Reconfigurable Intelligent Surface-Assisted Secret Key Generation in Spatially Correlated Channels

Lei Hu, Student Member, IEEE, Guyue Li, Member, IEEE, Xuewen Qian, Aiqun Hu, Senior Member, IEEE, and Derrick Wing Kwan Ng, Fellow, IEEE

Abstract-Reconfigurable intelligent surface (RIS) is a disruptive technology to enhance the performance of physicallayer key generation (PKG) thanks to its ability to smartly customize the radio environments. Existing RIS-assisted PKG methods are mainly based on the idealistic assumption of an independent and identically distributed (i.i.d.) channel model at both the base station (BS) and the RIS. However, the i.i.d. model is inaccurate for a typical RIS in an isotropic scattering environment and neglecting the existence of channel spatial correlation would possibly degrade the PKG performance. In this paper, we establish a general spatially correlated channel model and propose a new channel probing framework based on the transmit and the reflective beamforming. We derive a closed-form key generation rate (KGR) expression and formulate an optimization problem, which is solved by using the lowcomplexity Block Successive Upper-bound Minimization (BSUM) with Mirror-Prox method. Simulation results show that compared to the existing methods based on the i.i.d. fading model, our proposed method achieves about 5 dB transmit power gain when the spacing between two neighboring RIS elements is a quarter of the wavelength. Also, the KGR increases significantly with the number of RIS elements while that increases marginally with the number of BS antennas.

Index Terms—Physical layer security, secret key generation, reconfigurable intelligent surface, spatially correlated channels.

I. INTRODUCTION

In the last decades, the throughput of wireless communication systems has achieved a 1000-fold capacity increase [2]. At the same time, an enormous amount of confidential information, including financial information and trade secrets, has been exchanged via wireless channels. However, the broadcast property of wireless medium makes wireless transmissions vulnerable to security breaches, such as passive and active attacks by potential eavesdroppers. Traditionally, security communication is guaranteed by the public key cryptography

Part of this paper has been accepted by the IEEE Globecom 2022 [1]. (Corresponding author: Guyue Li.)

Lei Hu and Guyue Li are with the School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China. Guyue Li is also with Purple Mountain Laboratories, Nanjing 211111, China, and also with the Jiangsu Provincial Key Laboratory of Computer Network Technology, Nanjing 210096, China (e-mail: lei-hu@seu.edu.cn; guyuelee@seu.edu.cn.).

Xuewen Qian is with with Université Paris-Saclay, CNRS, CentraleSupélec, Laboratoire des Signaux et Systèmes, 91192 Gif-sur-Yvette, France (e-mail: xuewen.gian@centralesupelec.fr).

Aiqun Hu is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing, 210096, China, also with Purple Mountain Laboratories, Nanjing 211111, China, and also with the Jiangsu Provincial Key Laboratory of Computer Network Technology, Nanjing 210096, China (e-mail: aqhu@seu.edu.cn).

Derrick Wing Kwan Ng is with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia (e-mail: w.k.ng@unsw.edu.au). techniques adopted in the application layer. However, the public key in those traditional methods needs to be distributed to the involved legitimate ends in advance, which is difficult to realize in mobile and ad-hoc wireless networks. Alternatively, physical-layer key generation (PKG) is recognized as a promising paradigm to tackle this problem [3]. By leveraging the inherent random and reciprocal nature of wireless channels, PKG naturally establishes symmetric keys between the legitimate parties [4]. Also, due to its potential to achieve information-theoretic security cost-effectively, PKG has been applied to practical systems, such as WiFi, LoRa, and Zigbee, *et al* [5], [6].

The general PKG procedures can be divided into four consecutive stages: channel sounding, quantization, information reconciliation, and privacy amplification [7]. Specifically, for the channel probing stage, Alice and Bob alternatingly exchange pilots and perform channel estimations in a coherence time slot to extract correlated channel features. These features are converted into binary bits in the quantization stage. Then, in the information reconciliation stage, the mismatched bits between Alice and Bob are corrected via error-correcting codes. At last, during the privacy amplification stage, Alice and Bob discard the bits that could be potentially leaked in the previous stages. It can be observed that the feasibility of the PKG is strongly associated with the properties of wireless channels. Moreover, the existence of rich-scattering and dynamically varying channels is the essential premise to ensure the security level offered by the generated secret key [5], [8].

Unfortunately, the above condition can hardly be satisfied in some harsh propagation scenarios, such as shadowed environments [9]. As such, various previous works aim to enhance the PKG performance in these propagation scenarios to a certain extent by utilizing cooperative relaying [10]. However, the relay-based PKG approaches admit two main demerits. First, the key rate has limited growth unless the relay node keeps moving all the time to introduce randomness to the secret key [11]. Second, deploying active relays incurs high hardware costs and energy consumption [12]. As a result, a new costeffective and energy-effective paradigm that is capable of controlling the propagation environment is needed to facilitate PKG.

As a remedy, reconfigurable intelligent surface (RIS) was proposed to address this emerging need. In particular, RIS is a programmable and reconfigurable metasurface consisting of a large number of low-cost passive elements, e.g., printed dipoles and phase shifters [13], [14]. These elements are controlled collaboratively to alter the signal propagation environment. Hence, RIS provides a cost-effective approach to enable the customization of favorable wireless propagation environments for PKG while avoiding the deployment of powerhungry and expensive cooperative relays. However, to fully unleash the potential of RIS for effective KGR provisioning, the reflection coefficients of RIS elements have to be appropriately optimized. Inspired by this, several works have been proposed on the optimization design of RIS-assisted PKG systems, such as [15]–[17], starting from single-user systems to multi-user systems. In particular, the authors of [15] considered a simple scenario with a single-user and independent eavesdropping channels. They derived the expression of the KGR capacity and optimized the switch states of RIS units globally when the number of available RIS units is limited. Furthermore, RISassisted PKG systems comprising multiple eavesdroppers with correlated eavesdropping channels were investigated in [16], where the authors designed a semidefinite relaxation (SDR) and successive convex approximation (SCA)-based algorithm to maximize the lower bound of the secret key capacity. Despite the fruitful research in the literature, most of the above works considered only the single-user case, e.g., [15], [16], and their results are not applicable to practical cases having multiple users. On the other hand, in [17], the authors introduced a RIS-assisted multiuser key generation scheme and optimized the RIS phase shifts in the presence of independent and correlated eavesdropping channels. Nevertheless, all of these works are based on the independent and identically distributed (i.i.d.) Rayleigh fading model for the RIS-related channels. In practice, the non-negligible spatial correlations naturally exist among RIS elements due to their sub-wavelength sizes and distributions. More importantly, these correlations may jeopardize the PKG performance if they are not taken into account in the system design [18]. In addition, only a singleantenna BS was considered in these works, e.g., [15]-[17], and it is not straightforward to extend these existing results to the case of multi-antenna, which has a more complicated model, and the reflective beamforming at RIS and transmit beamforming at the BS need to be jointly optimized. Indeed, the design of RIS-assisted PKG methods in multi-antenna spatially correlated channels is of utmost importance but it has not been studied in the existing works, yet.

To address the above issues, this paper investigates the RIS-assisted PKG in a multiple-input single-output multipleeavesdropper (MISOME) system, with the consideration of the spatial correlation at both the BS and the RIS. The main contributions of this paper are as follows.

• We propose a transmit and reflective beamforming-based RIS-assisted PKG framework in multi-antenna spatially correlated channels. We derive the closed-form KGR expression as a function of the reflective beamforming at the RIS and the transmit beamforming at the BS. We formulate the design of beamforming as an optimization problem to maximize the minimum KGR for the worstcase eavesdropper channel. Furthermore, our analysis shows that the beamforming designed for the correlated model outperforms that for the i.i.d. model while the KGR gain increases with the channel correlation with the proposed design.

- To tackle the resulting non-convex optimization problem, we present an effective Block Successive Upper-bound Minimization (BSUM)-based algorithm. We prove that the BSUM algorithm yields a non-decreasing convergence over iterations. Then, to solve the non-smooth convex problem in each iteration of the BSUM algorithm in a complexity-effective manner, we reformulate it as an equivalent convex-concave saddle point problem and employ the Mirror-Prox method to solve it with closedform updates.
- Simulation results show that compared to existing methods based on the i.i.d. fading model, the proposed design achieves about 5 dB transmit power gain when the spacing between two neighbouring RIS elements is a quarter of the wavelength and the BS antenna correlation ρ is 0.2. Also, the KGR gain increases with the spatial correlation at both the BS and the RIS. Moreover, the computational time of the proposed algorithm is reduced approximately by two orders of magnitude compared to that of the commonly adopted algorithms, e.g., alternating optimization, semidefinite relaxation, successive convex approximation with Gaussian randomization (ASSG), while achieving a similar KGR performance.

Note that in the conference version of this paper [1], we considered the case where the eavesdropping channels are independent of the legitimate channels and derived the optimal beamforming to maximize the KGR. In this paper, we generalize it by taking into account the channel correlation between Eve and the legitimate parties. We provide a general KGR expression and formulate an optimization problem, which can be solved by the proposed low-complexity BSUM algorithm.

Notations: In this paper, matrices and vectors are denoted by boldface upper-case and boldface lower-case. $\mathbb{C}^{A\times B}$ denotes the space of complex matrices of size $A \times B$. $\Re(\cdot)$ and $\Im(\cdot)$ stand for the real and imaginary parts of a complex number. The imaginary unit of a complex number is denoted by $j = \sqrt{-1}$. $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$ denote the conjugate, transpose, and conjugate transpose, respectively. diag(x) is a matrix whose main diagonal elements are the entries of \boldsymbol{x} . vec (\boldsymbol{X}) denotes the vectorization of the matrix \boldsymbol{X} . The Kronecker product, Hadamard product, and Khatri-Rao product are represented by \otimes , \circ , and \odot , respectively. $\mathcal{I}(X;Y)$ and $\mathcal{H}(X,Y)$ are the mutual information and joint entropy of random variables X and Y, respectively. $det(\cdot)$ is the matrix determinant. $||\boldsymbol{x}||_1$, $||\boldsymbol{x}||_2$, and $||\boldsymbol{x}||_{\infty}$ denote the ℓ_1 , ℓ_2 , and ℓ_{∞} norms of vector \boldsymbol{x} . $\|\boldsymbol{X}\|_{F}$ is the Frobenius norm of matrix X. $\mathbb{E}\{\cdot\}$ represents statistical expectation. $\lambda_{\max}(X)$ is the maximum eigenvalue of matrix \mathbf{X} . $\mathcal{O}(\cdot)$ is the big-O notation. $X \succeq \mathbf{0}$ means X is a positive semidefinite matrix. $\nabla f(\cdot)$ and $\partial f/\partial x$ are the gradient operators of function f. I denotes the identity matrix. $b \sim C\mathcal{N}(0, \Sigma)$ denotes that b is a circularly symmetric complex Gaussian (CSCG) vector with zero mean and covariance matrix Σ .



Fig. 1. The model of RIS-assisted secret key generation in MISOME systems.

II. SYSTEM MODEL

As shown in Fig. 1, we study a RIS-assisted PKG method in a MISOME system. Assuming the time-division duplexing (TDD) protocol is adopted, a multi-antenna base station (BS), Alice, and a single-antenna user, Bob, aim to generate symmetric keys by exploiting the reciprocity of the wireless channel with the help of a RIS¹. Meanwhile, a multi-antenna eavesdropper, Eve, intends to obtain the secret key information from his/her received signals.

We assume that Alice and Eve are equipped with M and K antennas, respectively. The RIS consists of N passive reflection elements. Equipped with a smart controller that communicates with the BS, the RIS adapts the phase shift of each reflecting element to enable the secret key generation [20]. Since the spatial correlation affects the secret key rate, we consider the general spatial correlation channel model at both the RIS and the BS.

A. Channel Model

The direct channels of Alice-to-Bob, Eve-to-Bob, and Aliceto-Eve are denoted by $h_{ab} \in \mathbb{C}^{M \times 1}$, $h_{eb} \in \mathbb{C}^{K \times 1}$, and $H_{ae} \in \mathbb{C}^{M \times K}$, respectively. $h_{ak} \in \mathbb{C}^{M \times 1}$ denotes the channel from Alice to Eve's *k*-th antenna, $k \in \{1, \dots, K\}$. When a RIS is involved in the PKG system, it introduces additional communication channels. Specifically, the channels of RIS-to-Alice, RIS-to-Bob, and RIS-to-Eve are represented as $G_{ra} \in \mathbb{C}^{N \times M}$, $h_{rb} \in \mathbb{C}^{N \times 1}$, and $G_{re} \in \mathbb{C}^{N \times K}$, respectively. $h_{rk} \in \mathbb{C}^{N \times 1}$ denotes the channel from the RIS to Eve's *k*-th antenna. To account for the spatial correlation, the channel matrices are described by employing the Kronecker correlation channel model as [21]

$$\boldsymbol{G}_{ar} = \boldsymbol{G}_{ra}^{\mathsf{T}} = \beta_{ra}^{\frac{1}{2}} \boldsymbol{R}_{S}^{\frac{1}{2}} \tilde{\boldsymbol{H}} \boldsymbol{R}_{I}^{\frac{1}{2}}, \qquad (1)$$

$$\boldsymbol{h}_{ri} = \beta_{ri}^{\frac{1}{2}} \boldsymbol{R}_{I}^{\frac{1}{2}} \tilde{\boldsymbol{h}}_{ri}, \ i \in \{b, k\},$$
(2)

$$\boldsymbol{h}_{aj} = \beta_{aj}^{\frac{1}{2}} \boldsymbol{R}_{S}^{\frac{1}{2}} \tilde{\boldsymbol{h}}_{aj}, \ j \in \{b, k\},$$
(3)

respectively, where $\mathbf{R}_S \in \mathbb{C}^{M \times M}$ and $\mathbf{R}_I \in \mathbb{R}^{N \times N}$ are the spatial correlation matrices at Alice and the RIS, respectively

¹The case studied in this paper can be directly extended to multi-users scenarios, since the pilots used by different users are orthogonal to each other in a single-cell system [19] and thus their PKG processes are independent.

