Precoding Design for Key Generation in Near-Field Extremely Large-Scale MIMO Communications

Tianyu Lu*, Liquan Chen*†, Junqing Zhang‡, Chen Chen‡, Trung Q. Duong§, and Michail Matthaiou§
*School of Cyber Science and Engineering, Southeast University, Nanjing, 210096, China
†Purple Mountain Laboratories, Nanjing, 210096, China
‡Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, U.K.
§Centre for Wireless Innovation (CWI), Queen's University Belfast, Belfast, BT7 1NN, U.K.
Corresponding author: Liquan Chen, Email: lqchen@seu.edu.cn

***Abstract*—This paper investigates an artificial randomness-based key generation scheme in near-field extremely large-scale multiple-input multiple-output (XL-MIMO) communications, aiming to overcome the limitations of static wireless channels in generating secret keys. The proposed approach introduces artificial randomness via the precoding vector, enabling legitimate users to generate secret keys while preventing eavesdropping. To maximize the secret key rate (SKR), the singular value decomposition (SVD) method is utilized to identify the legitimate subspace for generating secret keys and its orthogonal subspace to thwart eavesdropping. Additionally, a Dinkelbach method-based power allocation algorithm is designed to inject noise into both the legitimate subspace and its orthogonal subspace. Our simulation results validate the efficiency of the proposed key generation scheme, demonstrating its superiority over existing approaches.**

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

I. Introduction

Significant research has been dedicated to developing advanced technologies, such as millimetre-wave (mmWave)/Tera Hertz (THz) networks as well as XL-MIMO, to meet the increasing requirements for widespread connectivity in the sixth generation (6G) wireless communications [1]. Ensuring secure communication services is a crucial objective for 6G networks. Alongside cryptographic techniques, physical layer key generation (PLKG) leverages channel randomness, channel reciprocity, and spatial decorrelation properties to generate secure keys [2], without introducing complicated key distribution and management procedures.

The advent of XL-MIMO systems [3] 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) field. The EM radiation field can be categorized into two regions: the far-field and the radiating near-field regions [3]. The Rayleigh distance acts as the boundary that separates these two distinct regions [4]. Beyond the Rayleigh distance is the far-field region, where the propagation channel model is based on planar waves (PWs). Within the Rayleigh distance, on the other hand, the spherical waves (SWs) channel model is applied [4]. Consequently, this transition towards near-field communications introduces unique characteristics to PLKG.

Current PLKG research concentrates on sub-6GHz systems with a focus on far-field scenarios. PLKG experiences significant challenges in sub-6GHz scenarios characterized by poor channel conditions, particularly when the channel variation is slow, such as in static environments. Madiseh *et al.* utilized the random beamforming within a MIMO system to simulate artificial "fast fading" channels, thereby improving the SKR in scenarios with slow channel variations [5]. However, a limitation of random beamforming arises when the direct channel is blocked or exhibits poor quality. In response, Ding *et al.* introduced the retrodirective array (RDA) concept as an alternative solution to induce artificial noise [6]. A RDA is particularly effective in scenarios where the direct channel is obstructed or has low quality. Aldaghri *et al.* proposed the implementation of an untrusted relay for generating secret keys in static conditions [7]. Lu *et al.* utilized a reconfigurable intelligent surface (RIS) as a passive technique to address the low-entropy problem in PLKG [8]. Gao *et al.* conducted prototype experiments to validate the feasibility of RIS-assisted key generation in static settings [9].

To address the issue of static channels, it is typically assumed that there exists a disparity in spatial angles between Bob and the eavesdropper in far-field key generation systems. Alice leverages spatial angles as a spatial degree of freedom (DoF) to introduce artificial randomness. For example, Jiao *et al.* utilized perturbed beamforming weights to introduce artificial randomness [10]. They harnessed the high directionality provided by massive MIMO-based beamforming to safeguard legitimate users from potential eavesdroppers in close proximity in mmWave channels. However, it is challenging for traditional secret beam schemes [10] 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.

To address the aforementioned challenges, this paper studies the near-field XL-MIMO key generation problem. Near-field communications present an advantageous opportunity to utilize distance as a novel spatial DoF to induce artificial randomness. Our main contributions are summarized as follows:

- We first investigate the key generation in near-field XL-MIMO communications. To solve the low-entropy problem, we exploit the DoF of distances in near-field communications and design a random precoding vector to induce artificial randomness in order to increase the SKR. We derive the analytical expression of the SKR.

- We use an SVD method to find the legitimate subspace for generating secret keys and the orthogonal subspace for interrupting Eve. In order to maximize the SKR, a Dinkelbach-based power allocation method is proposed to achieve optimal allocation of the noise power for legitimate and orthogonal subspaces.
- We conduct simulations to evaluate the SKR of the proposed schemes in terms of the transmit power, the distance between Eve and BS, and the spatial angle of Eve. Our results showcase that the proposed scheme outperforms the existing state of the art.

Notations: Italic letters, boldface lower-case letters, boldface upper-case letters and calligraphic letters denote scalars, vectors, matrices and sets, respectively; $(\cdot)^H$, $(\cdot)^{-1}$ and $(\cdot)^*$ denote the 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; $\mathbb{E}\{\cdot\}$ denotes the statistical expectation, while $I(.)$ denotes mutual information. The zero vector, denoted by $\mathbf{0}$, is a vector whose components are all zero.

