusts the power split between $\mathbf{w}_{S,k}$ and $\mathbf{w}_{N,k}$ to maximize the SKR. However, to improve the overall SKR, the algorithm may reduce the power allocated to certain $\mathbf{w}_{S,k}$, especially for UEs with weaker channels, or in order to strengthen interference against eavesdroppers. As a result, the reduced power for $\mathbf{w}_{S,k}$ leads to a lower SNR and thus a higher KDR. Likewise, the KDR of the **SVD w/ DLPA** scheme is slightly higher than that of the **SVD w/ PA** scheme due to its further adjustment of power allocation.

TABLE I
RANDOMNESS TEST RESULTS

	SVD w/o PA	**SVD w/ PA**	**SVD w/ DLPA**
Frequency	0.915	0.93	0.07
Block frequency	0.53	0.52	0.66
Runs	0.22	0.23	0.81
Longest run of 1s	0.92	0.93	0.57
DFT	0.34	0.60	0.34
Serial	0.41	0.34	0.73
	0.18	0.11	0.93
Approx. entropy	0.90	0.89	0.29
Cumulative sums (Fwd)	0.79	0.80	0.08
Cumulative sums (Rev)	0.69	0.73	0.06

To evaluate the statistical randomness of the quantized bit sequences, we employ tests from the National Institute of Standards and Technology (NIST) statistical test suite [45]. Under the configuration of $N = 256$ antennas and a transmit power of $P_t = 15$ dBm, we carry out 10,000 rounds of channel probing. This yields 10,000 complex-valued measurements, which are converted into 20,000 binary bits by applying the one-bit quantization in Sec. VI to extract both the real and imaginary components. We then utilize the implementation provided by the toolbox in [46] to perform 9 selected NIST tests. A p-value greater than 0.01 indicates that the bit sequence passes the corresponding randomness criterion. As shown in Table I, all tests yield p-values above this threshold, validating the randomness of the quantized bit sequence. These results confirm that the temporal randomness induced by randomly configuring the amplitude of $\mathbf{w}_k$ produces statistically independent measurements, suitable for key generation after quantization.

VIII. Discussion

A. Passive Eavesdropping

If the eavesdropper's channel is unavailable, our SVD-based precoding method cannot identify the eavesdropper's null space and inject randomness to prevent eavesdropping on secret keys. Future communications systems with sensing

technologies, as suggested by [47], may estimate the eavesdroppers' channels. The BS may transmit probing signals and process the echoes to estimate each eavesdropper's angle and distances, as shown in [48], [49]. These estimated parameters could construct a near-field LoS channel estimate for each eavesdropper. However, uncertainty in the eavesdropper's CSI must be considered. While our method is based on the ideal assumption of perfect eavesdropper CSI, it serves as a theoretical benchmark that reveals the potential performance limits. These results offer guidance for future systems where partial eavesdropper information may be available through emerging sensing technologies.

B. NLoS Channels

Our work focuses on LoS environments where the inherent randomness of the channel is limited. If NLoS paths exist, their randomness can be used for key generation. Under these circumstances, the channel model can be extended as $\mathbf{f}_k = \sqrt{N}\mathbf{c}(\psi_{b_k}, r_{b_k}) + \sqrt{\frac{N}{D_k}} \sum_{j=1}^{D_k} \alpha_{k,j}\mathbf{c}(\psi_{b_k,j}, r_{b_k,j})$, where D_k is the number of paths, $\alpha_{k,j}$ is the complex gain, $\psi_{b_k,j}$ is the spatial angle, and $r_{b_k,j}$ is the distance of the j-th NLoS path. Our current precoding vector can be designed to lie in the nullspace of the NLoS components, $\mathbf{b}_{k,j} = \sqrt{\frac{N}{D_k}}\alpha_{k,j}\mathbf{a}(\psi_{b_k,j}, r_{b_k,j})$, to suppress their influence and retain the effectiveness of the LoS-based scheme. Alternatively, to extract randomness from the NLoS components, additional beamformers can be designed to lie in the nullspace of the LoS path, thereby suppressing its influence. Since LoS and NLoS components have different channel variances, transmit power should be allocated properly—either to use NLoS randomness directly or to inject artificial randomness into the LoS path.

IX. Conclusion

This paper investigated the PLKG in near-field multi-user communications. We used precoding vectors to induce artificial randomness to the LoS channels to generate secret keys at the BS and UEs and prevent Eves from eavesdropping. We proposed a multi-user channel probing protocol that leverages the difference in the distance of UEs in near-field communications, which achieves non-orthogonal pilots. We also derived the SKR and proposed an alternating optimization algorithm to allocate the noise power for generating secret keys and the noise for preventing Eves from eavesdropping. To mitigate the influence of noise after precoding, we designed a deep learning-based power allocation method, which further improves the SKR. Our theoretical results were validated in terms of the transmit power, the distance of Eves, the spatial angle of Eves, and the number of antennas. Even if Eve shares the same spatial angles as the UE and when Eve is positioned closer to the BS than the UE, the key generation scheme in the near-field can still produce secret keys.

