Machine Learning-Based Secret Key Generation for IRS-assisted Multi-antenna Systems

Chen Chen*, Junqing Zhang*, Tianyu Lu†, Magnus Sandell‡, and Liquan Chen†
* Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom
Emails: c.chen77@liverpool.ac.uk, Junqing.Zhang@liverpool.ac.uk
† School of Cyber Science and Engineering, Southeast University, Nanjing, 210096, China
Emails: effronlu@seu.edu.cn, lqchen@seu.edu.cn
‡ Bristol Research and Innovation Laboratory, Toshiba Research Europe Ltd., Bristol, BS1 4ND, United Kingdom
Email: magnus.sandell@toshiba-bril.com

***Abstract*—Physical-layer key generation (PKG) based on wireless channels is a lightweight technique to establish secure keys between legitimate communication nodes. Recently, intelligent reflecting surfaces (IRSs) have been leveraged to enhance the performance of PKG in terms of secret key rate (SKR), as it can reconfigure the wireless propagation environment and introduce more channel randomness. In this paper, we investigate an IRS-assisted PKG system, taking into account the channel spatial correlation at both the base station (BS) and the IRS. Based on the considered system model, the closed-form expression of SKR is derived analytically. Aiming to maximize the SKR, a joint design problem of the BS's precoding matrix and the IRS's reflecting coefficient vector is formulated. To address this high-dimensional non-convex optimization problem, we propose a novel unsupervised deep neural network (DNN) based algorithm with a simple structure. Different from most previous works that adopt the iterative optimization to solve the problem, the proposed DNN based algorithm directly obtains the BS precoding and IRS phase shifts as the output of the DNN. Simulation results reveal that the proposed DNN-based algorithm outperforms the benchmark methods with regard to SKR.**

***Index Terms*—Physical-layer key generation, intelligent reflecting surfaces, deep neural network**

I. Introduction

Along with the surge in data traffic envisioned by sixth generation (6G) communication, data security risks emerge due to the broadcast nature of wireless transmissions [1]. In this context, physical-layer key generation (PKG) has been proposed as a promising technique that does not rely on conventional cryptographic approaches and is information-theoretically secure [2]. PKG utilizes the reciprocity of wireless channels during the channel coherent time to generate symmetric keys from bidirectional channel probings. The spatial decorrelation and channel randomness ensure the security of the generated keys.

However, PKG faces serious challenges in harsh propagation environments. The transmission link between two legitimate nodes may experience non-line-of-sight (NLOS) propagation conditions. In this case, the channel estimation will suffer from a low signal-to-noise ratio (SNR), resulting in a low secret key rate (SKR). Besides, in a quasi-static environment that lacks randomness, the achievable SKR is limited due to low channel entropy [2].

To address these challenges, a new paradigm, called intelligent reflecting surface (IRS), offers attractive solutions [3]–[5]. IRS consists of low-cost passive reflecting elements that can dynamically adjust their amplitudes and/or phases to reconfigure the wireless propagation environments [6]. The reflection channels provided by IRS are capable of enhancing the received signals at legitimate users and introducing rich channel randomness. The work in [3] improved the SKR of an IRS-aided single-antenna system by randomly configuring the IRS's phase shifts, in which closed-form expressions of the lower and upper bounds of the SKR were provided. In [4], the IRS reflecting coefficients were optimized to maximize the minimum achievable SKR. Successive convex approximation was adopted to address the non-convex optimization objective. In [5], the authors considered a multi-user scenario and designed IRS phase shifts to maximize the sum SKR. Generally, the optimal configuration of IRS is a complex non-convex optimization problem and requires iterative optimization. This problem is exacerbated in multi-antenna systems that require a joint design of multi-antenna precoding and IRS phase shifting.

Recently, machine learning has emerged as one of the key techniques of 6G and has been employed to address mathematically intractable non-convex optimization problems [7]. There have been several works [8], [9] leveraging machine learning to optimize IRS reflecting beamforming with the aim of maximizing downlink transmission rates. A recent work [10] proposed a machine learning based adaptive quantization method to balance key generation rate and bit disagreement ratio in an IRS-aided single-antenna system. Up to now, the employment of machine learning to jointly optimize BS precoding and IRS reflecting coefficient vector in an IRS-aided PKG system has not been investigated yet.