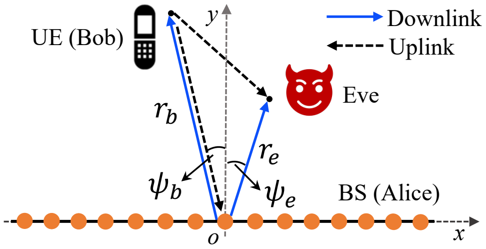

Fig. 1. Near-field channel model.

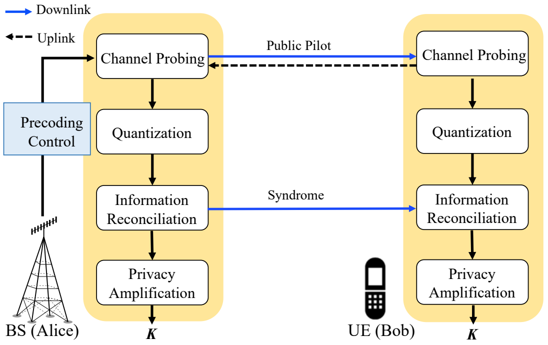

Fig. 2. Overview of key generation protocol.

II. System Model

A. Overview

Figure 1 presents the setup for the mmWave near-field XL-MIMO key generation system, comprising a base station (BS), a user equipment (UE), and an Eve. The BS is equipped with a N-antenna uniform linear array (ULA) while the UE and Eve are equipped with a single antenna. The BS designs an algorithm for controlling the precoding vector to induce artificial randomness to generate secret keys, which will be further discussed in Section IV. Eve tries to eavesdrop on transmissions so as to recover secret keys.

As shown in Fig. 2, the key generation protocol comprises four stages, namely channel probing, quantization, information reconciliation, and privacy amplification. During channel probing, the UE and BS transmit pilots to each other in turn and measure the channels between them. Additionally, these channel measurements are converted into binary sequences using a quantization algorithm. Due to the presence of noise, discrepancies may arise between the quantized sequences, which can be rectified during the subsequent information reconciliation stage. Finally, privacy amplification algorithms are employed to eliminate any potential information leakage from the preceding stages. The BS and UE agree on a unique secret key, $\boldsymbol{K}$. This paper focuses on the design of channel probing, which will be explained in Section III.

B. Device Configuration

We consider a two-dimensional coordinate system consisting of BS (Alice), UE (Bob) and Eve, as shown in Fig. 1. The BS is deployed along the x-axis. The coordinate of the central antenna of BS is situated at $(0, 0)$. The coordinates of the n-th antenna are $(\delta_n d, 0)$ with $\delta_n = \frac{2n-N+1}{2}$, $n = 0, \dots, N-1$, where d is the antenna spacing. Notably, a, b, and e are denoted as Alice, Bob, and Eve. The coordinates of u, $u \in \{b, e\}$, 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 between the user u and the centre of BS and ψ_u is the azimuth angle of arrival. The angle ψ_u is 0 degrees with the y-axis, ranging counterclockwise from 0 to 90 degrees and clockwise from 0 to -90 degrees. The BS designs a precoding vector, $\mathbf{w} \in \mathbb{C}^{N\times 1}$, for inducing artificial randomness.

C. Near-Field Channel Model

The Rayleigh distance is mathematically defined as

$$R = \frac{2D^2}{\lambda}, \tag{1}$$

where D represents the array aperture, and λ corresponds to the wavelength [4]. For a ULA, the array aperture is given by $D = Nd$. Thus, the Rayleigh distance of a ULA is $R = \frac{1}{2}N^2\lambda$ with $d = \lambda/2$. For instance, when the carrier frequency is 28 GHz and there are 100 antennas, any user located within a distance of 53.57 meters from the antenna is considered to be in its near-field region.

When the distance between the BS and the UE is less than the Rayleigh distance, the UE is positioned within the near-field region of the array. Consequently, the channel characteristics are best modeled as a near-field channel using the SW assumption.

The UE-BS line-of-sight (LoS) channel in near-field communications is modeled as

$$\mathbf{f} = \sqrt{N}\mathbf{c}(\psi_b, r_b), \tag{2}$$

where the array response vector is given by

$$\mathbf{c}(\psi_u, r_u) = \frac{1}{\sqrt{N}} \Big[\sqrt{\beta_{u0}} e^{-j\frac{2\pi}{\lambda}(r_{u0}-r_u)}, \ldots, \sqrt{\beta_{u(N-1)}} e^{-j\frac{2\pi}{\lambda}(r_{u(N-1)}-r_u)}\Big]^T, \tag{3}$$

where β_{un} is the path-loss effect from the receiver u to the n-th antenna and $r_{un} = \sqrt{r_u^2 + d^2\delta_n^2 - 2r_u\theta_u d\delta_n}$.

Similarly, we model the Eve-BS LoS channel in near-field communications as $\mathbf{h} = \sqrt{N}\mathbf{c}(\psi_e, r_e)$.

III. Channel Probing

The channel probing process consists of two steps. Firstly, using the designed precoding vector $\mathbf{w}$, the BS transmits downlink packets, while the UE probes the channel to generate secret keys. Secondly, the UE transmits uplink packets, and the BS measures the channel. The BS then multiplies the measured channel with the precoding vector $\mathbf{w}$ to enable further key generation. Since the LoS is static, the BS employs a precoding vector, $\mathbf{w}$, to create artificial randomness to mimic fast fading for generating secret keys, as described in Section IV.