References

[1] T. Lu, L. Chen, C. Chen, T. Q. Duong, and M. Matthaiou, "Precoding design for key generation in near-field extremely large-scale MIMO communications," in *Proc. IEEE GLOBECOM*, Dec. 2023, pp. 1–6.

[2] J. Zhang, E. Björnson, M. Matthaiou, D. W. K. Ng, H. Yang, and D. J. Love, "Prospective multiple antenna technologies for beyond 5G," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1637–1660, Aug. 2020.

[3] H. Lu and Y. Zeng, "Communicating with extremely large-scale array/surface: Unified modeling and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 4039–4053, Jun. 2022.

[4] Y. Han, S. Jin, M. Matthaiou, T. Q. S. Quek, and C.-K. Wen, "Toward extra large-scale MIMO: New channel properties and low-cost designs," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14 569–14 594, Aug. 2023.

[5] M. Matthaiou, O. Yurduseven, H. Q. Ngo, D. Morales-Jimenez, S. L. Cotton, and V. F. Fusco, "The road to 6G: Ten physical layer challenges for communications engineers," *IEEE Commun. Mag.*, vol. 59, no. 1, pp. 64–69, Jan. 2021.

[6] 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, Aug. 2020.

[7] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 2, pp. 1773–1828, Secondquarter 2019.

[8] 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.

[9] S. Yang, W. Lyu, Z. Hu, Z. Zhang, and C. Yuen, "Channel estimation for near-field XL-RIS-aided mmwave hybrid beamforming architectures," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 11 029–11 034, Aug. 2023.

[10] S. Yang, C. Xie, W. Lyu, B. Ning, Z. Zhang, and C. Yuen, "Near-field channel estimation for extremely large-scale reconfigurable intelligent surface (XL-RIS)-aided wideband mmwave systems," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 6, pp. 1567–1582, Jun. 2024.

[11] S. Yang, H. Chen, W. Liu, X.-P. Zhang, and C. Yuen, "Near-field channel estimation and localization: Recent developments, cooperative integration, and future directions," *IEEE Signal Process. Mag.*, vol. 42, no. 1, pp. 60–73, Jan. 2025.

[12] J. An, C. Yuen, L. Dai, M. Di Renzo, M. Debbah, and L. Hanzo, "Near-field communications: Research advances, potential, and challenges," *IEEE Trans. Wireless Commun.*, vol. 31, no. 3, pp. 100–107, Jun. 2024.

[13] H. Lu *et al.*, "A tutorial on near-field XL-MIMO communications towards 6G," *IEEE Commun. Surv. Tutorials*, vol. 26, no. 4, pp. 1–45, Fourthquarter 2024.

[14] H. Zhang, N. Shlezinger, F. Guidi, D. Dardari, and Y. C. Eldar, "6G wireless communications: From far-field beam steering to near-field beam focusing," *IEEE Commun. Mag.*, vol. 61, no. 4, pp. 72–77, Apr. 2023.

[15] M. Cui, Z. Wu, Y. Lu, X. Wei, and L. Dai, "Near-field MIMO communications for 6G: Fundamentals, challenges, potentials, and future directions," *IEEE Commun. Mag.*, vol. 61, no. 1, pp. 40–46, Jan. 2023.

[16] D. Guo, D. Ma, J. Xiong, X. Liu, and J. Wei, "On the secret-key capacity over multipath fading channel," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 6044–6054, May 2024.

[17] N. Wang, J. Duan, B. Chen, S. Guo, T. Xiang, and K. Zeng, "Efficient group key generation based on satellite cluster state information for drone swarm," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 4464–4479, Mar. 2024.

[18] M. G. Madiseh, S. W. Neville, and M. L. McGuire, "Applying beamforming to address temporal correlation in wireless channel characterization-based secret key generation," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 4, pp. 1278–1287, Aug. 2012.

[19] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

[20] G. Li, Y. Xu, W. Xu, E. Jorswieck, and A. Hu, "Robust key generation with hardware mismatch for secure MIMO communications," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 5264–5278, Nov. 2021.

[21] 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, Jun. 2024.

[22] H. Liu, Y. Wang, Y. Ren, and Y. Chen, "Bipartite graph matching based secret key generation," in *Proc. IEEE INFOCOM*, May 2021, pp. 1–10.

[23] R. Mehmood, J. W. Wallace, and M. A. Jensen, "Secure array synthesis," *IEEE Trans. Antennas Propag.*, vol. 63, no. 9, pp. 3887–3896, Sep. 2015.

[24] L. Jiao, N. Wang, and K. Zeng, "Secret beam: Robust secret key agreement for mmWave massive MIMO 5G communication," in *Proc. IEEE GLOBECOM*, Dec. 2018, pp. 1–6.