To the best of our knowledge, this is the first attempt to exploit machine learning in PKG for an IRS-assisted multi-antenna system. Our major contributions are summarized as follows:

- We propose a new PKG framework for an IRS-assisted multi-antenna system and derive the closed-form expression of SKR.
- The optimization problem of SKR maximization is for-

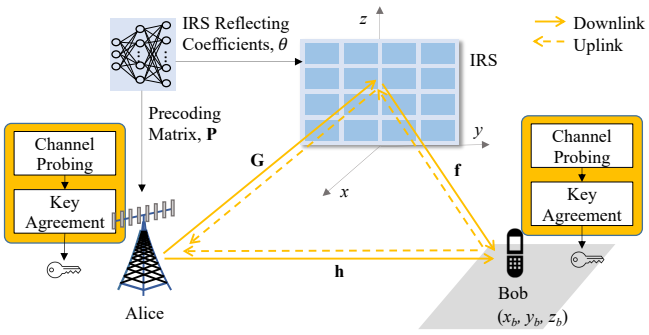

Fig. 1. System model.

mulated and a water-filling algorithm based baseline solution is developed.

- We novelly propose to obtain the optimal configuration of BS precoding and IRS phase shifting by using unsupervised deep neural networks (DNNs), referred to as "PKG-Net". Simulations demonstrate that the proposed PKG-Net can achieve a higher SKR than other benchmark methods.

Notations: In this paper, scalars are represented by italic letters, vectors by boldface lower-case letters, and matrices by boldface upper-case letters. $\mathbf{V}^T$, $\mathbf{V}^H$ and $\mathbf{V}^*$ are the transpose, conjugate transpose and conjugate of a matrix $\mathbf{V}$, respectively. $\mathbb{E}\{\cdot\}$ is the statistical expectation. $\mod(\cdot)$ and $\lfloor\cdot\rfloor$ denote modulus operator and floor function, respectively. $[\mathbf{V}]_{i,j}$ denotes the (i,j)-th element of a matrix $\mathbf{V}$. $\mathcal{CN}(\mu,\sigma^2)$ represents a circularly symmetric complex Gaussian distribution with mean μ and variance σ^2. $\mathrm{diag}(\mathbf{v})$ is a diagonal matrix with the entries of $\mathbf{v}$ on its main diagonal and $\mathrm{vec}(\mathbf{V})$ is the vectorization of a matrix $\mathbf{V}$. $||\cdot||_F$ denotes the Frobenius norm. $\odot$ and $\otimes$ are the Hadamard product and Kronecker product, respectively.

II. System Model

A. System Overview

We consider a narrowband scenario as shown in Fig. 1, which contains a multi-antenna BS, Alice, a single-antenna user equipment (UE), Bob, and an IRS. We assume that the BS is a uniform linear array with M antennas, and the IRS is a uniform planar array, which consists of $L = L_{\mathrm{H}} \times L_{\mathrm{V}}$ passive reflecting elements with L_{H} elements per row and L_{V} elements per column. To secure the communication, Alice and Bob perform PKG with the assistance of the IRS.

As shown in Fig. 1, the PKG protocol consists of two phases: channel probing and key agreement. During the channel probing phase, Alice and Bob perform bidirectional channel measurements by transmitting pilot signals to each other. We assume a time-division duplexing (TDD) protocol, and thus Alice and Bob can observe reciprocal channel information. During the key agreement phase, Alice and Bob quantize the channel observations into binary key bits. Then the disagreed key bits are corrected by information reconciliation and the leaked information is eliminated by privacy amplification [2]. In this paper, we focus on the channel probing phase.