A. Channel Probing for Secret LoS Channels

1) Downlink Channel Probing: The BS transmits the downlink packet, and the UE receives it, which is given by

$$y_b = \mathbf{f}^H \mathbf{w} s_d + n_b, \tag{4}$$

where s_d is the downlink pilot symbol with length 1, $s_d s_d^* = 1$, $n_b \sim \mathcal{CN}(0, \sigma_b^2)$ and σ_b^2 is the noise power variance at the UE. The UE applies the least square (LS) estimation to measure the near-field channel, $\mathbf{f} \in \mathbb{C}^{N\times 1}$, as follows:

$$z_b = \mathbf{f}^H \mathbf{w} + n_b s_d^*(s_d s_d^*)^{-1} = \mathbf{f}^H \mathbf{w} + \widehat{n}_b, \tag{5}$$

where $\widehat{n}_b \sim \mathcal{CN}(0, \widehat{\sigma}_b^2)$ is the estimation noise at the UE and $\widehat{\sigma}_b^2$ is the estimation noise variance that is equal to σ_b^2.

Eve receives the downlink packet, which is given by

$$y_{ae} = \mathbf{h}^H \mathbf{w} s_d + n_{ae}, \tag{6}$$

where $n_{ae} \sim \mathcal{CN}(0, \sigma_e^2)$ is the noise and σ_e^2 is the noise power variance at Eve. By the LS estimator, Eve measures the near-field channel, $\mathbf{h}$, which is given by

$$z_{ae} = \mathbf{h}^H \mathbf{w} + n_{ae} s_d^*(s_d s_d^*)^{-1} = \mathbf{h}^H \mathbf{w} + \widehat{n}_{ae}, \tag{7}$$

where $\widehat{n}_{ae} \sim \mathcal{CN}(0, \widehat{\sigma}_e^2)$ represents the estimation noise at Eve when it measures s from the downlink packet, whilst $\widehat{\sigma}_e^2$ is the estimation noise variance that is equal to σ_e^2.

2) Uplink Channel Probing: The UE transmits the uplink packet and the BS receives it, which is given by

$$\mathbf{y}_a = \mathbf{f} s_u + \mathbf{n}_a, \tag{8}$$

where s_u is the uplink packet with the length 1, $s_u s_u^* = P_b$ equals the transmit power at UE, and $\mathbf{n}_a \sim \mathcal{CN}(0, \sigma_a^2 \mathbf{I}_N)$ is the noise vector at the BS. The BS gets the measurements as

$$\mathbf{z}_a = \mathbf{f} + \mathbf{n}_a s_u^*(s_u s_u^*)^{-1} = \mathbf{f} + \widehat{\mathbf{n}}_a, \tag{9}$$

where $\widehat{\mathbf{n}}_a \sim \mathcal{CN}(0, \sigma_a^2/P_b \mathbf{I}_N)$ is the LS estimation noise.

Furthermore, the BS applies the random precoding vector to obtain the same equivalent channel, $\mathbf{w}^H\mathbf{f}$, as observed by the UE, which is given by

$$\bar{z}_a = \mathbf{w}^H \mathbf{z}_a = \mathbf{w}^H \mathbf{f} + \mathbf{w}^H \widehat{\mathbf{n}}_a. \tag{10}$$

The BS gets the conjugate transpose of the measurements as

$$z_a = \mathbf{f}^H \mathbf{w} + \widehat{n}_a, \tag{11}$$

where $\widehat{n}_a = \widehat{\mathbf{n}}_a^H \mathbf{w} \sim \mathcal{CN}(0, \widehat{\sigma}_a^2)$ is the estimation noise after precoding, and $\widehat{\sigma}_a^2 = \frac{P_a}{P_b}\sigma_a^2$ is the estimation noise variance.

Eve gets the measurement from the uplink packet as

$$z_{be} = h_{be} + \widehat{n}_{be}, \tag{12}$$

where $\widehat{n}_{be} \sim \mathcal{CN}(0, \widehat{\sigma}_{be}^2)$ is the estimation noise, h_{be} is the channel from the UE to Eve, and $\widehat{\sigma}_{be}^2$ is the estimation noise variance at Eve when it measures s_{be} from the uplink packet.

B. 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 [11], under the passive eavesdropping attack, the SKR is given by $I(z_a; z_b | z_{ae}, z_{be})$.

We assume that Eve is able to 1) receive the uplink pilot and downlink pilot from the UE and BS, respectively; 2) be in close proximity to the UE for experiencing correlated channels as the UE. Therefore, the SKR is simplified as

$$I(z_a; z_b | z_{ae}) = \log_2 \left(\frac{|\mathbf{K}_{z_a z_{ae}}||\mathbf{K}_{z_b z_{ae}}|}{\sigma_{EE}^2 |\mathbf{K}_{z_a, z_b, z_{ae}}|} \right). \tag{13}$$