[18]. In addition, $\tilde{H} \in \mathbb{C}^{M \times N}$, $\tilde{h}_{ri} \in \mathbb{C}^{N \times 1}$, and $\tilde{h}_{aj} \in \mathbb{C}^{M \times 1}$ are random matrices with i.i.d. Gaussian random entries of zero mean and unit variance. β_{ra} , β_{ri} , and β_{aj} are the path loss of the corresponding channels, respectively.

B. PKG Framework Based on Transmit and Reflective Beamforming

Now, we propose a new framework to take full advantage of the RIS-assisted PKG in multi-antenna systems. In the PKG system, Alice and Bob first perform channel probing to acquire the reciprocal channel estimation. The process of channel probing is described as follows.

Step 1: Uplink channel sounding. Bob transmits the publicly known pilot $s_u \in \mathbb{C}$ with $|s_u|^2 = 1$. Then, the equivalent baseband signal received at Alice and Eve is expressed as

$$\boldsymbol{y}_{l}^{u} = \sqrt{P_{\mathrm{B}} \left(\boldsymbol{G}_{lr} \boldsymbol{\Phi} \boldsymbol{h}_{rb} + \boldsymbol{h}_{lb} \right) s_{u}} + \boldsymbol{z}_{l}, l \in \{a, e\}, \quad (4)$$

respectively, where $\mathbf{\Phi} = \text{diag}\{\mathbf{v}\}$ with each element $|v_n| \leq 1, \forall n \in \{1, \dots, N\}$, is the reflection coefficients matrix of the RIS. In addition, P_{B} is the transmit power of Bob. The noise follows the circularly symmetric complex Gaussian distribution, i.e., $\mathbf{z}_l \sim C\mathcal{N}(0, \sigma_l^2 \mathbf{I})$, with σ_l^2 being the corresponding noise variances. Then, Alice and Eve perform a standard least-squares (LS) channel estimation [16], [17] as²

$$\hat{\boldsymbol{h}}_{l}^{u} \triangleq s_{u}^{*}\boldsymbol{y}_{l}^{u} = \sqrt{P_{\mathrm{B}}}(\boldsymbol{G}_{lr}\boldsymbol{\Phi}\boldsymbol{h}_{rb} + \boldsymbol{h}_{lb}) + \tilde{\boldsymbol{z}}_{l}^{u}, l \in \{a, e\}, \quad (5)$$

respectively, where the estimation noise is $\tilde{z}_l^u = s_u^* z_l^u$ and $\hat{h}_e^u = [\hat{h}_{e_1}^u, \cdots, \hat{h}_{e_K}^u]^{\mathsf{T}}$.

Step 2: Downlink channel sounding. Alice sends the downlink publicly known pilot $s_d \in \mathbb{C}$ with $|s_d|^2 = 1$ and the signals received at Bob and Eve are

$$y_b^d = (\boldsymbol{h}_{rb}^{\mathsf{T}} \boldsymbol{\Phi} \boldsymbol{G}_{ra} + \boldsymbol{h}_{ab}^{\mathsf{T}}) \boldsymbol{w} s_d + z_b^d, \tag{6}$$

$$\boldsymbol{y}_{e}^{d} = (\boldsymbol{G}_{re}^{\mathsf{T}} \boldsymbol{\Phi} \boldsymbol{G}_{ra} + \boldsymbol{H}_{ae}^{\mathsf{T}}) \boldsymbol{w} \boldsymbol{s}_{d} + \boldsymbol{z}_{e}^{d}, \tag{7}$$

respectively, where $\boldsymbol{w} \in \mathbb{C}^{M \times 1}$ is the transmit beamforming vector at Alice that satisfies $||\boldsymbol{w}||_2^2 \leq P_A$ with P_A being the maximum transmit power of Alice. z_b^d and \boldsymbol{z}_e^d are the additive Gaussian noise with $z_b^d \sim \mathcal{CN}(0, \sigma_b^2)$ and $\boldsymbol{z}_e^d \sim \mathcal{CN}(0, \sigma_e^2 \boldsymbol{I})$. After the LS estimation, Bob and Eve obtain the channel estimates as

$$\hat{h}_b \triangleq s_d^* y_b^d = (\boldsymbol{h}_{rb}^\mathsf{T} \boldsymbol{\Phi} \boldsymbol{G}_{ra} + \boldsymbol{h}_{ab}^\mathsf{T}) \boldsymbol{w} + \tilde{z}_b, \tag{8}$$

$$\hat{\boldsymbol{h}}_{e}^{d} \triangleq s_{d}^{*} \boldsymbol{y}_{e}^{d} = (\boldsymbol{G}_{re}^{\mathsf{T}} \boldsymbol{\Phi} \boldsymbol{G}_{ra} + \boldsymbol{H}_{ae}^{\mathsf{T}}) \boldsymbol{w} + \tilde{\boldsymbol{z}}_{e}^{u}, \qquad (9)$$

respectively, where the noises are $\tilde{z}_b^d = s_d^* z_b^d$ and $\tilde{z}_e^u = s_d^* z_e^u$, respectively, and $\hat{h}_e^d = [\hat{h}_{e_1}^d, \cdots, \hat{h}_{e_K}^d]^{\mathsf{T}}$. Step 3: Reciprocal components acquisition. Since the esti-

Step 3: Reciprocal components acquisition. Since the estimations obtained by Alice and Bob, as shown in (5) and (8), are quite different in terms of both the dimensions and values, we multiply Alice's channel estimation \hat{h}_a^u by w to obtain the combined reciprocal channel gain as

$$\hat{h}_a \triangleq \boldsymbol{w}^\mathsf{T} \hat{\boldsymbol{h}}_a^u = \sqrt{P_{\mathrm{B}}} \boldsymbol{w}^\mathsf{T} (\boldsymbol{G}_{ar} \boldsymbol{\Phi} \boldsymbol{h}_{rb} + \boldsymbol{h}_{ab}) + z_a, \quad (10)$$

where the noise is $z_a = \boldsymbol{w}^{\mathsf{T}} \tilde{\boldsymbol{z}}_a^u$.

Consequently, Alice's combined channel gain, \hat{h}_a , and Bob's channel gains, \hat{h}_b , are highly correlated in general. After

²The LS is adopted since it has been widely used in practical systems [22].

following the procedures of the PKG, i.e., quantization, information reconciliation, and privacy amplification, the channel gains are finally converted into secret keys [23]. Since these steps are similar to those adopted in existing PKG methods, such as [7], [5], in this paper, we focus on the channel probing step, where the transmit and reflective beamforming are jointly optimized to maximize the KGR.

III. PROBLEM FORMULATION AND TRANSFORMATION

In this section, based on the channel estimation acquired in Sec. II, we derive the closed-form KGR expression and formulate an optimization problem regarding the variables wand v to improve the system performance.

We first formulate the KGR given Eve's k-th antenna's channel estimation and maximize the minimal KGR³ [16]. Specifically, the KGR for Eve's k-th antenna is defined as the conditional mutual information of the legitimate parties' channel estimations given the observation of Eve's k-th antenna [7], i.e., $R_k = \mathcal{I}\left(\hat{h}_a; \hat{h}_b \mid \hat{h}_{e_k}^d, \hat{h}_{e_k}^u\right)$. Since Eve is located close to Bob but locates far away from Alice, the channel estimated by Eve in the uplink channel sounding is statistical independent with the legitimate parties' channel estimations [24]. Thus, we have $\mathcal{I}\left(\hat{h}_a; \hat{h}_b \mid \hat{h}_{e_k}^d, \hat{h}_{e_k}^u\right) = \mathcal{I}\left(\hat{h}_a; \hat{h}_b \mid \hat{h}_{e_k}^d\right)$. Therefore, the KGR given Eve's k-th antenna is given by [25], [26]

$$R_k = \log_2 \frac{\det\left(\boldsymbol{R}_{ae_k} \boldsymbol{R}_{be_k}\right)}{\det\left(\boldsymbol{R}_{abe_k}\right) \mathcal{R}_{e_k e_k}},\tag{11}$$

where the covariance matrices are denoted as

$$\boldsymbol{R}_{ue_k} = \begin{bmatrix} \mathcal{R}_{uu} & \mathcal{R}_{ue_k} \\ \mathcal{R}_{e_ku} & \mathcal{R}_{e_ke_k} \end{bmatrix}, u \in \{a, b\},$$
(12)

$$\boldsymbol{R}_{abe_{k}} = \begin{bmatrix} \mathcal{R}_{aa} & \mathcal{R}_{ab} & \mathcal{R}_{ae_{k}} \\ \mathcal{R}_{ba} & \mathcal{R}_{bb} & \mathcal{R}_{be_{k}} \\ \mathcal{R}_{e_{k}a} & \mathcal{R}_{e_{k}b} & \mathcal{R}_{e_{k}e_{k}} \end{bmatrix},$$
(13)

respectively. $\mathcal{R}_{xy} = \mathbb{E}\left\{\hat{h}_x \hat{h}_y^{\mathsf{H}}\right\}, x, y \in \{a, b, e_k\}$ denotes the channel covariances of the corresponding channel estimations.

Substituting the channel estimations into (11) and assuming $\sigma_a^2 = \sigma_b^2 = \sigma_{e_k}^2 = \sigma^2, k \in \{1, \dots, K\}$ for simplicity [16], [17], we provide the following lemma to characterize the KGR.

Lemma 1. The KGR between Alice and Bob, given the channel estimation at Eve's k-th antenna, is expressed as (14) at the top of this page, where $g_u = (\mathbf{w}^T \mathbf{R}_S \mathbf{w}^*)(\beta_r \mathbf{v}^H \tilde{\mathbf{R}}_I \mathbf{v} + \beta_{ab})$, $g_{ue}^k = (\mathbf{w}^T \mathbf{R}_S \mathbf{w}^*)\mathbf{v}^H \tilde{\mathbf{R}}_{bk}^r \mathbf{v} \sqrt{\beta_r \beta_r^k} + \mathbf{w}^T \tilde{\mathbf{R}}_{bk}^d \mathbf{w}^* \sqrt{\beta_{ab}\beta_{ak}}$, $g_e^k = (\mathbf{w}^T \mathbf{R}_S \mathbf{w}^*)(\beta_r^k \mathbf{v}^H \tilde{\mathbf{R}}_I \mathbf{v} + \beta_{ak})$, $\tilde{\mathbf{R}}_{bk}^r = ((\mathbf{R}_I^{\frac{1}{2}})^T \mathbf{R}_{bk}^r (\mathbf{R}_I^{\frac{1}{2}})^T) \circ \mathbf{R}_I$, $\tilde{\mathbf{R}}_{bk}^d = \mathbf{R}_S^{\frac{1}{2}} \mathbf{R}_{bk}^d \mathbf{R}_S^{\frac{1}{2}}$, and $\tilde{\mathbf{R}}_I = \mathbf{R}_I^T \circ \mathbf{R}_I$. Also, $\beta_r = \beta_{ra}\beta_{rb}$, $\beta_r^k = \beta_{ra}\beta_{rk}$, and the covariance matrices are defined as $\mathbf{R}_{bk}^r \triangleq \mathbb{E}{\{\tilde{\mathbf{h}}_{rk}^* \tilde{\mathbf{h}}_{rb}^T\}}$ and $\mathbf{R}_{bk}^d \triangleq \mathbb{E}{\{\tilde{\mathbf{h}}_{ab}^* \tilde{\mathbf{h}}_{ak}^H\}}$.

Remark 1. From the KGR expression in (14), we can observe that the KGR is only related to the beamforming vectors and

statistical channel information, i.e., the covariance matrices. Since the covariance matrices alter slowly in dense scattering environments [21], we assume that these matrices have been obtained from the previous several time slots by using existing methods, such as the general maximum-likelihood estimation in [27], and we focus on the beamforming optimization to improve the PKG performance.

Remark 2. If the existing i.i.d. channel model assumptions are adopted to optimize the RIS reflection coefficients, the spatial correlation matrices \mathbf{R}_S and \mathbf{R}_I will be the identity matrices. Hence, the $\mathbf{w}^{\mathsf{T}}\mathbf{R}_S\mathbf{w}^*$ and $\mathbf{v}^{\mathsf{H}}\mathbf{\tilde{R}}_I\mathbf{v}$ in (14) are calculated as P_A and N, respectively. For the case of $\mathbf{R}_{bk}^r = \rho_k \mathbf{I}_{N\times N}$ and $\mathbf{R}_{bk}^d = \rho_k \mathbf{I}_{M\times M}$, where ρ_k is the channel correlation between Eve and Bob, the beamforming design is considered to be independent of the KGR. This observation highlights the importance of taking into account the spatial correlation.

Thus, the beamforming design for spatially correlated channel models could be formulated as

$$\max_{\boldsymbol{w},\boldsymbol{v}} \min_{k} \left\{ \mathcal{I}\left(\hat{h}_{a}; \hat{h}_{b} \mid \hat{h}_{e_{k}}\right) \right\}$$
s.t. C1: $||\boldsymbol{w}||_{2}^{2} \leq P_{A}$,
C2: $|v_{n}| \leq 1, \forall n \in \{1, \cdots N\}$, (15)

where C1 indicates the transmit beamforming is constrained by the maximum transmit power budget at the BS, while C2 represents the modulus constraint of each RIS reflection coefficient.