B. Channel Model

We denote the BS-IRS, IRS-UE and BS-UE channels by $\mathbf{G} \in \mathbb{C}^{M\times L}$, $\mathbf{f} \in \mathbb{C}^{L\times 1}$ and $\mathbf{h} \in \mathbb{C}^{M\times 1}$, respectively. In practice, there exist spatial correlations among BS antennas and IRS elements. For simplicity, we adopt the spatial correlation model in isotropic scattering environments [11]. The (n,m)-th element of the spatial correlation matrix at the IRS is given by [11]

$$[\mathbf{R}_{\mathrm{I}}]_{n,m} = \frac{\sin(\frac{2\pi}{\lambda}||\mathbf{u}_n - \mathbf{u}_m||_2)}{\frac{2\pi}{\lambda}||\mathbf{u}_n - \mathbf{u}_m||_2}, \; n,m = 1,\ldots,L, \tag{1}$$

where λ is the wavelength, and $\mathbf{u}_n$ denotes the location of the n-th element and is computed as $\mathbf{u}_n = [0, y_n\Delta, z_n\Delta]^T$, where $y_n = \mod(n-1, L_{\mathrm{H}})$ and $z_n = \lfloor (n-1)/L_{\mathrm{H}} \rfloor$ are the horizontal and vertical indices of the n-th element, respectively, and Δ is the element spacing. The spatial correlation matrix at the BS is represented by $\mathbf{R}_{\mathrm{B}}$ with the (n,m)-th element given by

$$[\mathbf{R}_{\mathrm{B}}]_{m,n} = \eta^{|m-n|}, \tag{2}$$

where η is the correlation coefficient among BS antennas [12]. Then the channels can be described as

$$\mathbf{G} = \mathbf{R}_{\mathrm{B}}^{1/2}\widetilde{\mathbf{G}}\mathbf{R}_{\mathrm{I}}^{1/2}, \tag{3}$$

$$\mathbf{f} = \mathbf{R}_{\mathrm{I}}^{1/2}\widetilde{\mathbf{f}}, \tag{4}$$

$$\mathbf{h} = \mathbf{R}_{\mathrm{B}}^{1/2}\widetilde{\mathbf{h}}, \tag{5}$$

where $\widetilde{\mathbf{G}} \in \mathbb{C}^{M\times L}$, $\widetilde{\mathbf{f}} \in \mathbb{C}^{L\times 1}$ and $\widetilde{\mathbf{h}} \in \mathbb{C}^{M\times 1}$ consist of uncorrelated elements $\mathcal{CN}(0,\beta_{\mathrm{G}})$, $\mathcal{CN}(0,\beta_{\mathrm{f}})$ and $\mathcal{CN}(0,\beta_{\mathrm{h}})$, respectively, where β_{G}, β_{f} and β_{h} are the path loss of the BS-IRS, IRS-UE and BS-UE channels, respectively.

C. IRS Assisted Channel Probing

The channel probing is composed of bidirectional measurements, i.e., uplink and downlink probings.

1) Uplink Channel Probing: During the uplink phase, Bob transmits a pilot signal $s_u \in \mathbb{C}^{1\times 1}$ to Alice. The received signal at Alice is given by

$$\mathbf{y}_a = \sqrt{P_b}\,(\mathbf{h} + \mathbf{G}\boldsymbol{\Theta}\mathbf{f})\,s_u + \mathbf{n}_a, \tag{6}$$

where $\mathbf{y}_a \in \mathbb{C}^{M\times 1}$, P_b is the transmit power of Bob, $\boldsymbol{\Theta} = \mathrm{diag}\left(e^{j\theta_1}, e^{j\theta_2}, \ldots, e^{j\theta_L}\right)$ denotes the IRS reflecting-coefficient matrix with $\theta_l \in [0, 2\pi]$ for the l-th element and $\mathbf{n}_a \in \mathbb{C}^{M\times 1}$ is the complex Gaussian noise vector at Alice. Then Alice applies the precoding matrix $\mathbf{P} \in \mathbb{C}^{M\times M}$ to $\mathbf{y}_a$ and obtains

$$\widehat{\mathbf{y}}_a = \sqrt{P_b}\mathbf{P}^T\,(\mathbf{h} + \mathbf{G}\boldsymbol{\Theta}\mathbf{f})\,s_u + \mathbf{P}^T\mathbf{n}_a. \tag{7}$$

After the least square (LS) channel estimation, the uplink channel is estimated as

$$\widetilde{\mathbf{y}}_a = \sqrt{P_b}\mathbf{P}^T\,(\mathbf{h} + \mathbf{G}\boldsymbol{\Theta}\mathbf{f}) + \mathbf{P}^T\mathbf{n}_a s_u^*. \tag{8}$$