The channel variances of the measurements are derived as

$$\begin{aligned}
\sigma_{AA}^2 &= \mathbb{E}\left\{(\mathbf{f}^H\mathbf{w} + \widehat{n}_a)(\mathbf{f}^H\mathbf{w} + \widehat{n}_a)^H\right\} = \mathbf{f}^H\mathbf{W}\mathbf{f} + \widehat{\sigma}_a^2,\\
\sigma_{BB}^2 &= \mathbb{E}\left\{(\mathbf{f}^H\mathbf{w} + \widehat{n}_b)(\mathbf{f}^H\mathbf{w} + \widehat{n}_b)^H\right\} = \mathbf{f}^H\mathbf{W}\mathbf{f} + \widehat{\sigma}_b^2,\\
\sigma_{EE}^2 &= \mathbb{E}\left\{(\mathbf{h}^H\mathbf{w} + \widehat{n}_e)(\mathbf{h}^H\mathbf{w} + \widehat{n}_e)^H\right\} = \mathbf{h}^H\mathbf{W}\mathbf{h} + \widehat{\sigma}_e^2,\\
\sigma_{AE}^2 &= \sigma_{BE}^2 = \mathbf{f}^H\mathbf{W}\mathbf{h}.
\end{aligned} \tag{14}$$

We define $\sigma_B^2 = \mathbf{f}^H\mathbf{W}\mathbf{f}$ and $\sigma_E^2 = \mathbf{h}^H\mathbf{W}\mathbf{h}$. Note that $\mathbf{W} = \mathbb{E}\{\mathbf{w}\mathbf{w}^H\}$ is the pilot covariance matrix.

The covariance matrix of Eve's and BS's measurements is

$$\mathbf{K}_{z_a, z_{ae}} = \mathbb{E}\left\{ \begin{bmatrix} z_a \\ z_{ae} \end{bmatrix} \begin{bmatrix} z_a^* & z_{ae}^* \end{bmatrix} \right\} = \begin{bmatrix} \sigma_{AA}^2 & \sigma_{AE}^2 \\ (\sigma_{AE}^2)^* & \sigma_{EE}^2 \end{bmatrix}. \tag{15}$$

The covariance matrix of Eve's and UE's measurements is

$$\mathbf{K}_{z_b, z_{ae}} = \mathbb{E}\left\{ \begin{bmatrix} z_b \\ z_{ae} \end{bmatrix} \begin{bmatrix} z_b^* & z_{ae}^* \end{bmatrix} \right\} = \begin{bmatrix} \sigma_{BB}^2 & \sigma_{BE}^2 \\ (\sigma_{BE}^2)^* & \sigma_{EE}^2 \end{bmatrix}. \tag{16}$$

The covariance matrix of the full measurements is given by

$$\mathbf{K}_{z_a, z_b, z_{ac}} = \begin{bmatrix} \sigma_{AA}^2 & \sigma_B^2 & \sigma_{AE}^2 \\ \sigma_B^2 & \sigma_{BB}^2 & \sigma_{BE}^2 \\ (\sigma_{AE}^2)^* & (\sigma_{BE}^2)^* & \sigma_{EE}^2 \end{bmatrix}. \tag{17}$$

We calculate the determinants of the above three matrices in (13) as follows:

$$|\mathbf{K}_{z_a z_{ae}}| = (\sigma_B^2 + \widehat{\sigma}_a^2)(\sigma_E^2 + \widehat{\sigma}_e^2) - |\sigma_{AE}^2|^2, \tag{18}$$

$$|\mathbf{K}_{z_b z_{ae}}| = (\sigma_B^2 + \widehat{\sigma}_b^2)(\sigma_E^2 + \widehat{\sigma}_e^2) - |\sigma_{AE}^2|^2, \tag{19}$$

$$\begin{aligned}
|\mathbf{K}_{z_a z_b z_{ae}}| &= (\sigma_B^2 + \widehat{\sigma}_a^2)(\sigma_B^2 + \widehat{\sigma}_b^2)(\sigma_E^2 + \widehat{\sigma}_e^2) - |\sigma_{AE}^2|^2 \\
&\quad \times (\widehat{\sigma}_a^2 + \widehat{\sigma}_b^2) - \sigma_B^4(\sigma_E^2 + \widehat{\sigma}_e^2).
\end{aligned} \tag{20}$$

Substituting (18) and (19) into the numerator of (13), we have

$$|\mathbf{K}_{z_a z_{ae}}||\mathbf{K}_{z_b z_{ae}}| = (\sigma_B^2 + \widehat{\sigma}_a^2)(\sigma_B^2 + \widehat{\sigma}_b^2)(\sigma_E^2 + \widehat{\sigma}_e^2)^2 \\ - |\sigma_{AE}^2|^2(\sigma_E^2 + \widehat{\sigma}_e^2)(2\sigma_B^2 + \widehat{\sigma}_a^2 + \widehat{\sigma}_b^2) + |\sigma_{AE}^2|^4. \quad (21)$$

Substituting (20) into the denominator of (13), we have

$$\sigma_{EE}^2 |\mathbf{K}_{z_a, z_b, z_{ae,k}}| = (\sigma_B^2 + \widehat{\sigma}_a^2)(\sigma_B^2 + \widehat{\sigma}_b^2)(\sigma_E^2 + \widehat{\sigma}_e^2)^2 \\ - (\sigma_E^2 + \widehat{\sigma}_e^2)(\sigma_B^4(\sigma_E^2 + \widehat{\sigma}_e^2) + |\sigma_{AE}^2|^2(\widehat{\sigma}_a^2 + \widehat{\sigma}_b^2)). \quad (22)$$

Substituting (21) and (22) into (13), the objective function is simplified as (23), shown at the top of the next page.