It could be found that in problem (15), the variables w and v are in high-order and coupled in the objective function. To tackle this problem, we first simplify the optimization problem by using the following lemma.

Lemma 2. The original problem (15) is equivalent to the following problem:

$$\max_{\bar{\boldsymbol{w}},\boldsymbol{v}} \min_{k} \left\{ f_k(\bar{\boldsymbol{w}}, \boldsymbol{v}) \right\}$$

s.t. C1, C2, (16)

where $f_k(\bar{w}, v) = \bar{w}^{\mathsf{H}} R_S \bar{w} v^{\mathsf{H}} \bar{R}_u \bar{k}_{bk} v + \bar{w}^{\mathsf{H}} \bar{R}_{bk} \bar{w}^{\mathsf{H}} \bar{z}_{k}$, $\bar{R}_u = \beta_r R_I^{\mathsf{T}} \circ R_I + \frac{\beta_{ab}}{N} I$, $\bar{w}^{\mathsf{H}} R_S \bar{w} v^{\mathsf{H}} \bar{R}_k v + \sigma^2$, $\bar{R}_u = \beta_r R_I^{\mathsf{T}} \circ R_I + \frac{\beta_{ab}}{N} I$, $\bar{R}_{bk}^r = \sqrt{\beta_r \beta_r^k} \tilde{R}_{bk}^r$, $\bar{R}_{bk}^d = \sqrt{\beta_{ab} \beta_{ak}} \tilde{R}_{bk}^d$, $\bar{R}_k = \beta_r^k R_I^{\mathsf{T}} \circ R_I + \frac{\beta_{ak}}{N} I$, and the variable is defined as $\bar{w} \stackrel{\Delta}{=} w^*$ for the sake of notational simplicity.

Proof: It can be proved by using Appendix B in [1] and defining $x = f_k(\bar{w}, v)$.

An intuitive solution to tackle problem (16) is to apply the existing ASSG algorithm. Specifically, the ASSG algorithm can be applied to alternatingly solve for w and v while fixing the other variable, yielding two subproblems with respect to w and v, respectively. In each subproblem, SDR-SCA with Gaussian randomization in [16] can be then leveraged to convexify the problem. However, in the ASSG algorithm, a series of SDP problems generated by the SCA method need to be solved at each alternating iteration. In fact, the number of optimization variables in each SDP problem is the square of the number of RIS elements or the BS antennas, contributing

³The KGR expression and the beamforming design in this paper can also be applied to the scenario with multiple single-antenna eavesdroppers.

$$R_{k} = \log_{2} \left(\frac{\left(P_{\mathrm{B}} g_{u} g_{e}^{k} + (P_{\mathrm{B}} g_{u} + g_{e}^{k} ||\boldsymbol{w}||^{2}) \sigma^{2} + ||\boldsymbol{w}||_{2}^{2} \sigma^{4} - P_{\mathrm{B}} |g_{ue}^{k}|^{2} \right) \left(g_{u} g_{e}^{k} + (g_{u} + g_{e}^{k}) \sigma^{2} + \sigma^{4} - |g_{ue}^{k}|^{2} \right)}{\left[(P_{\mathrm{B}} + ||\boldsymbol{w}||_{2}^{2}) \left(g_{u} g_{e}^{k} + (g_{u} + g_{e}^{k}) \sigma^{2} + \sigma^{4} - |g_{ue}^{k}|^{2} \right) - P_{\mathrm{B}} \sigma^{2} (g_{e}^{k} + \sigma^{2}) \right] \left(g_{e}^{k} + \sigma^{2}) \sigma^{2} \right)}.$$
(14)

to a high-dimensional optimization problem [28]. At the same time, in RIS-assisted wireless communication systems, the RIS is often equipped with a large number of elements [29]. The required computational effort may be unaffordable when ASSG is applied to solve Problem (16), which motivates us to develop a new low-complexity algorithm for RIS-assisted PKG systems.

IV. IMPACT OF DIFFERENT BEAMFORMING METHODS ON **PKG PERFORMANCE**

Before solving Problem (16), in this section, we aim to compare the PKG performance under the existing assumptions of the i.i.d. channel model [15]–[17] and the spatially correlated model when Eve experiences independent fading channels.

Lemma 3. In the case where the eavesdropping channels are independent of the legitimate channels, the KGR increases monotonically with $\bar{w}^{\mathsf{H}} R_S w(\beta_r v^{\mathsf{H}} \tilde{R}_I v + \beta_{ab})$.

Proof: See Lemma 1 in [1].

Remark 3. We first note that the channel correlation between the uplink and downlink channels is \mathcal{R}_{ab} = $\sqrt{P_{\rm B}} \bar{\boldsymbol{w}}^{\sf H} \boldsymbol{R}_S \boldsymbol{w}(\beta_r \boldsymbol{v}^{\sf H} \tilde{\boldsymbol{R}}_I \boldsymbol{v} + \beta_{ab})$. Thus, when optimizing the KGR, the overall channel correlations is increased with the assistance of RIS. In addition, since $\bar{w}^{\mathsf{H}} R_S w$ and $\beta_r v^{\mathsf{H}} \tilde{R}_I v +$ β_{ba} are both non-negative, solving Problem (16) is equivalent to maximize these two terms separately. Thus, the optimal solution to Problem (16) is $\bar{w}_{opt} = \sqrt{P_A} u_{\lambda_{max}}$ and $v_n = e^{j\theta_n}$ with $\theta_n = \theta, \forall n \in \{1, \dots, N\}$, where $u_{\lambda_{\max}}$ is the dominant eigenvector of the matrix \mathbf{R}_S corresponding to its maximum eigenvalue λ_{\max} and θ could take on any value in the interval of $[0, 2\pi)$.

A. KGR under Different Assumptions of Channel Model at BS

As shown in Lemma 3, the KGR is proportional to $\bar{w}^{\mathsf{H}}R_{S}\bar{w}$. Under the assumption of the i.i.d. model, the spatial correlation matrix R_S is the identity matrix. In this case, the design of transmit beamforming is independent of KGR. As such, random beamforming $\widetilde{\boldsymbol{w}} = \sqrt{P_{\rm A}}\widetilde{\boldsymbol{w}}_0/||\widetilde{\boldsymbol{w}}_0||_2$ is applied without loss of generality and optimality, where the entries in \widetilde{w}_0 are i.i.d. random variables with zero mean. Then, the expectation of $\widetilde{w}^{\mathsf{H}} R_S \widetilde{w}$ can be calculated as $\mathbb{E} \{ \widetilde{w}^{\mathsf{H}} R_S \widetilde{w} \} =$ $P_{\rm A}$, which is independent of the antenna number and the spatial correlation at the BS. To investigate the performance loss caused by the design based on the i.i.d. channel assumption, we focus on a typical implementation model of multiple antennas for massive multiple-input multiple-output (MIMO). We consider a general uniform planar array (UPA) model, where the spatial correlation matrix can be approximated as $R_S \approx R_h \otimes R_v$ [30], where $R_h \succeq 0$ and $R_v \succeq 0$ are the covariance matrices of the horizontal and the vertical uniform linear array (ULA), respectively. The ULA spatial correlation is modeled as a Toeplitz matrix with each element $[\mathbf{R}_l]_{i,j} =$ $\rho^{|i-j|}, l \in \{h, v\}$, where $0 \le \rho \le 1$ is the correlation index among the antennas. Given the optimal transmit beamforming $ar{w}_{\mathrm{opt}}$, we further characterize $ar{w}_{\mathrm{opt}}^{\mathsf{H}} R_S ar{w}_{\mathrm{opt}}$ via the following lemma.

Lemma 4. For a UPA model, the upper and lower bounds for $ar{w}_{\text{opt}}^{\mathsf{H}} R_S ar{w}_{\text{opt}}$ are given by

$$f_l(N_{\rm H}^t, N_{\rm V}^t, \rho) \le \bar{\boldsymbol{w}}_{\rm opt}^{\sf H} \boldsymbol{R}_S \bar{\boldsymbol{w}}_{\rm opt} \le f_u(N_{\rm H}^t, N_{\rm V}^t, \rho), \quad (17)$$

where $f_l(N_{\rm H}^t, N_{\rm V}^t, \rho) = P_{\rm A} \frac{\left(N_{\rm H}^t(1-\rho^2)-2\rho(1-\rho^{N_{\rm H}^t})\right)}{N_{\rm H}^t N_{\rm V}^t(1-\rho)^4} \times \left(N_{\rm V}^t(1-\rho^2)-2\rho(1-\rho^{N_{\rm V}^t})\right) \text{ and } f_u(N_{\rm H}^t, N_{\rm V}^t, \rho) = P_{\rm A} \frac{(1+\rho^2)(1-\rho^{N_{\rm H}^t-1})(1-\rho^{N_{\rm V}^t-1})}{(1-\rho)^2}. N_{\rm H}^t \text{ and } N_{\rm V}^t \text{ are the number of antennas at horizontal and vertical domains, respectively.}$

Proof: See Lemma 3 in the conference version of this paper [1].

This lemma shows that both the upper and lower bounds increase monotonically with the correlation coefficients ρ , the number of antennas $N_{\rm H}^t$, and $N_{\rm V}^t$. This is because the SNR of the combined channel gain increases with the spatial correlation. Specifically, when $\rho = 0$, the bounds are $f_l =$ $f_u = P_A$, which means the optimal transmit beamforming and random beamforming achieve the same PKG performance in the i.i.d. fading channels. In addition, it can be observed that both the upper and lower bounds converge to $P_{\rm A}(\frac{1+\rho}{1-\rho})^2$ as $N_{\rm H}^t \to \infty$ and $N_{\rm V}^t \to \infty$. This means that when the BS is equipped with a large number of antennas, the KGR depends only on the correlations among the antennas of the BS for a given power. Also, the KGR increases monotonically with the correlation coefficient ρ . The limit of $\bar{w}_{opt}^{\mathsf{H}} R_S \bar{w}_{opt}$ for $\rho = 1$ is $P_{\rm A} N_{\rm H}^t N_{\rm V}^t$, which is bounded by the transmit power and the antenna numbers at the BS.

B. KGR under Different Assumptions of Channel Model at RIS

In Lemma 3, the KGR is proportional to $v^{\mathsf{H}}\tilde{R}_{I}v$. Under the assumption of the i.i.d. channel model adopting in existing works, e.g., [15]–[17], the spatial correlation matrix is $\hat{R}_{I} =$ I. By employing random reflection, the expectation of $\tilde{v}^{\mathsf{H}} R_I \tilde{v}$ is $\mathbb{E}{\{\widetilde{v}^{\mathsf{H}}\widetilde{R}_{I}\widetilde{v}\}} = N$, where each phase in \widetilde{v} can be drawn from the uniform distribution, i.e., $\tilde{\theta}_i \sim U[0, 2\pi), i \in \{1, \dots, N\}.$

Taking the spatial correlation model into account, the maximum value of $v^{\mathsf{H}}\tilde{R}_{I}v$ is $||R_{I}||_{F}^{2}$. In isotropic scattering environments, the spatial correlation of RIS is expressed as [18]

$$[\mathbf{R}_{I}]_{n,m} = \operatorname{sinc} \frac{2 \| u_{n} - u_{m} \|_{2}}{\lambda}, \ \forall n, m \in \{1, \cdots, N\}, \ (18)$$

where $\|\boldsymbol{u}_n - \boldsymbol{u}_m\|_2$ denotes the distance between the *n*-th RIS element and the *m*-th RIS element, λ is the wavelength. Since the sinc function $\operatorname{sinc}(x) = \operatorname{sinc}(\pi x)/(\pi x)$ is monotonically decreasing in interval [0,1), the entries in \mathbf{R}_I is larger as the inter-element spacing becomes smaller, when the distance between each element pair fulfills $||\boldsymbol{u}_n - \boldsymbol{u}_m||_2 \leq \frac{\lambda}{2}$. Moreover, the optimal value of $\boldsymbol{v}^{\mathsf{H}} \tilde{\boldsymbol{R}}_I \boldsymbol{v}$ satisfies $||\boldsymbol{R}_I||_F^2 > N$ because the correlation between the elements always exists in practical RIS systems [18]. Hence, the KGR performance of the proposed reflective beamforming is better than the counterpart adopting the assumption of the i.i.d. channel model.

C. Security Analysis

In the above analysis, we assume the channels between Bob and Eve are independent. However, in reality Eve may experience correlated channels w.r.t. Bob if Eve's antennas are close to Bob [23]. Therefore, we first analyze the information leakage to Eve if the correlation between eavesdropping channels and legitimate channels is not considered when optimizing w and v. To this end, we have the following Lemma.

Lemma 5. Assume that ρ_k is the cross channel correlation between Bob and Eve [23], i.e., $\mathbf{R}_{bk}^r = \rho_k \mathbf{I}_{N \times N}$ and $\mathbf{R}_{bk}^d = \rho_k \mathbf{I}_{M \times M}$. Given the $\bar{\mathbf{w}}_{opt}$ and \mathbf{v}_{opt} in Remark 3, the amount of information leaked to Eve increases with the spatial correlation at the BS and the RIS grows.