2) Downlink Channel Probing: During the downlink phase, Alice transmits a pilot signal of length M, $\mathbf{S}_d \in \mathbb{C}^{M\times M}$, with $\mathbf{S}_d^H\mathbf{S}_d = \mathbf{I}_M$ to Bob. The received signal at Bob is given by

$$\mathbf{y}_b = \left(\mathbf{h} + \mathbf{G}\boldsymbol{\Theta}\mathbf{f}\right)^T \mathbf{P}\mathbf{S}_d^H + \mathbf{n}_b, \tag{9}$$

where $\mathbf{y}_b \in \mathbb{C}^{1\times M}$, $\mathbf{n}_b \in \mathbb{C}^{1\times M}$ is the complex Gaussian noise vector at Bob. After LS channel estimation, the downlink channel is estimated as

$$\begin{aligned}\widetilde{\mathbf{y}}_b &= \left(\mathbf{h} + \mathbf{G}\boldsymbol{\Theta}\mathbf{f}\right)^T \mathbf{P}\mathbf{S}_d^H\mathbf{S}_d\left(\mathbf{S}_d^H\mathbf{S}_d\right)^{-1} + \mathbf{n}_b\mathbf{S}_d\left(\mathbf{S}_d^H\mathbf{S}_d\right)^{-1} \\ &= \left(\mathbf{h} + \mathbf{G}\boldsymbol{\Theta}\mathbf{f}\right)^T \mathbf{P} + \mathbf{n}_b\mathbf{S}_d. \end{aligned}\tag{10}$$

Then Bob transposes $\widetilde{\mathbf{y}}_b$ and obtains

$$\widetilde{\mathbf{y}}_b^T = \mathbf{P}^T\left(\mathbf{h} + \mathbf{G}\boldsymbol{\Theta}\mathbf{f}\right) + \mathbf{S}_d^T\mathbf{n}_b^T. \tag{11}$$

III. Secret Key Rate

In this paper, we assume that the passive Eve is far away from both Alice and Bob and the eavesdropping channels are independent of the channels between Alice and Bob [2]. The scenario with correlated eavesdropping channels will be investigated in our future work. Under this assumption, the SKR can be calculated by the mutual information of legitimate nodes' channel estimations as follows:

$$I\left(\widetilde{\mathbf{y}}_a; \widetilde{\mathbf{y}}_b^T\right) = H\left(\widetilde{\mathbf{y}}_a\right) + H\left(\widetilde{\mathbf{y}}_b^T\right) - H\left(\widetilde{\mathbf{y}}_a, \widetilde{\mathbf{y}}_b^T\right), \tag{12}$$

where $I(X;Y)$ denotes the mutual information between random variables X and Y, and $H(\cdot)$ denotes differential entropy.

To facilitate further derivations, we introduce cascaded channel $\mathbf{h}_c \in \mathbb{C}^{M(L+1)\times 1}$, which is given by

$$\mathbf{h}_c = \mathrm{vec}([\mathbf{h}\ \mathbf{G}\mathrm{diag}(\mathbf{f})]). \tag{13}$$

Then the combined channel can be expressed in a compact form:

$$\mathbf{h} + \mathbf{G}\boldsymbol{\Theta}\mathbf{f} \overset{(a)}{=} \begin{bmatrix}\mathbf{h}\ \mathbf{G}\mathrm{diag}(\mathbf{f})\end{bmatrix}\begin{bmatrix}1\\ \boldsymbol{\theta}\end{bmatrix} \overset{(b)}{=} (\widetilde{\boldsymbol{\theta}}^T \otimes \mathbf{I}_M)\mathbf{h}_c, \tag{14}$$

where $\boldsymbol{\theta} = [[\boldsymbol{\Theta}]_{1,1}, [\boldsymbol{\Theta}]_{2,2}, \cdots, [\boldsymbol{\Theta}]_{L,L}]^T$, $\widetilde{\boldsymbol{\theta}} = [1, \boldsymbol{\theta}^T]^T$, (a) holds because $\mathrm{diag}(\boldsymbol{\theta})\mathbf{f} = \mathrm{diag}(\mathbf{f})\boldsymbol{\theta}$ and (b) holds because $\mathrm{vec}(\mathbf{XYZ}) = (\mathbf{Z}^T \otimes \mathbf{X})\mathrm{vec}(\mathbf{Y})$. Plugging (14) into (8) and (11), we have