[25] S. Yun, J. M. Kang, I. M. Kim, and J. Ha, "Deep artificial noise: Deep learning-based precoding optimization for artificial noise scheme," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3465–3469, Mar. 2020.
[26] X. Zhang and M. Vaezi, "Multi-objective DNN-based precoder for MIMO communications," *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4476–4488, Jul. 2021.
[27] C. Chen, J. Zhang, T. Lu, M. Sandell, and L. Chen, "Secret key generation for IRS-assisted multi-antenna systems: A machine learning-based approach," *IEEE Trans. Inf. Forensics Secur.*, pp. 1086 – 1098, Nov. 2024.
[28] G. Li, C. Sun, W. Xu, M. DiRenzo, and A. Hu, "On maximizing the sum secret key rate for reconfigurable intelligent surface-assisted multiuser systems," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 211–225, Jan. 2022.
[29] J. Chu, R. Liu, M. Li, Y. Liu, and Q. Liu, "Joint secure transmit beamforming designs for integrated sensing and communication systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 4778–4791, Apr. 2023.
[30] E. Björnson, O. T. Demir, and L. Sanguinetti, "A primer on near-field beamforming for arrays and reconfigurable intelligent surfaces," in *Proc. IEEE ACSSC*, Jul. 2021, pp. 105–112.
[31] M. Cui and L. Dai, "Channel estimation for extremely large-scale MIMO: Far-Field or near-field?" *IEEE Trans. Commun.*, vol. 70, no. 4, pp. 2663–2677, Apr. 2022.
[32] H. Zhang, N. Shlezinger, F. Guidi, D. Dardari, M. F. Imani, and Y. C. Eldar, "Beam focusing for multi-user MIMO communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 7476–7490, Sep. 2022.
[33] R. Jin and K. Zeng, "Secure inductive-coupled near field communication at physical layer," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 12, pp. 3078–3093, Dec. 2018.
[34] Z. Wu and L. Dai, "Multiple access for near-field communications: SDMA or LDMA?" *IEEE J. Sel. Areas Commun.*, vol. 41, no. 6, pp. 1918–1935, Jun. 2023.
[35] X. Li, H. Lu, Y. Zeng, S. Jin, and R. Zhang, "Near-field modeling and performance analysis of modular extremely large-scale array communications," *IEEE Commun. Lett.*, vol. 26, no. 7, pp. 1529–1533, Jul. 2022.
[36] M. Cui, L. Dai, Z. Wang, S. Zhou, and N. Ge, "Near-field rainbow: Wideband beam training for XL-MIMO," *IEEE Trans. Wireless Commun.*, vol. 22, no. 6, pp. 3899–3912, Jun. 2023.
[37] X. Wei and L. Dai, "Channel estimation for extremely large-scale MIMO: Far-Field, near-field or hybrid-field?" *IEEE Commun. Lett.*, vol. 70, no. 4, pp. 2663–2677, Jan. 2022.
[38] B. T. Quist and M. A. Jensen, "Optimal channel estimation in beamformed systems for common-randomness-based secret key establishment," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 558–559, Jul. 2013.
[39] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.
[40] K. Shen and W. Yu, "Fractional programming for communication systems—Part I: Power control and beamforming," *IEEE Trans. Signal Process.*, vol. 66, no. 10, pp. 2616–2630, May 2018.
[41] E. Süli and D. F. Mayers, *An Introduction to Numerical Analysis*. Cambridge University Press, 2003.
[42] R. Long, Y.-C. Liang, Y. Pei, and E. G. Larsson, "Active reconfigurable intelligent surface-aided wireless communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 4962–4975, Aug. 2021.
[43] G. Zhou, C. Pan, H. Ren, K. Wang, and Z. Peng, "Secure wireless communication in RIS-aided MISO system with hardware impairments," *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1309–1313, Jun. 2021.
[44] Z. Zhang, Y. Liu, Z. Wang, X. Mu, and J. Chen, "Physical layer security in near-field communications," *IEEE Trans. Veh. Technol.*, vol. 73, no. 7, pp. 10 761–10 766, Jul. 2024.
[45] 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.
[46] K. A. Steven. Randomness testsuite. GitHub repository. Accessed Mar. 27, 2022. [Online]. Available: https://github.com/stevenang/randomness_testsuite
[47] N. Su, F. Liu, and C. Masouros, "Sensing-assisted eavesdropper estimation: An ISAC breakthrough in physical layer security," *IEEE Trans. on Wireless Commun.*, vol. 23, no. 4, pp. 3162–3174, Apr. 2024.
[48] Z. Wang, X. Mu, and Y. Liu, "Near-field integrated sensing and communications," *IEEE Commun. Lett.*, vol. 27, no. 8, pp. 2048–2052, Aug. 2023.
[49] Y. Cao, L. Duan, and R. Zhang, "Sensing for secure communication in ISAC: Protocol design and beamforming optimization," *IEEE Trans. Wireless Commun.*, vol. 24, no. 2, pp. 1207–1220, Feb. 2025.