Proof: Given the \bar{w}_{opt} and v_{opt} , the second term in (16) is denoted as

$$f_k^e = \rho_k^2 \left(\lambda_{\max}(\boldsymbol{R}_S)\right)^2 \frac{\left(\|\boldsymbol{R}_I\|_F^2 \sqrt{\beta_r \beta_r^k} + \sqrt{\beta_{ab} \beta_{ak}}\right)^2}{\lambda_{\max}(\boldsymbol{R}_S)(\beta_r^k \|\boldsymbol{R}_I\|_F^2 + \beta_{ak}) + \sigma^2}.$$
(19)

Since $\frac{\partial f_k^e}{\partial(\lambda_{\max}(\mathbf{R}_S))} \geq 0$ and $\frac{\partial f_k^e}{\partial(\|\mathbf{R}_I\|_F^2)} \geq 0$, the amount of information leaked to Eve is monotonically increasing for $\lambda_{\max}(\mathbf{R}_S)$ and $\|\mathbf{R}_I\|_F^2$. Also, $\lambda_{\max}(\mathbf{R}_S)$ and $\|\mathbf{R}_I\|_F^2$ increase with the spatial correlation at the BS and the RIS, respectively. This completes the proof.

Lemma 5 states the connections between spatial correlation and security when the correlation between Bob and Eve's channels are ignored. In the following section, we will consider a more general case, i.e., Problem (16), and propose an effective algorithm to tackle it.

V. BSUM Algorithm For Maximum Key Generation Rate

In this section, we propose an BSUM-based algorithm to tackle Problem (16). We decompose the optimization variables, i.e., \bar{w} and v, into independent blocks and update the blocks by successively maximizing a sequence of approximations of the objective function in (16).

A. The BSUM Algorithm for Problem (16)

For the simplicity of algorithm design, we first convert Problem (16) from the complex domain to the real domain⁴. By defining $\tilde{\boldsymbol{v}} = \left[\Re\{\boldsymbol{v}\}^{\top}, \Im\{\boldsymbol{v}\}^{\top}\right]^{\top} \in \mathbb{R}^{2N}$ and $\tilde{\boldsymbol{w}} =$

⁴We transform the problem into the real domain since the modulus operator of complex number in (16) makes the problem intractable.

 $\left[\Re\{\bar{\boldsymbol{w}}\}^{\top}, \Im\{\bar{\boldsymbol{w}}\}^{\top}\right]^{\top} \in \mathbb{R}^{2N}$, the optimization problem (16) is equivalent to

$$\max_{\tilde{\boldsymbol{w}}, \tilde{\boldsymbol{v}}} \min_{k} \left\{ \tilde{f}_{k}(\tilde{\boldsymbol{w}}, \tilde{\boldsymbol{v}}) \right\}$$
s.t.
$$\overline{\text{C1:}} \|\tilde{\boldsymbol{w}}\|_{2}^{2} \leq P_{\text{A}},$$

$$\overline{\text{C2:}} \tilde{v}_{n}^{2} + \tilde{v}_{n+N}^{2} \leq 1, \forall n \in \{1, \cdots N\},$$

$$(20)$$

where
$$\tilde{f}_{k}(\tilde{w}, \tilde{v}) = \tilde{w}^{\mathsf{T}} \tilde{R}_{S} \tilde{w} \tilde{v}^{\mathsf{T}} \tilde{R}_{u} \tilde{v} - \frac{(\tilde{w}^{\mathsf{T}} \tilde{R}_{S} \tilde{w} \tilde{v}^{\mathsf{T}} \tilde{Q}_{k}^{\mathsf{T}} \tilde{v} + \tilde{w}^{\mathsf{T}} \tilde{Q}_{k}^{\mathsf{T}} \tilde{w})^{2}}{\tilde{w}^{\mathsf{T}} \tilde{R}_{S} \tilde{w} \tilde{v}^{\mathsf{T}} \tilde{R}_{k} \tilde{v} + \sigma^{2}} - \frac{(\tilde{w}^{\mathsf{T}} \tilde{R}_{S} \tilde{w} \tilde{v}^{\mathsf{T}} \tilde{R}_{k} \tilde{v} + \tilde{w}^{\mathsf{T}} \tilde{P}_{k}^{\mathsf{T}} \tilde{w})^{2}}{\tilde{w}^{\mathsf{T}} \tilde{R}_{S} \tilde{w} \tilde{v}^{\mathsf{T}} \tilde{R}_{k} \tilde{v} + \sigma^{2}},$$

$$\tilde{Q}_{k}^{l} = \begin{bmatrix} \Re\{\frac{\bar{R}_{bk}^{l} + (\bar{R}_{bk}^{l})^{\mathsf{H}}}{2}\} - \Im\{\frac{\bar{R}_{bk}^{l} + (\bar{R}_{bk}^{l})^{\mathsf{H}}}{2}\} - \Im\{\frac{\bar{R}_{bk}^{l} + (\bar{R}_{bk}^{l})^{\mathsf{H}}}{2}\} \end{bmatrix},$$

$$\tilde{P}_{k}^{l} = \begin{bmatrix} \Re\{\frac{\bar{R}_{bk}^{l} - (\bar{R}_{bk}^{l})^{\mathsf{H}}}{2j}\} - \Im\{\frac{\bar{R}_{bk}^{l} - (\bar{R}_{bk}^{l})^{\mathsf{H}}}{2}\} \end{bmatrix}, l \in \{r, d\},$$
and $\tilde{A} = \begin{bmatrix} \Re\{\bar{A}_{k}^{\mathsf{T}} - \Im\{\bar{A}_{k}^{\mathsf{T}} - \Im\{\bar{A}_{k}^{\mathsf{T}}$

and $\mathbf{A} = \begin{bmatrix} \Im\{\bar{\mathbf{A}}\} & \Re\{\bar{\mathbf{A}}\} \end{bmatrix}$, $\mathbf{A} \in \{\mathbf{R}_S, \mathbf{R}_u, \mathbf{R}_k\}$. Then, since \tilde{w} and \tilde{v} are coupled in Problem (20), we utilize the BSUM algorithm [31] to decompose them into independent blocks. Specifically, in each iteration, the BSUM algorithm updates a single block of variables by solving an approximate problem of the original problem. If each approximated problem fulfills some conditions as in [32], the sequence of the objective values converges and first-order optimality holds upon convergence. Specifically, according to Sec. III-C in [32], given $\tilde{w}^{(i)}$ in the *i*-th iteration of BSUM, we could construct a lower bound of $\tilde{f}_k(\tilde{w}^{(i)}, \tilde{v})$ as

$$\tilde{f}_{k}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}) \geq \tilde{f}_{k}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i)}) + \left(\nabla_{\tilde{\boldsymbol{v}}} \tilde{f}_{k}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i)})\right)^{\mathsf{T}} \\
\times \left(\tilde{\boldsymbol{v}} - \tilde{\boldsymbol{v}}^{(i)}\right) - \frac{1}{2} (\tilde{\boldsymbol{v}} - \tilde{\boldsymbol{v}}^{(i)})^{\mathsf{T}} \mathbf{M}_{k}^{(i)} (\tilde{\boldsymbol{v}} - \tilde{\boldsymbol{v}}^{(i)}) \\
= -\frac{1}{2} \tilde{\boldsymbol{v}}^{\mathsf{T}} \mathbf{M}_{k}^{(i)} \tilde{\boldsymbol{v}} + \left(\boldsymbol{p}_{k}^{(i)}\right)^{\mathsf{T}} \tilde{\boldsymbol{v}} + q_{k}^{(i)},$$
(21)

where $\mathbf{M}_{k}^{(i)} = \bar{L}_{k}^{(i)} \mathbf{I}_{2N \times 2N}$ that satisfies $\mathbf{M}_{k}^{(i)} \succeq -\nabla_{\tilde{\boldsymbol{v}}}^{2} \tilde{f}_{k}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}})$, and $\bar{L}_{k}^{(i)}$ is calculated as

$$\begin{split} \bar{L}_{k}^{(i)} = & \frac{N}{\sigma^{2}} \left(\frac{4((\tilde{q}_{w}^{(i)} + N\lambda_{\max}(\hat{\boldsymbol{Q}}_{k}^{(i)}))^{2} + (\tilde{p}_{w}^{(i)} + N\lambda_{\max}(\hat{\boldsymbol{P}}_{k}^{(i)}))^{2})}{\sigma^{4}} \\ & \times (m_{w}^{(i)})^{2} N\lambda_{\max} \left(\tilde{\boldsymbol{R}}_{k} \tilde{\boldsymbol{R}}_{k} \right) + 2N \left(\lambda_{\max} \left(\hat{\boldsymbol{Q}}_{k}^{(i)} (\hat{\boldsymbol{Q}}_{k}^{(i)} + (\hat{\boldsymbol{Q}}_{k}^{(i)})^{\mathsf{T}}) \right) \right) \\ & + \lambda_{\max} \left(\hat{\boldsymbol{P}}_{k}^{(i)} (\hat{\boldsymbol{P}}_{k}^{(i)} + (\hat{\boldsymbol{P}}_{k}^{(i)})^{\mathsf{T}}) \right) \right) + \left(\tilde{q}_{w}^{(i)} + N\lambda_{\max} \left(\hat{\boldsymbol{Q}}_{k}^{(i)} \right) \\ & \times \lambda_{\max} \left(\hat{\boldsymbol{Q}}_{k}^{(i)} + (\hat{\boldsymbol{Q}}_{k}^{(i)})^{\mathsf{T}} \right) + \left(\tilde{p}_{w}^{(i)} + N\lambda_{\max} \left(\hat{\boldsymbol{P}}_{k}^{(i)} \right) \right) \\ & \times \lambda_{\max} \left(\hat{\boldsymbol{P}}_{k}^{(i)} + (\hat{\boldsymbol{P}}_{k}^{(i)})^{\mathsf{T}} \right) \right), \end{split}$$

where $m_w^{(i)} = (\tilde{\boldsymbol{w}}^{(i)})^{\mathsf{T}} \tilde{\boldsymbol{R}}_S \tilde{\boldsymbol{w}}^{(i)}, \tilde{q}_w^{(i)} = (\tilde{\boldsymbol{w}}^{(i)})^{\mathsf{T}} \tilde{\boldsymbol{Q}}_k^d \tilde{\boldsymbol{w}}^{(i)}, \tilde{p}_w^{(i)} = (\tilde{\boldsymbol{w}}^{(i)})^{\mathsf{T}} \tilde{\boldsymbol{P}}_k^d \tilde{\boldsymbol{w}}^{(i)}, \hat{\boldsymbol{Q}}_k^{(i)} = m_w^{(i)} \tilde{\boldsymbol{Q}}_k^r, \hat{\boldsymbol{P}}_k^{(i)} = m_w^{(i)} \tilde{\boldsymbol{P}}_k^r.$ In addition, $\boldsymbol{p}_k^{(i)} = \left(\nabla_{\tilde{\boldsymbol{v}}} \tilde{f}_k(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i)}) \right)^{\mathsf{T}} \tilde{\boldsymbol{v}}^{(i)} + \bar{L}_k^{(i)} \tilde{\boldsymbol{v}}^{(i)}, \text{ and } q_k^{(i)} = \tilde{f}_k(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i)}) - \left(\nabla_{\tilde{\boldsymbol{v}}} \tilde{f}_k(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i)}) \right)^{\mathsf{T}} \tilde{\boldsymbol{v}}^{(i)} - \bar{L}_k^{(i)} (\tilde{\boldsymbol{v}}^{(i)})^{\mathsf{T}} \tilde{\boldsymbol{v}}^{(i)}.$ As a result, we have

$$\min_{k} \left\{ \tilde{f}_{k}(\tilde{\boldsymbol{w}}, \tilde{\boldsymbol{v}}) \right\} \geq \min_{k} \left\{ -\frac{1}{2} \tilde{\boldsymbol{v}}^{\mathsf{T}} \mathbf{M}_{k}^{(i)} \tilde{\boldsymbol{v}} + (\boldsymbol{p}_{k}^{(i)})^{\mathsf{T}} \tilde{\boldsymbol{v}} + q_{k}^{(i)} \right\},$$
(23)

and the optimal solution $\tilde{v}^{(i+1)}$ can be obtained by solving the nonsmooth convex problem

$$\max_{\tilde{\boldsymbol{v}}} \min_{k} \left\{ -\frac{1}{2} \tilde{\boldsymbol{v}}^{\mathsf{T}} \mathbf{M}_{k}^{(i)} \tilde{\boldsymbol{v}} + (\boldsymbol{p}_{k}^{(i)})^{\mathsf{T}} \tilde{\boldsymbol{v}} + q_{k}^{(i)} \right\}$$

s.t. $\overline{\text{C2.}}$ (24)