$$\begin{aligned}\widetilde{\mathbf{y}}_a &= \sqrt{P_b}\left(\widetilde{\boldsymbol{\theta}}^T \otimes \mathbf{P}^T\right)\mathbf{h}_c + \mathbf{P}^T\mathbf{n}_a s_u^* \\ &= \sqrt{P_b}\left(\widetilde{\boldsymbol{\theta}} \otimes \mathbf{P}\right)^T \mathbf{h}_c + \mathbf{P}^T\mathbf{n}_a s_u^*, \end{aligned}\tag{15}$$

$$\widetilde{\mathbf{y}}_b^T = \left(\widetilde{\boldsymbol{\theta}} \otimes \mathbf{P}\right)^T \mathbf{h}_c + \mathbf{S}_d^T\mathbf{n}_b^T. \tag{16}$$

Theorem 1: The SKR of the IRS assisted multi-antenna system is given by

$$I\left(\widetilde{\mathbf{y}}_a; \widetilde{\mathbf{y}}_b^T\right) = \log_2\left(\frac{\left|P_b\mathbf{R}_{\mathrm{Z}} + \delta^2\mathbf{P}^T\mathbf{P}^*\right|\left|\mathbf{R}_{\mathrm{Z}} + \delta^2\mathbf{I}_M\right|}{\left|P_b\delta^2\mathbf{R}_{\mathrm{Z}} + \delta^2\mathbf{P}^T\mathbf{P}^*\left(\mathbf{R}_{\mathrm{Z}} + \delta^2\mathbf{I}_M\right)\right|}\right), \tag{17}$$

where δ^2 is the Gaussian noise power and $\mathbf{R}_{\mathrm{Z}} = \left(\widetilde{\boldsymbol{\theta}} \otimes \mathbf{P}\right)^T \mathbf{R}_c \left(\widetilde{\boldsymbol{\theta}} \otimes \mathbf{P}\right)^*$ with

$$\mathbf{R}_c = \begin{bmatrix}\beta_{\mathrm{h}}\mathbf{R}_{\mathrm{B}} & \mathbf{0}^T \\ \mathbf{0} & \beta_{\mathrm{G}}\beta_{\mathrm{f}}\mathbf{R}_{\mathrm{I}} \odot \mathbf{R}_{\mathrm{I}} \otimes \mathbf{R}_{\mathrm{B}}\end{bmatrix}. \tag{18}$$

Proof: See Appendix A. ∎

In this paper, we aim to maximize the SKR by jointly optimizing the BS precoding matrix of $\mathbf{P}$ and the IRS reflecting coefficient vector of $\boldsymbol{\theta}$. The channel spatial covariance is assumed to be known by the BS [13]. Accordingly, the optimization problem is formulated as

$$(\mathcal{P}1)\ \max_{\mathbf{P},\boldsymbol{\theta}}\ I\left(\widetilde{\mathbf{y}}_a; \widetilde{\mathbf{y}}_b^T\right) \tag{19}$$

$$s.t.\ \mathrm{Tr}\left(\mathbf{P}\mathbf{P}^H\right) = P_a M, \tag{19a}$$

$$|[\boldsymbol{\Theta}]_{l,l}| = 1, l = 1, 2, \cdots, L, \tag{19b}$$

where P_a is the transmit power of Alice.

IV. Baseline Solution

The original optimization problem is a high-dimensional non-convex problem, which is difficult to solve with conventional optimization methods. For ease of further simplification, we rewrite $I\left(\widetilde{\mathbf{y}}_a; \widetilde{\mathbf{y}}_b^T\right)$ as