C. The Monotonicity of the SKR

Next, we investigate the monotonicity of (23). We define $\alpha = \sigma_B^2 - \frac{\sigma_{AE}^4}{(\sigma_E^2 + \widehat{\sigma}_e^2)}$. We also define the function $f(\alpha)$ in terms of α, which is given by

$$f(\alpha) = 1 + \frac{\alpha^2}{(\widehat{\sigma}_a^2 + \widehat{\sigma}_b^2)\alpha + \widehat{\sigma}_a^2 \widehat{\sigma}_b^2}. \quad (24)$$

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

$$\frac{\partial f}{\partial \alpha} = \frac{(\widehat{\sigma}_a^2 + \widehat{\sigma}_b^2)\alpha^2 + 2\widehat{\sigma}_a^2 \widehat{\sigma}_b^2 \alpha}{((\widehat{\sigma}_a^2 + \widehat{\sigma}_b^2)\alpha + \widehat{\sigma}_a^2 \widehat{\sigma}_b^2)^2}. \quad (25)$$

From the first-order derivative, we find that $\frac{\partial f}{\partial \alpha} > 0$ for $\alpha > 0$. Therefore, the objective function in (23) increases monotonically with α. Next, we only have to maximize α.

IV. SVD-Based Precoding Vector Design for SKR Optimization

The random precoding vector, $\mathbf{w}$, can be represented as a sum of random coefficients, p_k, multiplied by the $N \times 1$ beamforming weight vectors, $\mathbf{w}_k$, i.e., $\mathbf{w} = \sum_k p_k \mathbf{w}_k$. The random coefficients, p_k, are complex Gaussian-distributed and contribute to the artificial randomness simulating fast fading in the LoS channel for key generation. However, to mitigate Eve's eavesdropping, the BS needs to carefully control the random coefficients p_k by introducing additional random noise. Note that $\mathbf{w}_k$ serves the purpose of steering the direction of the random signals, either for key generation or for disrupting Eve's eavesdropping attempts.

Since the SKR monotonically increases with α and α is a function of $\mathbf{W}$, we design $\mathbf{W}$ to optimize α and then decompose it to $\mathbf{w}$. To design $\mathbf{W}$ to maximize the SKR, the BS leverages the knowledge of the LoS channel. For accurately estimating the LoS channel in near-field communications, a channel estimation method can be found in [4].

With the constraint on the transmit power, we formulate the optimization problem as follows:

$$\text{(P1):} \ \max \ \sigma_B^2 - \frac{|\sigma_{AE}^2|^2}{(\sigma_E^2 + \widehat{\sigma}_e^2)} \\ \text{s.t. } \operatorname{Tr}(\mathbf{W}) \le P_a, \quad (26)$$

where P_a is the transmit power at the BS. Since the objective function of (P1) is non-concave, we introduce an SVD-based method to simplify (P1). To determine the legitimate subspace for inducing artificial randomness to generate secret keys and the orthogonal subspace to interrupt Eve, we compute the SVD of the vector $\mathbf{f}$ as follows: $\mathbf{f} = \mathbf{U\Lambda V} = [\mathbf{u}_s \ \mathbf{U}_n] \begin{bmatrix} \lambda_s \\ \mathbf{0} \end{bmatrix}$, where $\mathbf{V} = 1$ since $\mathbf{f}$ is a vector. Notably, $\mathbf{u}_s$ represents the legitimate subspace for generating secret keys, whilst $\mathbf{U}_n$, the matrix constituting vectors that are orthogonal to $\mathbf{u}_s$, indicates the orthogonal subspace for preventing Eve from eavesdropping on secret keys. We set $\bar{\mathbf{B}} = \mathbf{u}_s \mathbf{u}_s^H$ and $\mathbf{C} = \mathbf{U}_n \mathbf{\Sigma}_n \mathbf{U}_n^H$, where $\mathbf{\Sigma}_n$ is a diagonal matrix with identical elements $1/(N-1)$. We define $\mathbf{W} = \mathbf{W}_S + \mathbf{W}_N$, where $\mathbf{W}_S = P_S \bar{\mathbf{B}}$, $\mathbf{W}_N = P_N \mathbf{C}$, P_S is the transmit power for key generation and P_N is the noise power for interrupting Eve. We also define $\mathbf{A} = \mathbf{h}\mathbf{h}^H$ and $\mathbf{B} = \mathbf{f}\mathbf{f}^H$. Thus, we have $\sigma_B^2 = \mathbf{f}^H \mathbf{W} \mathbf{f} = \operatorname{Tr}(\mathbf{WB})$, $\sigma_E^2 = \mathbf{h}^H \mathbf{W} \mathbf{h} = \operatorname{Tr}(\mathbf{WA})$, and $|\sigma_{AE}^2|^2 = \operatorname{Tr}(\mathbf{WAWB})$.