Similarly, when the beamforming vector $\tilde{\boldsymbol{v}}^{(i)}$ is fixed in the *i*-th iteration, we could construct the lower bound of $\tilde{f}_k(\tilde{\boldsymbol{w}}, \tilde{\boldsymbol{v}}^{(i)})$ with respect to $\tilde{\boldsymbol{w}}$ as

$$\tilde{f}_{k}(\tilde{\boldsymbol{w}}, \tilde{\boldsymbol{v}}^{(i)}) \geq \tilde{f}_{k}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i)}) + \left(\nabla_{\tilde{\boldsymbol{v}}} \tilde{f}_{k}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i)})\right)^{\mathsf{T}} \\
\times \left(\tilde{\boldsymbol{w}} - \tilde{\boldsymbol{w}}^{(i)}\right) - \frac{1}{2} (\tilde{\boldsymbol{w}} - \tilde{\boldsymbol{w}}^{(i)})^{\mathsf{T}} \mathbf{L}_{k}^{(i)} (\tilde{\boldsymbol{w}} - \tilde{\boldsymbol{w}}^{(i)}) \\
= -\frac{1}{2} \tilde{\boldsymbol{w}}^{\mathsf{T}} \mathbf{L}_{k}^{(i)} \tilde{\boldsymbol{w}} + (\boldsymbol{a}_{k}^{(i)})^{\mathsf{T}} \tilde{\boldsymbol{w}} + b_{k}^{(i)}, \quad (25)$$

where $\mathbf{L}_{k}^{(i)} = \tilde{L}_{k}^{(i)} \mathbf{I}_{2M \times 2M}$ and $\tilde{L}_{k}^{(i)}$ is calculated as

$$\begin{split} \tilde{L}_{k}^{(i)} &= \frac{2P_{A}}{\sigma^{2}} \left(\lambda_{\max} \left(\bar{\boldsymbol{Q}}_{k}^{(i)} (\bar{\boldsymbol{Q}}_{k}^{(i)} + (\bar{\boldsymbol{Q}}_{k}^{(i)})^{\mathsf{T}} + (\bar{\boldsymbol{Q}}_{k}^{(i)})^{\mathsf{T}} \right) \\ &\times (\bar{\boldsymbol{Q}}_{k}^{(i)} + (\bar{\boldsymbol{Q}}_{k}^{(i)})^{\mathsf{T}}) \right) + \lambda_{\max} \left(\bar{\boldsymbol{Q}}_{k}^{(i)} \right) \\ &\times \lambda_{\max} \left(\bar{\boldsymbol{Q}}_{k}^{(i)} + (\bar{\boldsymbol{Q}}_{k}^{(i)})^{\mathsf{T}} \right) + (m_{v}^{(i)})^{2} \frac{4P_{A}^{3}}{\sigma^{4}} \lambda_{\max} \left(\tilde{\boldsymbol{R}}_{S} \tilde{\boldsymbol{R}}_{S} \right) \\ &\times (\lambda_{\max}^{2} \left(\bar{\boldsymbol{Q}}_{k}^{(i)} \right) + \lambda_{\max}^{2} \left(\bar{\boldsymbol{P}}_{k}^{(i)} \right)) + \lambda_{\max} \left(\bar{\boldsymbol{P}}_{k}^{(i)} \right) \\ &\times \lambda_{\max} \left(\bar{\boldsymbol{P}}_{k}^{(i)} + (\bar{\boldsymbol{P}}_{k}^{(i)})^{\mathsf{T}} \right) + \lambda_{\max} \left(\bar{\boldsymbol{Q}}_{k}^{(i)} (\bar{\boldsymbol{Q}}_{k}^{(i)} + (\bar{\boldsymbol{Q}}_{k}^{(i)})^{\mathsf{T}} \\ &+ (\bar{\boldsymbol{Q}}_{k}^{(i)})^{\mathsf{T}} (\bar{\boldsymbol{Q}}_{k}^{(i)} + (\bar{\boldsymbol{Q}}_{k}^{(i)})^{\mathsf{T}}) \right) \right), \end{split}$$

where $\bar{\boldsymbol{Q}}_{k}^{(i)} = \tilde{\boldsymbol{v}}^{(i)} \tilde{\boldsymbol{Q}}_{k}^{r} \tilde{\boldsymbol{v}}^{(i)} \tilde{\boldsymbol{R}}_{S} + \tilde{\boldsymbol{Q}}_{k}^{d}, \bar{\boldsymbol{P}}_{k}^{(i)} = \tilde{\boldsymbol{v}}^{(i)} \tilde{\boldsymbol{P}}_{k}^{r} \tilde{\boldsymbol{v}}^{(i)} \tilde{\boldsymbol{R}}_{S} + \tilde{\boldsymbol{P}}_{k}^{d}, m_{v}^{(i)} = (\tilde{\boldsymbol{v}}^{(i)})^{\mathsf{T}} \tilde{\boldsymbol{R}}_{k} \tilde{\boldsymbol{v}}^{(i)}.$ Also, $\boldsymbol{a}_{k}^{(i)} = \left(\nabla_{\tilde{\boldsymbol{w}}} \tilde{f}_{k}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i)})\right)^{\mathsf{T}} \tilde{\boldsymbol{w}}^{(i)} + \bar{L}_{k}^{(i)} \tilde{\boldsymbol{w}}^{(i)},$ and $\boldsymbol{b}_{k}^{(i)} = \tilde{f}_{k}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i)}) - \left(\nabla_{\tilde{\boldsymbol{w}}} \tilde{f}_{k}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i)})\right)^{\mathsf{T}} \tilde{\boldsymbol{w}}^{(i)} - \bar{L}_{k}^{(i)} (\tilde{\boldsymbol{w}}^{(i)})^{\mathsf{T}} \tilde{\boldsymbol{w}}^{(i)}.$ Then, we have $\min_{k} \left\{ \bar{f}_{k}(\tilde{\boldsymbol{w}}, \tilde{\boldsymbol{v}}^{(i)}) \right\} \geq \min_{k} \left\{ -\frac{1}{2} \tilde{\boldsymbol{w}}^{\mathsf{T}} \mathbf{L}_{k}^{(i)} \tilde{\boldsymbol{w}} + (\boldsymbol{a}_{k}^{(i)})^{\mathsf{T}} \tilde{\boldsymbol{w}} + \boldsymbol{b}_{k}^{(i)} \right\}$ and the convex problem to find the optimal transmit beamforming $\tilde{\boldsymbol{w}}^{(i+1)}$ can be described as

$$\max_{\tilde{\boldsymbol{w}}} \min_{k} \left\{ -\frac{1}{2} \tilde{\boldsymbol{w}}^{\mathsf{T}} \mathbf{L}_{k}^{(i)} \tilde{\boldsymbol{w}} + (\boldsymbol{a}_{k}^{(i)})^{\mathsf{T}} \tilde{\boldsymbol{w}} + b_{k}^{(i)} \right\}$$

s.t. $\overline{\text{CI}}.$ (27)

B. Convergence Analysis

The overall BSUM algorithm for solving Problem (20) is summarized as Algorithm 1. After obtaining the optimized vectors \tilde{v}_* and \tilde{w}_* , we convert them to the complex domain. The convergence analysis of the BSUM algorithm is shown as the following lemma.

Lemma 6. The objective values of Problem (20) achieved by the iteration sequence $\{\tilde{\boldsymbol{v}}^{(i)}, \tilde{\boldsymbol{w}}^{(i)}\}_{i=0}^{\infty}$ are non-decreasing and convergence.

Proof: See Appendix B.

Algorithm 1 The BSUM Algorithm for Problem (20).

Require: Threshold ε_0 and covariance matrices $\tilde{R}_S, \tilde{R}_u, \tilde{Q}_k^r, \tilde{Q}_k^d, \tilde{P}_k^r, \tilde{P}_k^d, k \in \{1, \cdots, K\};$

1: Set:
$$i =$$

2: Initial: $\tilde{\boldsymbol{v}}^{(0)}$ and $\tilde{\boldsymbol{w}}^{(0)}$;

3: repeat

4: Update $\tilde{v}^{(i+1)}$ by solving Problem (24);

5: Update $\tilde{w}^{(i+1)}$ by solving Problem (27);

6: Calculate the objective value of Problem (20) as

$$R^{(i+1)} = \min_{k} \tilde{f}_{k}(\tilde{\boldsymbol{w}}^{(i+1)}, \tilde{\boldsymbol{v}}^{(i+1)}); \qquad (28)$$

7: $i \leftarrow i + 1;$ 8: **until** $|R^{(i)} - R^{(i-1)}| \le \varepsilon_0;$

C. Computational Complexity

In the proposed BSUM algorithm, solving the non-smooth convex problems in (24) and (27) in each iteration contributes to the most computational cost. The standard method to solve non-smooth max-min convex problems is to introduce an auxiliary variable r that yields the problem

$$\max_{\tilde{\boldsymbol{v}},r} r$$
s.t. $\overline{\mathbf{C2}}, \mathbf{C9}: -\frac{1}{2}\tilde{\boldsymbol{v}}^{\mathsf{T}}\mathbf{M}_{k}^{(i)}\tilde{\boldsymbol{v}} + (\boldsymbol{p}_{k}^{(i)})^{\mathsf{T}}\tilde{\boldsymbol{v}} + q_{k}^{(i)} \ge r.$ (29)

Problem (29) is a convex QCQP problem that can be solved by the standard interior-point method [33]. However, the computational complexity of interiorpoint method to obtain an ϵ -optimal solution is $\mathcal{O}\left(\left(2N^3 + KN^2\right)\left(\sqrt{N+K}\log\frac{2(N+K)}{\epsilon}\right)\right)$. Thus, the overall computational cost to solve the original problem is still expensive, especially in the case of large N, M, or K.

Another algorithm to solve the problems in (24) and (27) is the projected sub-gradient methods [34], [35]. Although these methods have low complexity in each iteration, they suffer from a slow convergence rate in general. Specifically, the required iterations to attain an ϵ -optimal solution is no less than $\mathcal{O}\left(\frac{1}{\epsilon^2}\right)$. To address these issues, we further propose a computationally efficient algorithm with a fast convergence rate to solve the problems in (24) and (27).

VI. MIRROR-PROX METHOD FOR SOLVING PROBLEMS (24) AND (27)

In this section, we transform the problems in (24) and (27) to convex-concave saddle point problems and apply the Mirror-Prox method [36] to solve the resulting problems more efficiently.

A. Mirror-Prox Method for Problems (24) and (27)

First, we can transform the non-smooth max-min problem in (24) into the following equivalent smooth min-max problem by using the primal-dual transformation [37]

$$\min_{\tilde{\boldsymbol{v}}} \max_{\boldsymbol{y}} \psi^{(i)}(\tilde{\boldsymbol{v}}, \boldsymbol{y}) \stackrel{\Delta}{=} \left(\bar{\boldsymbol{\tau}}^{(i)} \|\tilde{\boldsymbol{v}}\|_{2}^{2} + \mathbf{P}^{(i)} \tilde{\boldsymbol{v}} + \mathbf{q}^{(i)}\right)^{\mathsf{T}} \boldsymbol{y}$$

s.t. $\overline{\text{C2}}, \text{C10:} y_{k} \ge 0, \sum_{k=1}^{K} y_{k} = 1, \boldsymbol{y} \in \mathbb{R}^{K \times 1},$ (30)

where $\bar{\boldsymbol{\tau}}^{(i)} = \frac{1}{2} [\bar{L}_1^{(i)}, \bar{L}_1^{(i)} \cdots, \bar{L}_K^{(i)}]^{\mathsf{T}}$ and the objective function $\psi^{(i)}(\tilde{\boldsymbol{v}}, \boldsymbol{y})$ is convex in $\tilde{\boldsymbol{v}}$ and concave in \boldsymbol{y} . Then, the optimal solution $\tilde{\boldsymbol{v}}_{\text{opt}}$ and $\boldsymbol{y}_{\text{opt}}$ corresponds to the saddle point of objective function $\psi^{(i)}(\tilde{\boldsymbol{v}}, \boldsymbol{y})$ [38]. By defining $\boldsymbol{z} = [\tilde{\boldsymbol{v}}^{\mathsf{T}}, \boldsymbol{y}^{\mathsf{T}}]^{\mathsf{T}}$ and $\Psi^{(i)}(\boldsymbol{z}) = [\nabla_{\tilde{\boldsymbol{v}}}\psi^{(i)}(\tilde{\boldsymbol{v}})^{\mathsf{T}}, -\nabla_{\tilde{\boldsymbol{v}}}\psi^{(i)}(\boldsymbol{y})^{\mathsf{T}}]^{\mathsf{T}}$, the problem (30) is equivalent to solve the following variational inequality problem

Find
$$\boldsymbol{z}_{opt}$$

s.t. $\Psi^{(i)}(\boldsymbol{z}_{opt})^{\mathsf{T}}(\boldsymbol{z} - \boldsymbol{z}_{opt}) \ge 0.$ (31)

By analyzing the saddle-point operator $\Psi^{(i)}(z)$, we have the following Lemma.

Lemma 7. The operator $\Psi^{(i)}(\boldsymbol{z})$ is monotone and L_v -Lipschitz continuous, where the Lipschitz parameter is $L_v = 2\sqrt{N} \|\bar{\boldsymbol{\tau}}^{(i)}\|_2 + \max_k \|\mathbf{p}_k^{(i)}\|_2$.

Proof: See Appendix C

Now, we apply the Mirror-Prox method to solve the Problem (31). The Mirror-Prox method solves the variational inequality problem optimally with $\mathcal{O}(\frac{1}{\epsilon})$ convergence rate. We now briefly outline the Mirror-Prox method and the details of this algorithm could be found in [36].

Algorithm 2 Mirror-Prox Method for Solving the Convexconcave Saddle Point Problem (24).