$$I\left(\widetilde{\mathbf{y}}_a; \widetilde{\mathbf{y}}_b^T\right) = \log_2\left(\frac{\left|P_b\delta_h^2\mathbf{P}^T\mathbf{R}_{\mathrm{B}}\mathbf{P}^* + \delta^2\mathbf{P}^T\mathbf{P}^*\right|\left|\delta_h^2\mathbf{P}^T\mathbf{R}_{\mathrm{B}}\mathbf{P}^* + \delta^2\mathbf{I}_M\right|}{\left|P_b\delta^2\delta_h^2\mathbf{P}^T\mathbf{R}_{\mathrm{B}}\mathbf{P}^* + \delta^2\mathbf{P}^T\mathbf{P}^*\left(\delta_h^2\mathbf{P}^T\mathbf{R}_{\mathrm{B}}\mathbf{P}^* + \delta^2\mathbf{I}_M\right)\right|}\right), \tag{20}$$

where $\delta_h^2 = \beta_{\mathrm{h}} + \beta_{\mathrm{G}}\beta_{\mathrm{f}}\boldsymbol{\theta}^H(\mathbf{R}_{\mathrm{I}} \odot \mathbf{R}_{\mathrm{I}})\boldsymbol{\theta}$. We further rewrite $\mathbf{P}$ as $\mathbf{P} = \sqrt{P_a}\mathbf{P}_{\mathrm{e}}$, where $\mathbf{P}_{\mathrm{e}}$ is a normalized matrix. Then $I\left(\widetilde{\mathbf{y}}_a; \widetilde{\mathbf{y}}_b^T\right)$ can be derived as

$$I\left(\widetilde{\mathbf{y}}_a; \widetilde{\mathbf{y}}_b^T\right) = \log_2\left(\frac{\left|P_bP_a\delta_h^2\widehat{\mathbf{R}}_{\mathrm{Z}} + \delta^2P_a{\mathbf{P}_{\mathrm{e}}}^T\mathbf{P}_{\mathrm{e}}^*\right|\left|P_a\delta_h^2\widehat{\mathbf{R}}_{\mathrm{Z}} + \delta^2\mathbf{I}_M\right|}{\left|\delta^2P_bP_a\delta_h^2\widehat{\mathbf{R}}_{\mathrm{Z}} + \delta^2P_a{\mathbf{P}_{\mathrm{e}}}^T\mathbf{P}_{\mathrm{e}}^*\left(P_a\delta_h^2\widehat{\mathbf{R}}_{\mathrm{Z}} + \delta^2\mathbf{I}_M\right)\right|}\right), \tag{21}$$

where $\widehat{\mathbf{R}}_{\mathrm{Z}} = {\mathbf{P}_{\mathrm{e}}}^T\mathbf{R}_{\mathrm{B}}\mathbf{P}_{\mathrm{e}}^*$. To facilitate further optimization, we approximate ${\mathbf{P}_{\mathrm{e}}}^T{\mathbf{P}_{\mathrm{e}}}^*$ as $\mathbf{I}_M$ in the noise term. Accordingly, $I\left(\widetilde{\mathbf{y}}_a; \widetilde{\mathbf{y}}_b^T\right)$ is approximated as

$$\widehat{I}\left(\widetilde{\mathbf{y}}_a; \widetilde{\mathbf{y}}_b^T\right) = \log_2\left(\frac{\left|P_bP_a\delta_h^2\widehat{\mathbf{R}}_{\mathrm{Z}} + \delta^2P_a\mathbf{I}_M\right|\left|P_a\delta_h^2\widehat{\mathbf{R}}_{\mathrm{Z}} + \delta^2\mathbf{I}_M\right|}{\left|\delta^2P_bP_a\delta_h^2\widehat{\mathbf{R}}_{\mathrm{Z}} + \delta^2P_a\left(P_a\delta_h^2\widehat{\mathbf{R}}_{\mathrm{Z}} + \delta^2\mathbf{I}_M\right)\right|}\right). \tag{22}$$

After Cholesky factorization, we have

$$\begin{aligned}\widehat{\mathbf{R}}_{\mathrm{Z}} &= \mathbf{P}_{\mathrm{e}}^T\mathbf{R}_{\mathrm{B}}^{1/2}\left(\mathbf{R}_{\mathrm{B}}^{1/2}\right)^H\mathbf{P}_{\mathrm{e}}^* \\ &= \left(\left(\mathbf{R}_{\mathrm{B}}^{1/2}\right)^H\mathbf{P}_{\mathrm{e}}^*\right)^H\left(\left(\mathbf{R}_{\mathrm{B}}^{1/2}\right)^H\mathbf{P}_{\mathrm{e}}^*\right). \end{aligned}\tag{23}$$