The optimization problem (P1) is transformed to (P2) in matrix form as follows:

$$\text{(P2):} \ \min \ \frac{\operatorname{Tr}(\mathbf{WAWB})}{\operatorname{Tr}(\mathbf{WA}) + \widehat{\sigma}_e^2} - \operatorname{Tr}(\mathbf{WB}) \\ \text{s.t. } \operatorname{Tr}(\mathbf{W}) \le P_a, \\ \mathbf{W} = \mathbf{W}_S + \mathbf{W}_N. \quad (27)$$

Given $\mathbf{W} = \mathbf{W}_S + \mathbf{W}_N$, we calculate $\operatorname{Tr}(\mathbf{WB}) = \operatorname{Tr}(\mathbf{W}_S\mathbf{B}) = P_S \operatorname{Tr}(\mathbf{B})$. Through mathematical steps, we can simplify the objective function of (P2) as follows:

$$-\alpha = \frac{P_S^2 \operatorname{Tr}(\bar{\mathbf{B}}\mathbf{AB}) + P_S(P_t - P_S)\operatorname{Tr}(\mathbf{CAB})}{P_S \operatorname{Tr}(\bar{\mathbf{B}}\mathbf{A}) + (P_t - P_S)\operatorname{Tr}(\mathbf{CA}) + \widehat{\sigma}_e^2} - P_S \operatorname{Tr}(\mathbf{B}) \\ = \frac{m_1 P_S^2 + m_2 P_S}{m_3 P_S + m_4}, \quad (28)$$

where the coefficients in the above objective function are presented as follows:

$$m_1 = \operatorname{Tr}(\bar{\mathbf{B}}\mathbf{AB}) - \operatorname{Tr}(\mathbf{B})\operatorname{Tr}(\bar{\mathbf{B}}\mathbf{A}) + \operatorname{Tr}(\mathbf{CA})\operatorname{Tr}(\mathbf{B}) - \operatorname{Tr}(\mathbf{CAB}), \\ m_2 = P_t \operatorname{Tr}(\mathbf{CAB}) - P_t \operatorname{Tr}(\mathbf{B})\operatorname{Tr}(\mathbf{CA}) - \widehat{\sigma}_e^2 \operatorname{Tr}(\mathbf{B}), \\ m_3 = \operatorname{Tr}(\bar{\mathbf{B}}\mathbf{A}) - \operatorname{Tr}(\mathbf{CA}), \ m_4 = P_t \operatorname{Tr}(\mathbf{CA}) + \widehat{\sigma}_e^2. \quad (29)$$

The optimization problem (P2) is reformulated as

$$\text{(P3):} \ \min_{P_S} \ \frac{m_1 P_S^2 + m_2 P_S}{m_3 P_S + m_4} \\ \text{s.t. } 0 \le P_S \le P_a. \quad (30)$$

In order to make the problem (P3) tractable, we can use the Dinkelbach method to solve the following problem.

$$\text{(P4):} \ \min_{P_S} \ y(P_S) \\ \text{s.t. } 0 \le P_S \le P_a, \quad (31)$$

where $y(P_S) = m_1 P_S^2 + (m_2 - \beta m_3)P_S - \beta m_4$ and β is the slope parameter. The algorithm for solving the problem (P4) is presented in Algorithm 1. In line 1, we set the initial power for generating secret keys as $P_{S,0} = P_a$. From line 3 to line 7, for the t-th loop, we calculate the slope parameter β_t. Given β_t, we then find the optimal transmit power $P_{S,t}$. Upon reaching

$$I(z_a; z_b|z_{ae}) = \log_2 \left(\frac{(\sigma_B^2 + \widehat{\sigma}_a^2)(\sigma_B^2 + \widehat{\sigma}_b^2)(\sigma_E^2 + \widehat{\sigma}_e^2)^2 - \sigma_{AE}^4(\sigma_E^2 + \widehat{\sigma}_e^2)(2\sigma_B^2 + \widehat{\sigma}_a^2 + \widehat{\sigma}_b^2) + \sigma_{AE}^8}{(\sigma_B^2 + \widehat{\sigma}_a^2)(\sigma_B^2 + \widehat{\sigma}_b^2)(\sigma_E^2 + \widehat{\sigma}_e^2)^2 - (\sigma_E^2 + \widehat{\sigma}_e^2)(\sigma_B^4(\sigma_E^2 + \widehat{\sigma}_e^2) + \sigma_{AE}^4(\widehat{\sigma}_a^2 + \widehat{\sigma}_b^2))} \right)$$

$$= \log_2 \left(1 + \frac{(\sigma_B^2 - \frac{\sigma_{AE}^4}{\sigma_E^2 + \widehat{\sigma}_e^2})^2}{(\widehat{\sigma}_a^2 + \widehat{\sigma}_b^2)(\sigma_B^2 - \frac{\sigma_{AE}^4}{(\sigma_E^2 + \widehat{\sigma}_e^2)}) + \widehat{\sigma}_a^2 \widehat{\sigma}_b^2} \right). \quad (23)$$

```
Algorithm 1 Dinkelbach Algorithm
Input: $m_1$, $m_2$, $m_3$, $m_4$, $P_{max}$, $\epsilon$;
Output: $P_S$, $\beta$, $t$.
1: Set $P_{S,0} = P_a$, Set $t = 1$;
2: while $|m_1 P_{S,t}^2 + m_2 P_{S,t} - \beta_t(m_3 P_{S,t} + m_4)| > \epsilon$ do
3:     In the $t$-th loop, the slope parameter, $\beta_t$, is calculated as follows $\beta_t = \frac{m_1 P_{S,t-1}^2 + m_2 P_{S,t-1}}{m_3 P_{S,t-1} + m_4}$;
4:     In the $t$-th loop, the optimal value of (P4) can be determined based on the expression: $P_{S,t} = \arg\min\{y(0), y(P_a), y(\frac{\beta_t m_3 - m_2}{2m_1})\}$, Set $t = t + 1$;
5: end while
```

the stopping criterion $|m_1 P_{S,t}^2 + m_2 P_{S,t} - \beta_t(m_3 P_{S,t} + m_4)| \leq \epsilon$, we designate β_t as the optimal value.