Require: Threshold ϵ , stepsize $\alpha = \frac{1}{2L}$, and operator $\Psi^{(i)}(\cdot);$ 1: Set: l = 0; 2: Initial: $\boldsymbol{z}_0 = [\tilde{\boldsymbol{v}}_0^{\mathsf{T}}, \boldsymbol{y}_0^{\mathsf{T}}]^{\mathsf{T}};$ 3: repeat $\nabla \phi(\mathbf{r}_{l+1}') = \nabla \phi(\mathbf{z}_l) - \alpha \Psi^{(i)}(\mathbf{z}_l),$ 4: $\boldsymbol{r}_{l+1}^{'} = \nabla \phi^{-1} (\nabla \phi(\boldsymbol{z}_l) - \alpha \Psi^{(i)}(\boldsymbol{z}_l)),$ 5:
$$\begin{split} & r_{l+1} = \arg \min_{\tilde{\boldsymbol{z}}} D_{\phi}(\boldsymbol{z}, \boldsymbol{r}_{l+1}^{'}), \\ & \nabla \phi(\boldsymbol{z}_{l+1}^{'}) = \nabla \phi(\boldsymbol{z}_{l}) - \alpha \Psi^{(i)}(\boldsymbol{r}_{l+1}), \\ & \boldsymbol{z}_{l+1}^{'} = \nabla \phi^{-1} (\nabla \phi(\boldsymbol{z}_{l}) - \alpha \Psi^{(i)}(\boldsymbol{r}_{l+1})), \end{split}$$
6: 7: 8: $\boldsymbol{z}_{l+1} = \arg\min_{\tilde{\boldsymbol{z}}} D_{\phi}(\boldsymbol{z}, \boldsymbol{z}_{l+1}');$ 9: Set: $l \leftarrow l + 1$; 10: 11: **until** $D(\boldsymbol{z}_l, \boldsymbol{z}_{l+1}) \leq \varepsilon$; 12: Set: $\boldsymbol{z}_{opt} \leftarrow \frac{1}{L} \sum_{l=1}^{L} \boldsymbol{z}_l$.

The Mirror-Prox algorithm is a variant of the mirror descent algorithm [37], [39]. By denoting $\alpha = 1/(2L_v)$, the overall Mirror-Prox algorithm is comprosed of two iterations of Mirror Descent. As shown in Algorithm 2, steps 4-6 correspond to the first mirror descent step, which starts from \tilde{z}_l to r_{l+1} . Then, steps 7-9 follow the similar procedures and start from \tilde{z}_l to \tilde{z}_{l+1} , using an operator evaluation at r_{l+1} . In each mirror descent, the projection is done by the Bregman distance $D_{\phi}(z, z')$, which is to monitor the local geometry of the constraints to improve the algorithm performance [40]. The Bregman distance is defined as

$$D_{\phi}(\boldsymbol{z}, \boldsymbol{z}') = \phi(\boldsymbol{z}) - \phi(\boldsymbol{z}') - \nabla \phi(\boldsymbol{z}')^{\mathsf{T}}(\boldsymbol{z} - \boldsymbol{z}'), \quad (32)$$

where $\phi(z)$ is the mapping function. According to the structure of $\overline{C2}$ and C10, we select the mapping function as $\phi(z) = \frac{1}{2} \|\tilde{v}\|^2 + \sum_{k=1}^{K} y_k \ln y_k$ [41], where the first

term is the mirror map for the Euclidean space $\overline{C2}$, and the second term denotes the mirror map for the simplex space C10. Thus the $\nabla \phi(\boldsymbol{z})$ and $\nabla^{-1} \phi(\boldsymbol{z})$ is expressed as $\nabla \phi(\boldsymbol{z}) = [\tilde{\boldsymbol{v}}, \ln y_1 + 1, \cdots, \ln y_K + 1]^{\mathsf{T}}$, and $\nabla^{-1} \phi(\tilde{\boldsymbol{z}}) = [\tilde{\boldsymbol{v}}, \exp(y_1 - 1), \cdots, \exp(y_K - 1)]^{\mathsf{T}}$. Hence, the Bregman distance in (32) can be expressed as

$$D_{\phi}(\boldsymbol{z}, \boldsymbol{z}') = \frac{1}{2} \|\tilde{\boldsymbol{v}} - \tilde{\boldsymbol{v}}'\|^{2} + \sum_{k=1}^{K} y_{k} \ln \frac{y_{k}}{y_{k}'} - \sum_{k=1}^{K} (y_{k} - y_{k}').$$
(33)

Based on (33), the non-Euclidean projection problem in step 6 can be solved by minimizing the first term in (33) with respect to \tilde{v} and the others terms in (33) with respect to y separately. Specifically, the closed-form solution of \tilde{v} to the problem in step 6 is expressed as

$$\tilde{v}_{i} = \begin{cases} \frac{\tilde{v}_{i}'}{\left(\left(v_{i}'\right)^{2} + \left(\tilde{v}_{N+i}'\right)^{2}\right)^{\frac{1}{2}}}, & u_{i}^{2} + u_{N+i}^{2} \ge 1, \\ \tilde{v}_{i}', & \text{otherwise,} \end{cases}$$
(34)

and the optimal solution of y is $y_{opt} = \frac{y'}{\|y'\|_1}$ [42]. The above implementation details can be applied to steps 7-9 in Algorithm 2 directly.

Similarly to the above steps that tackle the problem in (24), we can apply Algorithm 2 to tackle the problem in (27) by replacing $\mathbf{M}_{k}^{(i)}$, $\boldsymbol{p}_{k}^{(i)}$, and $q_{k}^{(i)}$ with $\mathbf{L}_{k}^{(i)}$, $\boldsymbol{a}_{k}^{(i)}$, and $b_{k}^{(i)}$, respectively.

B. Computational Complexity

For Algorithm 2, the mirror projections are all closed-form operations. The computation cost to solve problem (24) is dominated by the computation of $\Psi^{(i)}(\cdot)$, where the complexity is $\mathcal{O}(NK)$. Also, the complexity to tackle problem (27) is $\mathcal{O}(MK)$. In Sec. VII, we will present the specific running time comparison to verify the effectiveness of our proposed algorithm.

VII. SIMULATION RESULTS

In this section, we provide simulation results to illustrate the PKG performance of the proposed method and the impact of spatial correlation on KGR.

A. Simulation Settings

We consider a three-dimensional coordinate system where the central point of Alice, Bob, and RIS are located at (5 m, 0 m, 20 m), (3 m, 100 m, 0 m), and (0 m, 60 m, 2 m), respectively [16]. We assume that Alice is equipped with a UPA located in x - z plane, and the RIS is equipped with a uniform rectangular array (URA) located in y - z plane. The UPA at the BS has $N_{\rm H}^t = 5$ antennas per row and $N_{\rm V}^t = M/5$ antennas per column. The RIS has $N_{\rm H}^r = 5$ elements per row and $N_{\rm V}^r = N/5$ elements per column. The antennas of Eve are randomly distributed within a circle of radius R centered at Bob and the channel correlation coefficient is $\rho_k = [J_0(2\pi d/\lambda)]^2$, where d is the distance and J_0 is the first-kind of Bessel function [16]. The channel between Alice and Bob is generated by (3) and the large-scale path loss



Fig. 2. Convergence behavior of the BSUM algorithm under different N when $P_{\rm A} = P_{\rm B} = 20$ dBm, M = 15, $\rho = 0.3$, the spacing of two neighbouring RIS elements is $\lambda/4$, and K = 10.

 $\beta_{ba} = \sqrt{\zeta_0 d_{ba}^{-\alpha_{ba}}}$, where d_{ba} , ζ_0 , and α_{ba} are the distance, path loss at 1 m, and the path loss exponent, respectively. The simulation settings are $\alpha_{ba} = \alpha_{e_k a} = 4$, $\alpha_{ar} = 3.5$, $\alpha_{br} = \alpha_{e_k r} = 2$, $\zeta_0 = -30$ dB, $\sigma^2 = -80$ dBm, and $\epsilon = 10^{-4}$ [16]. The results in the following subsections were averaged over 1000 random channel realizations.

B. Convergence of the Proposed Algorithms

First, we evaluate the convergence behavior of the proposed BSUM with Mirror-Prox algorithm. Fig. 2 depicts the average minimum KGR versus the number of iterations for various RIS elements, i.e., for N = 20, 40, and 60. It can be observed that having more RIS elements leads to a slightly slower convergence speed. As more optimization variables are involved, the more iterations are required for convergence due to the enlarged solution space. However, for different values of N, the proposed algorithm converges within 15 iterations on average, which illustrates the practicality of the proposed algorithm.

C. KGR versus the Transmit Power

In Fig. 3, the average minimum KGR versus the transmit power under different algorithms and channel assumptions is plotted. First, it can be observed that the KGR at all the settings increases with the transmit power, since the negative impacts of noises in the channel estimation and key generation are reduced. For comparison, some benchmarks are provided: (1) the ASSG algorithm based on different channel models; (2) the case without RIS. It is noted that the proposed design outperforms these benchmarks. In particular, the BSUM with Mirror-Prox and ASSG algorithms under correlated channel model assumption lead to a higher KGR than the benchmarks under i.i.d. channel model assumptions. Specifically, when $P \ge 30$ dBm, the proposed setting achieves about 5 dB and 6 dB transmit power gain compared to the beamforming scheme under the i.i.d. channel assumption and the optimal transmit beamforming without RIS, respectively. This is because when



Fig. 3. Average minimum KGR achieved by different algorithms with different channel assumptions when $P_{\rm A} = P_{\rm B} = P$, N = 60, M = 15, K = 5, $\rho = 0.2$, and the spacing of two neighbouring RIS elements is $\lambda/4$.

correlations exist between the BS antennas and the RIS elements, the i.i.d. model fails in capturing this important characteristic which degrades the KGR performance. In contrast, the proposed scheme can effectively exploit the properties of the channels to perform a more precise beamforming. It can also be observed that the beamforming design under the i.i.d. assumption at the RIS achieves a higher KGR gain than that under the i.i.d. assumption at the BS. This is because when $\rho = 0.2$ and the neighbouring RIS element spacing is $\lambda/4$, having the optimal w is more effective than that of v in combating the noises in R_k . Finally, we observe that in spatially correlated channels, the BSUM with Mirror-Prox algorithm and ASSG algorithm achieve almost the same KGR under different transmit powers, since both algorithms guarantee to converge to a stationary point. However, Gaussian randomization is applied in ASSG algorithm to obtain a rank-1 solution, which results in slight KGR degradation on average.

D. Computation Time Comparision

In Fig. 4, we present the ratio of the average computation time of the BSUM algorithm to that of the ASSG algorithm. As can be observed, the BSUM with Mirror-Prox algorithm consumes much shorter computation time than the ASSG algorithm and the ratio decreases as the number of the BS antennas or the RIS elements increases. This is because the dimension of the optimization variable is the square of the BS antennas, i.e., M^2 or N^2 , in the ASSG algorithm, while the BSUM algorithm optimizes the M or N-dimensional vector directly. The above results verify the computational effectiveness of the proposed algorithm.

E. The Impact of RIS Elements Number and Size

Fig. 5 shows the KGR of different RIS neighbour elements spacing versus the number of RIS elements adopting the proposed algorithm. As can be observed, the KGR of all of these cases increases with the number of RIS elements. This is because with more RIS elements in place, the proposed



Fig. 4. Ratio of the average computation time of the BSUM algorithm to the ASSG algorithm when $P_{\rm A} = P_{\rm B} = 20$ dBm, K = 4, the spacing of two neighbouring RIS elements is $\lambda/2$, and $\rho = 0.3$.



Fig. 5. Average KGR achieved for different N when $P_{\rm A}=30$ dBm, $P_{\rm B}=20$ dBm, M=15,~K=5, and $\rho=0.2.$

design becomes more flexible to create pencil-like energy focusing beams at the RIS to realize better KGR performance. In addition, it is noted that with the RIS elements spacing becoming smaller, the minimum KGR increases significantly. The reason behind this is that with smaller elements spacing, the values of the spatial correlation R_I are larger, e.g., (18), contributing to a higher KGR. Finally, it is found that even with $\lambda/2$ RIS element spacing, the KGR of the proposed method is still slightly superior than that adopting the i.i.d. channel assumption. In fact, the correlation among the RIS elements is weak in $\lambda/2$ spacing, although it always exists if $N_{\rm H}^r > 1$ or $N_{\rm V}^r > 1$, which can be exploited by the proposed method.

F. The Impact of BS Antennas Number and Correlation

Fig. 6 shows the KGR versus the number of the antennas at the BS. The beamforming vectors are optimized by the proposed BSUM with Mirror-Prox algorithm. As can be observed, the KGR of the design method based on the i.i.d. fading model is identical to that of the proposed design when



Fig. 6. Average KGR versus different M when $P_{\rm A} = 30$ dBm, $P_{\rm B} = 20$ dBm, K = 5, and the spacing of two neighbouring RIS elements is $\lambda/2$.



Fig. 7. Comparison of the average minimum KGR for different channel assumptions versus the Eve's distribution radius R when $P_{\rm A} = P_{\rm B} = 30$ dBm, N = 60, M = 20, $\rho = 0.4$, and the spacing of two neighbouring RIS elements is $\lambda/4$.

 $\rho = 0$, which is independent of the antenna numbers at the BS. For the cases of $\rho > 0$, the proposed method can always achieve higher KGR gain, since the upper and lower bounds of the KGR both increase with the spatial correlation between antennas. Moreover, with the number of antennas increases, the KGR increases with diminishing returns. This is due to channel hardening [18] and the limited transmit power at the BS. Indeed, the greater correlation coefficient ρ contributes to higher converged value, which is consistent with Lemma 4.

G. The Impact of Eve Antennas Number and Location

In Fig. 7, the average minimum KGR versus the number and the location of the eavesdropper's antennas is plotted. First, the KGR decreases when there are more antennas for Eve. This is due to the fact that more antennas at Eve create better quality in the eavesdropping channels. In addition, Fig. 7 also reports that the radius of Eve's antennas location, R, has a significant impact on the KGR. With a larger radius of Eve's distribution, the average minimum correlation between Eve's antennas and



Fig. 8. Comparison of the average BDRs for different channel assumptions versus the transmit power P.

Bob decreases, that contributes to higher KGR. Finally, as expected, the KGR of the proposed algorithm outperforms those benchmarks that adopt the i.i.d. channel assumption at the BS or the RIS. The results above verify the effectiveness of the proposed method under different eavesdropping conditions.

H. BDR Comparison and Randomness Evaluation

After the channel probing stage, Alice and Bob quantize their combined channel gains into raw key bits. The bit disagreement ratio (BDR) denotes the ratio of the number of disagreements bits to the number of total quantized bits. When the BDR becomes higher, the legitimate ends have to consume larger signaling overhead to correct these inconsistent bits. Fig. 8 presents the BDR performance under different channel assumptions using the proposed algorithm and the 1-bit Cumulative Distribution Function (CDF)-based quantization method [43] under 10^6 times channel probings. As shown in Fig. 8, the algorithm that designed under the spatially correlated channel model achieves lower BDR than that under the benchmarks. Indeed, the optimized beamforming design improves the ratio of the power of the combined reciprocal component to the noise. Finally, we conduct the National

TABLE I NIST random test result

	Pass ratio	P-value
Approximate entropy	0.9833	0.4862
Runs	0.9893	0.4979
Ranking	0.9901	0.4959
Longest runs of ones	0.9899	0.4959
Frequency	0.9900	0.5047
FFT	0.9853	0.4825
Block frequency	0.9887	0.5013
Cumulative sums	0.9908	0.5197
Serial	0.9901	0.5275, 0.4917

Institute of Standards and Technology (NIST) randomness test [44] on the quantized bits to verify the randomness of the obtained bit sequences for cryptographic applications. The output of the NIST is called p-value and the tested bits pass the NIST test if the p-value is greater than the threshold 0.01. In the simulation, we perform 9 kinds of NIST tests for 10,000 trials. The test results are shown in Table I, where the pass ratio denotes the ratio of the number of passed trials to the number of all trials. From this table, the pass ratio of 9 NIST tests is higher than 0.9 and the average p-value is greater than 0.01. These results indicate the excellent randomness of the bits generated by the proposed method.

VIII. CONCLUSION

In this paper, we introduced a transmit and reflective beamforming-based RIS-assisted PKG framework in multiantenna spatially correlated channels. Based on this framework, we derived the general closed-form KGR expression and formulated an optimization problem to maximize the minimum KGR. We designed a BSUM with a Mirror-Prox algorithm to tackle the non-convex optimization problem. Our analysis proved that the KGR increases with the spatial correlation between the BS antennas and RIS elements. In particular, the KGR can be improved significantly with the increase of RIS elements, while it increases with diminishing returns when the number of BS antennas is sufficiently large. Numerical results showed that our method achieves higher KGR and lower BDR compared to the benchmarks in the same eavesdropping condition.

APPENDIX

A. Proof of Lemma 1

First, we calculate the covariance of channel estimation \hat{h}_a as

$$\mathcal{R}_{aa} = P_{\mathrm{B}} \boldsymbol{w}^{\mathsf{T}} \mathbb{E} \{ \boldsymbol{G}_{ar} \boldsymbol{\Phi} \boldsymbol{h}_{rb} \boldsymbol{h}_{rb}^{\mathsf{H}} \boldsymbol{\Phi}^{\mathsf{H}} \boldsymbol{G}_{ar}^{\mathsf{H}} \} \boldsymbol{w}^{*} + P_{\mathrm{B}} \boldsymbol{w}^{\mathsf{T}} \mathbb{E} \{ \boldsymbol{h}_{ab} \boldsymbol{h}_{ab}^{\mathsf{H}} \} \boldsymbol{w}^{*} + || \boldsymbol{w} ||_{2}^{2} \sigma_{a}^{2}.$$
(35)

By exploting the channel correlations in (1)–(3), the first term in (35) is given by

$$\mathbb{E}\{\boldsymbol{G}_{ar}\boldsymbol{\Phi}\boldsymbol{h}_{rb}\boldsymbol{h}_{rb}^{\mathsf{H}}\boldsymbol{\Phi}^{\mathsf{H}}\boldsymbol{G}_{ar}^{\mathsf{H}}\}$$
(36)
= $\beta_{r}\boldsymbol{R}_{S}\mathbb{E}\{\operatorname{vec}\{\tilde{\boldsymbol{h}}_{rb}^{\mathsf{H}}\boldsymbol{R}_{I}^{\frac{1}{2}}\boldsymbol{\Phi}^{\mathsf{H}}\boldsymbol{R}_{I}^{\frac{1}{2}}\}^{\mathsf{H}}\operatorname{vec}\{\tilde{\boldsymbol{h}}_{rb}^{\mathsf{H}}\boldsymbol{R}_{I}^{\frac{1}{2}}\boldsymbol{\Phi}^{\mathsf{H}}\boldsymbol{R}_{I}^{\frac{1}{2}}\}\}$ (37)

$$\stackrel{(a)}{=} \beta_{r} \boldsymbol{R}_{S} \mathbb{E} \{ \boldsymbol{v}^{\mathsf{H}} ((\boldsymbol{R}_{I}^{\frac{1}{2}})^{\mathsf{T}} \odot (\boldsymbol{R}_{I}^{\frac{1}{2}}))^{\mathsf{H}} (\tilde{\boldsymbol{h}}_{rb}^{*} \otimes \boldsymbol{I}_{N}) \\ \times (\tilde{\boldsymbol{h}}_{rb}^{\mathsf{T}} \otimes \boldsymbol{I}_{N}) ((\boldsymbol{R}_{I}^{\frac{1}{2}})^{\mathsf{T}} \odot (\boldsymbol{R}_{I}^{\frac{1}{2}})) \boldsymbol{v} \}$$
(38)

$$=\beta_{r}\boldsymbol{R}_{S}\boldsymbol{v}^{\mathsf{H}}((\boldsymbol{R}_{I}^{\frac{1}{2}})^{\mathsf{T}}\odot(\boldsymbol{R}_{I}^{\frac{1}{2}}))^{\mathsf{H}}((\boldsymbol{R}_{I}^{\frac{1}{2}})^{\mathsf{T}}\odot(\boldsymbol{R}_{I}^{\frac{1}{2}}))\boldsymbol{v}$$
$$=\beta_{r}\boldsymbol{R}_{s}\boldsymbol{v}^{\mathsf{H}}(\boldsymbol{R}_{I}^{\mathsf{T}}\circ\boldsymbol{R}_{I})\boldsymbol{v}=\beta_{r}\boldsymbol{R}_{S}\boldsymbol{v}^{\mathsf{H}}\tilde{\boldsymbol{R}}_{I}\boldsymbol{v}.$$
(39)

(a) follows from $vec(ABC) = (C^T \otimes A)vec(B)$ and $vec(Adiag(d)C) = (C^T \odot A)d$. Then, the second term of the

right-hand side of (35) is calculated as $\mathbb{E}\{h_{ab}h_{ab}^{H}\} = \beta_{ab}R_{S}$. Similarly, we have

$$\mathcal{R}_{bb} = \beta_r \boldsymbol{w}^\mathsf{T} \boldsymbol{R}_S \boldsymbol{w}^* \boldsymbol{v}^\mathsf{H} \tilde{\boldsymbol{R}}_I \boldsymbol{v} + \beta_{ab} \boldsymbol{w}^\mathsf{T} \boldsymbol{R}_S \boldsymbol{w}^* + \sigma_b^2, \quad (40)$$
$$\mathcal{R}_{ab} = \sqrt{P_{\mathrm{B}}} \beta_r \boldsymbol{w}^\mathsf{T} \boldsymbol{R}_S \boldsymbol{w}^* \boldsymbol{v}^\mathsf{H} \tilde{\boldsymbol{R}}_I \boldsymbol{v} + \sqrt{P_{\mathrm{B}}} \beta_{ab} \boldsymbol{w}^\mathsf{T} \boldsymbol{R}_S \boldsymbol{w}^*$$

$$= \mathcal{R}_{ba}, \qquad (41)$$
$$\mathcal{R}_{e_k e_k} = \beta_r^k \boldsymbol{w}^\mathsf{T} \boldsymbol{R}_S \boldsymbol{w}^* \boldsymbol{v}^\mathsf{H} \tilde{\boldsymbol{R}}_I \boldsymbol{v} + \beta_{ak} \boldsymbol{w}^\mathsf{T} \boldsymbol{R}_S \boldsymbol{w}^* + \sigma_{e_k}^2, \quad (42)$$

$$\begin{aligned} \mathcal{R}_{be_k} &= \sqrt{\beta_r \beta_r^k} \boldsymbol{v}^{\mathsf{H}} \left[((\boldsymbol{R}_I^{\frac{1}{2}})^{\mathsf{T}} \boldsymbol{R}_k^r (\boldsymbol{R}_I^{\frac{1}{2}})^{\mathsf{T}}) \circ \boldsymbol{R}_I \right] \boldsymbol{v} \boldsymbol{w}^{\mathsf{T}} \boldsymbol{R}_S \boldsymbol{w}^* \\ &+ \sqrt{\beta_{ab} \beta_{ak}} \boldsymbol{w}^{\mathsf{T}} \boldsymbol{R}_S^{\frac{1}{2}} \boldsymbol{R}_k^d \boldsymbol{R}_S^{\frac{1}{2}} \boldsymbol{w}^* \end{aligned}$$

$$= \mathcal{R}_{e_k b}^{\mathsf{H}} = \mathcal{R}_{a e_k} / \sqrt{P_{\mathsf{B}}} = \mathcal{R}_{e_k a}^{\mathsf{H}} / \sqrt{P_{\mathsf{B}}}.$$
 (43)

Then, we can calculate the two determinants in (11) and obtain the KGR as (14).

B. Proof of Lemma 6

We denote the objective value of Problem (20) as $\varphi(\tilde{w}, \tilde{v}) =$ $\min_k f_k(\tilde{w}, \tilde{v})$. By denoting the objective value of the subproblem in (24) and the subproblem in (27) as $\bar{\varphi}(\tilde{w}, \tilde{v})$ and $\tilde{\varphi}(\tilde{\boldsymbol{w}}, \tilde{\boldsymbol{v}})$, respectively, we have $\varphi(\tilde{\boldsymbol{w}}^{(i+1)}, \tilde{\boldsymbol{v}}^{(i+1)}) \stackrel{(b)}{\geq}$ $\bar{\varphi}(\tilde{\boldsymbol{w}}^{(i+1)}, \tilde{\boldsymbol{v}}^{(i+1)}) \stackrel{(c)}{=} \tilde{\varphi}(\tilde{\boldsymbol{w}}^{(i+1)}, \tilde{\boldsymbol{v}}^{(i+1)}) \stackrel{(d)}{\geq} \tilde{\varphi}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i+1)}),$ where inequality (b) holds because $\bar{\varphi}(\tilde{w}, \tilde{v})$ is a lower bound of $\varphi(\tilde{w}, \tilde{v})$, inequality (c) holds since $\tilde{\varphi}(\tilde{w}, \tilde{v})$ is a local approximation of $\bar{\varphi}(\tilde{w}, \tilde{v})$ at the point $(\tilde{w}^{(i+1)}, \tilde{v}^{(i+1)})$. The inequality (d) holds since $\tilde{\boldsymbol{w}}^{(i+1)} = \arg \max_{\tilde{\boldsymbol{w}}} \tilde{\varphi}(\tilde{\boldsymbol{w}}, \tilde{\boldsymbol{v}}^{(i+1)}).$ Similarly, we have $\tilde{\varphi}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i+1)}) \stackrel{(e)}{\geq} \tilde{\varphi}(\tilde{\boldsymbol{w}}^{(i)}, \tilde{\boldsymbol{v}}^{(i+1)}) \stackrel{(f)}{\geq}$ $ar{arphi}(ilde{m{w}}^{(i)}, ilde{m{v}}^{(i)}) \stackrel{(g)}{=} arphi(ilde{m{w}}^{(i)}, ilde{m{v}}^{(i)}), ext{ where } (e) ext{ holds since }$ $\bar{\varphi}(\tilde{w}, \tilde{v}^{(i+1)})$ is an lower bound of $\tilde{\varphi}(\tilde{w}, \tilde{v}^{(i+1)})$, (f) holds because $\tilde{v}^{(i+1)} = \arg \max_{\tilde{v}} \bar{\varphi}(\tilde{w}^{(i)}, \tilde{v})$, and (q) holds since $\bar{\varphi}(\tilde{\boldsymbol{w}}, \tilde{\boldsymbol{v}})$ is a local approximation of $\varphi(\tilde{\boldsymbol{w}}, \tilde{\boldsymbol{v}})$ at the point $(\tilde{w}^{(i)}, \tilde{v}^{(i)})$. Therefore, we have proved the equality $\varphi(\tilde{w}^{(i+1)}, \tilde{v}^{(i+1)}) \geq \varphi(\tilde{w}^{(i)}, \tilde{v}^{(i)})$, i.e., the sequence $\{\varphi(ilde{w}^{(i)}, ilde{v}^{(i)})\}_{i=0}^\infty$ is non-increasing over iterations. In addition, assuming the channel gain is finite and the transmit power $P_{\rm A}$ and $P_{\rm B}$ is limited, the solution set is compact and the KGR has an upper bound. Consequently, the objective values of Problem (20) are non-increasing and convergence.