Given $\mathbf{W}$, the precoding vector, $\mathbf{w}_S$, is expressed as $\mathbf{w}_S = p_0 \mathbf{u}_s$, where p_0 follows a complex Gaussian distribution with variance P_S. The precoding vector, $\mathbf{w}_N$, is defined as $\mathbf{w}_N = \sum_{k=1}^{N-1} p_k \mathbf{u}_k$, with $\mathbf{u}_k$ representing the k-th column of $\mathbf{U}_n$, while coefficients p_k follow a complex Gaussian distribution with variance $P_N/(N-1)$. Here, $\mathbf{u}_s$ denotes the beamforming weight vector to shape the transmitted signal's direction for secret key generation, while $\mathbf{u}_k$ signifies the beamforming weight vector tailored to direct the signal to prevent eavesdropping on secret keys by Eve. The coefficient p_0 controls the amplitude of the signals to induce artificial randomness for generating secret keys. The coefficients p_k, where $k = 1, \ldots, N-1$, contribute to injecting random noise to prevent Eve from eavesdropping on secret keys. The overall precoding vector is obtained by $\mathbf{w} = \mathbf{w}_S + \mathbf{w}_N$.

V. Simulation Results

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

A. Setup

The BS equipped with $N = 256$ antennas is positioned along the y-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. The transmit powers of both the BS and the UE are configured to be equal, denoted as $P_t = P_a = P_b$ dBm. The noise powers are set as $\sigma_a^2 = \sigma_b^2 = \sigma_e^2 = -105$ dBm. The path-loss effect from $u \in \{a, e\}$ to the n-th antenna is $\beta_{un} = \beta_0(\frac{r_{un}}{d_0})^{-2}$, where $\beta_0 = (\frac{\lambda}{4\pi})^2$ denotes the path-loss effect at $d_0 = 1$ m.

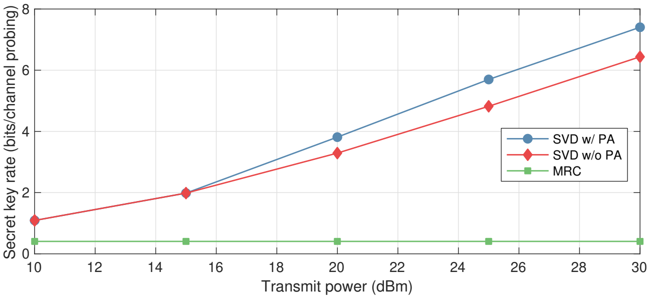

Fig. 3. SKR versus the transmit power. Here, $N = 256$, $r_b = 12.2$ m, $r_e = 12$ m, $\psi_b = 0.2$ radian and $\psi_e = 0.2$ radian.

B. Considered Algorithms

The considered algorithms are described as follows:

1) **Maximal-Ratio Combining (MRC):** The BS applies the MRC beamforming to let the precoding vector align with the channel [12] , i.e., $\mathbf{w} = \sqrt{P_a}\mathbf{f}/\|\mathbf{f}\|_F$. This process enhances the signal-to-noise ratio (SNR) of the desired signal while mitigating the effects of noise.
2) **SVD without Power Allocation (SVD w/o PA):** The design of the precoding vector is based on Section IV. The transmit power is equally allocated to P_S and P_N.
3) **SVD with Power Allocation (SVD w/ PA):** The design of the precoding vector is based on Section IV. The transmit power allocated to generate secret keys, P_S, and interrupt the Eve, P_N, is according to the algorithm for solving the optimization problem (31).

C. Results

We evaluate the SKR against the transmit power P_a, the distance between Eve and BS, and the spatial angle of Eve.

Figure 3 presents the SKR versus the transmit power. The relationship between the SKR and the transmit power is evident, as increasing the transmit power leads to a higher SNR, which is beneficial for SKR. As depicted in Fig. 3, the MRC scheme exhibits the poorest performance due to its failure to introduce artificial noise to disrupt Eve's reception. The SVD w/ PA scheme outperforms the SVD w/o PA, thereby validating the efficacy of the power allocation algorithm for P_S and P_N.

Figure 4 illustrates the SKR when the distance between Eve and BS, r_e, varies. The UE is located 14 m away from the BS. When Eve and UE share the same spatial angle, i.e. $\psi_b = \psi_e = 0.2$ radian, the top two curves initially decrease, attaining their minimum values at 14 m and then increase

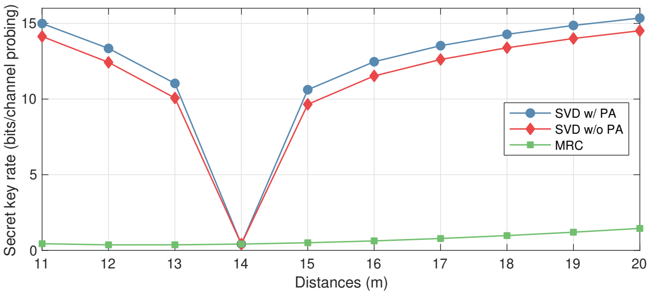

Fig. 4. SKR versus the distance between Eve and BS. Here, $P_t = 30$ dBm, $N = 256$, $r_b = 14$ m, $\psi_b = 0.2$ radian and $\psi_e = 0.2$ radian.