C. Proof of Lemma 7

According to [36], the function $\Psi^{(i)}(\cdot)$ is monotone and Lipschitz continuous. Then, $\Psi^{(i)}(\cdot)$ is defined as *L*-Lipschitz if it satisfies with the following constraints [39]

$$\left\|\nabla_{\tilde{\boldsymbol{v}}}\psi^{(i)}(\tilde{\boldsymbol{v}},\boldsymbol{y}) - \nabla_{\tilde{\boldsymbol{v}}}\psi^{(i)}(\tilde{\boldsymbol{v}}',\boldsymbol{y})\right\|_{2} \le L \left\|\tilde{\boldsymbol{v}} - \tilde{\boldsymbol{v}}'\right\|_{2}, \quad (44)$$

$$\left\| \nabla_{\boldsymbol{y}} \psi^{(i)}(\tilde{\boldsymbol{v}}, \boldsymbol{y}) - \nabla_{\boldsymbol{y}} \psi^{(i)}(\tilde{\boldsymbol{v}}, \boldsymbol{y}') \right\|_{\infty} \le L \left\| \boldsymbol{y} - \boldsymbol{y}' \right\|_{1}, \quad (45)$$

$$\left\|\nabla_{\tilde{\boldsymbol{v}}}\psi^{(i)}(\tilde{\boldsymbol{v}},\boldsymbol{y}) - \nabla_{\tilde{\boldsymbol{v}}}\psi^{(i)}_{(t)}(\tilde{\boldsymbol{v}},\boldsymbol{y}')\right\|_{2} \le L \left\|\boldsymbol{y} - \boldsymbol{y}'\right\|_{1}, \quad (46)$$

$$\left\|\nabla_{\boldsymbol{y}}\psi^{(i)}(\tilde{\boldsymbol{v}},\boldsymbol{y}) - \nabla_{\boldsymbol{y}}\psi^{(i)}(\tilde{\boldsymbol{v}}',\boldsymbol{y})\right\|_{\infty} \leq L \left\|\tilde{\boldsymbol{v}} - \tilde{\boldsymbol{v}}'\right\|_{2}.$$
 (47)

First, the equality in (44) holds because $\|\nabla_{\tilde{\boldsymbol{v}}}\psi^{(i)}(\tilde{\boldsymbol{v}},\boldsymbol{y}) - \nabla_{\tilde{\boldsymbol{v}}}\psi^{(i)}(\tilde{\boldsymbol{v}}',\boldsymbol{y})\|_2 \leq \|2(\bar{\boldsymbol{\tau}}^{(i)})^{\mathsf{T}}\boldsymbol{y}\|_2\|\tilde{\boldsymbol{v}} - \tilde{\boldsymbol{v}}'\|_2 \leq L\|\tilde{\boldsymbol{v}} - \tilde{\boldsymbol{v}}'\|_2$, which follows the Cauchy-Schwarz inequality. Then, the equality in (45) holds since

 $\nabla_{\boldsymbol{y}}\psi^{(i)}(\tilde{\boldsymbol{v}},\boldsymbol{y}) = \nabla_{\boldsymbol{y}}\psi^{(i)}(\tilde{\boldsymbol{v}},\boldsymbol{y}') = \bar{\boldsymbol{\tau}}^{(i)}\tilde{\boldsymbol{v}}^{\top}\tilde{\boldsymbol{v}} + \mathbf{P}^{(i)}\tilde{\boldsymbol{v}} + \mathbf{q}^{(i)},$ which is irrelevant to the variable \boldsymbol{y} . In addition, the inequality in (46) holds due to

$$\left\|\nabla_{\tilde{\boldsymbol{v}}}\psi^{(i)}(\tilde{\boldsymbol{v}},\boldsymbol{y}) - \nabla_{\tilde{\boldsymbol{v}}}\psi^{(i)}(\tilde{\boldsymbol{v}},\boldsymbol{y}')\right\|_{2}$$
(48)

$$\leq 2 \|(\bar{\boldsymbol{\tau}}^{(i)})^{\mathsf{T}} \boldsymbol{y} - (\bar{\boldsymbol{\tau}}^{(i)})^{\mathsf{T}} \boldsymbol{y}'\|_{2} \|\tilde{\boldsymbol{v}}\|_{2} + \|\mathbf{P}^{\mathsf{T}} \boldsymbol{y} - \mathbf{P}^{\mathsf{T}} \boldsymbol{y}'\|_{2} \quad (49)$$

$$\leq 2 \left(\| \bar{\boldsymbol{\tau}}^{(i)} \|_2 \sqrt{N} + \left(\max_k \| \mathbf{p}_k^{(i)} \|_2 \right) \right) \| \boldsymbol{y} - \boldsymbol{y}' \|_1$$
(50)
= $L \| \boldsymbol{y} - \boldsymbol{y}' \|_1,$ (51)

where (49) follows the triangle inequality. At last, the inequality (47) holds as

$$\leq \left(\|\bar{\boldsymbol{\tau}}^{(i)}\|_{2}(\|\tilde{\boldsymbol{v}}\|_{\infty} + \|\tilde{\boldsymbol{v}}'\|_{\infty}) + \max_{k} \left\{\|(\mathbf{p}_{k}^{(i)})\|_{2}\right\}\right) \|(\tilde{\boldsymbol{v}} - \tilde{\boldsymbol{v}}')\|_{2}$$
(54)

$$= L \| (\tilde{\boldsymbol{v}} - \tilde{\boldsymbol{v}}') \|_2. \tag{55}$$

REFERENCES

- [1] L. Hu, G. Li, X. Qian, D. W. K. Ng, and A. Hu, "Joint transmit and reflective beamforming for RIS-assisted secret key generation," *accepted by IEEE Glob. Commun. Conf.(GLOBECOM)*, vol. abs/2207.11752, pp. 1–6, 2022. [Online]. Available: http://arxiv.org/abs/2207.11752
- [2] M. Ylianttila, R. Kantola, A. V. Gurtov, and et al., "6G white paper: Research challenges for trust, security and privacy," *CoRR*, vol. abs/2004.11665, 2020. [Online]. Available: https://arxiv.org/abs/2004. 11665
- [3] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," *IEEE Wireless Commun. Mag.*, vol. 26, no. 5, pp. 48–54, Oct. 2019.
- [4] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
- [5] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, no. 3, pp. 614– 626, Jan. 2017.
- [6] S. Mathur, W. Trappe, N. Mandayam, and et al., "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in Proc. 14th Annu. Int. Conf. Mobile Computing and Networking (MobiCom), San Francisco, California, USA, Sept. 2008, pp. 128–139.
- [7] G. Li, A. Hu, J. Zhang, and et al., "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022–3034, Mar. 2018.
- [8] G. Li, Z. Zhang, J. Zhang, and A. Hu, "Encrypting wireless communications on the fly using one-time pad and key generation," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 357–369, Jun. 2021.
- [9] G. Li, L. Hu, P. Staat, H. Elders-Boll, C. Zenger, C. Paar, and A. Hu, "Reconfigurable intelligent surface for physical layer key generation: Constructive or destructive?" *IEEE Wireless Commun. Mag.*, pp. 1–12, May 2022.
- [10] H. Zhou, L. M. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 476–488, Jan. 2014.
- [11] R. Guillaume, S. Ludwig, A. Muller, and A. Czylwik, "Secret key generation from static channels with untrusted relays," in *Proc. IEEE WiMob*, Abu Dhabi, United Arab Emirates, Oct. 2015, pp. 1–8.
- [12] X. Yu, D. Xu, D. W. K. Ng, and R. Schober, "IRS-assisted green communication systems: Provable convergence and robust optimization," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 6313–6329, Sept. 2021.
- [13] M. Di Renzo, M. Debbah, D. T. Phan-Huy, and et al., "Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come," *EURASIP J Wirel Commun Netw*, vol. 129, no. 2019, pp. 1–20, May 2019.

- [14] X. Yu, V. Jamali, D. Xu, D. W. K. Ng, and R. Schober, "Smart and reconfigurable wireless communications: From IRS modeling to algorithm design," *IEEE Wireless Commun. Mag.*, vol. 28, no. 6, pp. 118–125, Dec. 2021.
- [15] X. Lu, J. Lei, Y. Shi, and W. Li, "Intelligent reflecting surface assisted secret key generation," *IEEE Signal Process. Lett.*, vol. 28, pp. 1036– 1040, Feb. 2021.
- [16] Z. Ji, P. L. Yeoh, D. Zhang, and et al., "Secret key generation for intelligent reflecting surface assisted wireless communication networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 1030–1034, Dec. 2021.
- [17] G. Li, C. Sun, W. Xu, M. D. Renzo, and A. Hu, "On maximizing the sum secret key rate for reconfigurable intelligent surface-assisted multiuser systems," *IEEE Tran. Inf. Forensics Security*, vol. 17, pp. 211–225, Dec. 2022.
- [18] E. Björnson and L. Sanguinetti, "Rayleigh fading modeling and channel hardening for reconfigurable intelligent surfaces," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 830–834, Apr. 2021.
- [19] H. Yin, L. Cottatellucci, D. Gesbert, R. R. Müller, and G. He, "Robust pilot decontamination based on joint angle and power domain discrimination," *IEEE Trans. Signal Process.*, vol. 64, no. 11, pp. 2990–3003, Feb. 2016.
- [20] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2019.
- [21] G. Yang, H. Zhang, Z. Shi, S. Ma, and H. Wang, "Asymptotic outage analysis of spatially correlated Rayleigh MIMO channels," *IEEE Trans. Broadcast*, vol. 67, no. 1, pp. 263–278, Oct. 2020.
- [22] P. Staat, H. Elders-Boll, M. Heinrichs, R. Kronberger, C. Zenger, and C. Paar, "Intelligent reflecting surface-assisted wireless key generation for low-entropy environments," in *Proc. IEEE Int. Symp. Person. Indoor Mobile Radio Commun. (PIMRC)*, Virtual, Sep. 2021, pp. 1–7.
- [23] G. Li, C. Sun, E. A. Jorswieck, and et al., "Sum secret key rate maximization for TDD multi-user massive MIMO wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 968–982, Sept. 2021.
- [24] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *European Conference on Antennas & Propagation*, Jun. 2009, pp. 1499– 1503.
- [25] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret key generation from reciprocal spatially correlated MIMO channels," in 2013 IEEE Globecom Workshops (GC Wkshps), 2013, pp. 1245–1250.
- [26] T. F. Wong, M. Bloch, and J. M. Shea, "Secret sharing over fast-fading MIMO wiretap channels," *EURASIP J. Wirel. Comm.*, vol. 2009, pp. 1–17, 2009.
- [27] D. Neumann, M. Joham, and W. Utschick, "Covariance matrix estimation in massive MIMO," *IEEE Signal Process. Lett.*, vol. 25, no. 6, pp. 863–867, Apr. 2018.
- [28] Z. Q. Luo, W. K. Ma, M. C. So, and et al., "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, Apr. 2010.
- [29] C. Pan, H. Ren, K. Wang, and et al., "Reconfigurable intelligent surfaces for 6G systems: Principles, applications, and research directions," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 14–20, Jul. 2021.
- [30] J. Choi and D. J. Love, "Bounds on eigenvalues of a spatial correlation matrix," *IEEE Commun. Lett.*, vol. 18, no. 8, Aug. 2014.
- [31] M. Razaviyayn, M. Hong, and Z.-Q. Luo, "A unified convergence analysis of block successive minimization methods for nonsmooth optimization," *SIAM J. Optim.*, vol. 23, no. 2, pp. 1126–1153, 2013.
- [32] Y. Sun, P. Babu, and D. P. Palomar, "Majorization-minimization algorithms in signal processing, communications, and machine learning," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 794–816, Aug. 2017.
- [33] N. Sidiropoulos and T. Davidson, "Broadcasting with channel state information," in *Proc. Workshop, Sensor Array Multichannel Signal*, 2004, pp. 489–493.
- [34] B. T. Polyak, "Introduction to optimization. optimization software," Inc., Publications Division, New York, vol. 1, p. 32, 1987.
- [35] N. Z. Shor, Minimization methods for non-differentiable functions. Springer Science & Business Media, 2012, vol. 3.
- [36] A. Nemirovski, "Prox-method with rate of convergence O(1/t) for variational inequalities with lipschitz continuous monotone operators and smooth convex-concave saddle point problems," *SIAM J. Optim.*, vol. 15, no. 1, pp. 229–251, 2004.
- [37] W. Fang, Y. Jiang, Y. Shi, Y. Zhou, W. Chen, and K. B. Letaief, "Overthe-air computation via reconfigurable intelligent surface," *IEEE Trans. Commun.*, vol. 69, no. 12, pp. 8612–8626, Dec. 2021.
- [38] M. Sion, "On general minimax theorems." Pac. J. Math., vol. 8, no. 1, pp. 171–176, 1958.

- [39] A. Konar and N. D. Sidiropoulos, "Fast approximation algorithms for a class of non-convex QCQP problems using first-order methods," *IEEE Trans. Signal Process.*, vol. 65, no. 13, pp. 3494–3509, Apr. 2017.
- [40] A. S. Nemirovskij and D. B. Yudin, "Problem complexity and method efficiency in optimization," 1983.
- [41] M. S. Ibrahim, A. Konar, M. Hong, and N. D. Sidiropoulos, "Mirror-prox SCA algorithm for multicast beamforming and antenna selection," in 2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), 2018, pp. 1–5.
- [42] S. Bubeck, "Convex optimization: Algorithms and complexity," Found. Trends Mach. Learn., vol. 8, no. 3-4, pp. 231–357, 2015.
- [43] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mob. Comput.*, vol. 9, no. 1, pp. 17–30, May 2010.
- [44] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," DTIC Document, Tech. Rep., 2001.