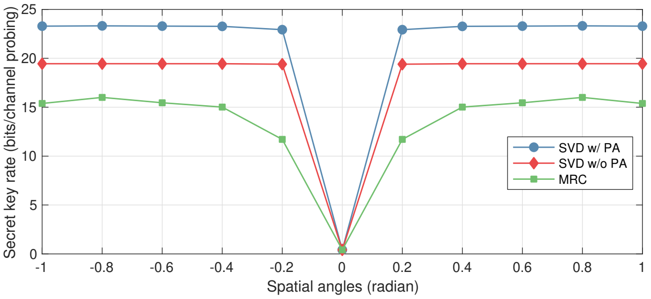

Fig. 5. SKR versus the spatial angle of Eve. Here, $P_t = 30$ dBm, $N = 256$, $r_b = 15$ m, $r_e = 15$ m and $\psi_b = 0$ radian.

as r_e varies. This behavior indicates that Eve's location is gradually shifting from being closer to the UE to being farther away from the UE. The correlation between the near-field channels of UE and Eve gets stronger when Eve is gradually near the UE. The MRC scheme can still generate secret keys if $r_e > r_b$. If $r_e \leq r_b$, the SKR of MRC approaches 0 because Eve has better channel quality than UE and there is no artificial noise to interrupt it. This phenomenon is inherently typical in traditional far-field key generation [10], where the artificial noise is injected into the legitimate channels and the scheme in [10] used the spatial angles to distinguish UE from Eve. To address the problem, more transmit antennas should be employed to find the difference between the spatial angles of Eve and UE. However, in near-field communications, the distance difference can be used to help the UE gain an advantage over Eve to generate secret keys. Other than Eve having the same distance and spatial angle as the UE, the schemes in the near-field can generate secret keys. Besides, the proposed SVD w/ PA scheme shows better performance than the baseline schemes SVD w/o PA and MRC schemes.

Figure 5 presents the SKR plotted against Eve's spatial angles. When Eve shares the same spatial angle with the UE, the SKR approaches 0. The SKR exhibits symmetry, which is due to the spatial angle of the BS being set at 0 radian. Besides, the SKR aligns with the peak of each sidelobe, resulting in periodic fluctuations with increasing and decreasing values [11]. The MRC scheme yields satisfactory performance when there is a notable difference in spatial angles between the UE and Eve. This is because the channels of the UE and Eve become less correlated, enhancing security. The SVD w/ PA scheme shows an advantage over the MRC and SVD w/o PA schemes, indicating the superiority in enhancing the SKR.

VI. Conclusion

This paper has investigated the PLKG in near-field XL-MIMO communications. We have used a precoding vector to induce artificial randomness in LoS channels to generate secret keys at the BS and UE as well as prevent Eve from eavesdropping. We have derived the SKR and proposed an SVD-based method to allocate the transmit power for generating secret keys and the noise power for interrupting Eve. Our theoretical analysis has been validated in terms of the transmit power, the distance between Eve and BS and the spatial angle of Eve.

Acknowledgment

This research is supported by the National Natural Science Foundation of China (No. U22B2026) and the National Key R&D Program of China (No. 2020YFE0200600). The work of J. Zhang and C. Chen was also supported by the UK EPSRC under grant ID EP/V027697/1. This work of T. Q. Duong was supported in part by the U.K. Royal Academy of Engineering (RAEng) under the RAEng Research Chair and Senior Research Fellowship scheme Grant RCSRF2021\11\41. The work of M. Matthaiou was supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 101001331). For the purpose of open access, the authors have applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising.

References

[1] M. Matthaiou *et al.*, "The road to 6G: Ten physical layer challenges for communications engineers," *IEEE Commun. Mag.*, vol. 59, no. 1, pp. 64–69, Jan. 2021.

[2] J. Zhang *et al.*, "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.

[3] P. Ramezani and E. Björnson, "Near-field beamforming and multiplexing using extremely large aperture arrays," Sep. 2022, arXiv:2209.03082v1.

[4] 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.

[5] 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.

[6] Y. Ding, J. Zhang, and V. F. Fusco, "Retrodirective-assisted secure wireless key establishment," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 320–334, Jan. 2017.

[7] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2692–2705, Feb. 2020.

[8] T. Lu *et al.*, "Reconfigurable intelligent surface assisted secret key generation in quasi-static environments," *IEEE Commun. Lett.*, vol. 26, no. 2, pp. 244–248, Feb. 2022.

[9] G. Ning *et al.*, "When physical layer key generation meets RIS: Opportunities, challenges, and road ahead," Jul. 2023, arXiv:2210.02337v2.

[10] 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.

[11] 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.

[12] H. Lu and Y. Zeng, "Near-field modeling and performance analysis for multi-user extremely large-scale MIMO communication," *IEEE Commun. Lett.*, vol. 26, no. 2, pp. 277–281, Feb. 2022.