Then we perform the following eigenvalue decomposition:

$$\left(\mathbf{R}_{\mathrm{B}}^{1/2}\right)^H\mathbf{P}_{\mathrm{e}}^* = \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^H, \tag{24}$$

where $\mathbf{\Lambda} = \text{diag}(p_1, p_2, \ldots, p_M)$ with the eigenvalues sorted in descending order. Substituting (23) and (24) into (22), $\widehat{I}\left(\widetilde{\mathbf{y}}_a; \widetilde{\mathbf{y}}_b^T\right)$ can be rewritten as (25), which is shown at the top of the next page.

Lemma 1: $\widehat{I}\left(\widetilde{\mathbf{y}}_a; \widetilde{\mathbf{y}}_b^T\right)$ is maximized when all the IRS reflecting elements have the same phase configuration, i.e., $\theta_i = \theta_j, \forall i \neq j$.

Proof: Due to the space limitation, the proof will be given in the extended journal version. ■

Following Lemma 1, we set $\theta_i = \theta_j, \forall i \neq j$ and have $\delta_h^2 = \beta_{\text{h}} + \beta_{\text{G}}\beta_{\text{f}} \sum_{i=1}^{L}\sum_{j=1}^{L} \left[\mathbf{R}_{\text{I}} \odot \mathbf{R}_{\text{I}}\right]_{i,j}$.

We further perform eigenvalue decomposition on $\mathbf{R}_{\text{B}}$ and obtain $\mathbf{R}_{\text{B}} = \mathbf{U}_{\text{B}}\mathbf{\Lambda}_{\text{B}}\mathbf{U}_{\text{B}}^H$, where $\mathbf{\Lambda}_{\text{B}} = \text{diag}\left(p_{\text{B},1}, p_{\text{B},2}, \ldots, p_{\text{B},M}\right)$ with the eigenvalues sorted in descending order. The optimal $\mathbf{\Lambda}$ can be obtained by solving the following optimization problem:

$$(\mathcal{P}2) \ \max_{p_i} \ \sum_{i=1}^{M} \log_2 \left(\frac{\left(P_b P_a \delta_h^2 p_i^2 + \delta^2 P_a\right)\left(P_a \delta_h^2 p_i^2 + \delta^2\right)}{\delta^2 P_b P_a \delta_h^2 p_i^2 + \delta^2 P_a^2 \delta_h^2 p_i^2 + \delta^4 P_a} \right) \tag{26}$$

$$s.t. \ \sum_{i=1}^{M} \frac{p_i^2}{p_{\text{B},i}} = M, \tag{26a}$$

where (26a) comes from the constraint $\text{Tr}\left(\mathbf{P}_{\text{e}}\mathbf{P}_{\text{e}}^H\right) = \text{Tr}(\mathbf{\Lambda}_{\text{B}}^{-1}\mathbf{\Lambda}^2) = M$. $(\mathcal{P}2)$ can be solved by using water-filling algorithm [14], the details of which are omitted here due to limited space. Denoting the optimal $\mathbf{\Lambda}$ obtained from $(\mathcal{P}2)$ by $\mathbf{\Lambda}^{\text{opt}}$, the corresponding $\mathbf{P}_{\text{e}}$ can be computed from (24) and expressed as $\mathbf{P}_{\text{e}}^{\text{opt}} = \left(\mathbf{R}_{\text{B}}^{-1/2}\mathbf{U}\mathbf{\Lambda}^{\text{opt}}\mathbf{U}^H\right)^*$. Notice that $\mathbf{P}_{\text{e}}^{\text{opt}}$ is suboptimal to the original optimization problem $(\mathcal{P}1)$ due to the approximation in (22).

V. Proposed Machine Learning Based Method

The baseline solution is an iterative algorithm with a complex structure. In this section, we propose to directly solve $(\mathcal{P}1)$ using DNNs. More specifically, we aim to train a DNN to learn the mapping relationship between the location information of Bob and the optimal $\mathbf{P}$ and $\boldsymbol{\theta}$ that maximize the SKR.

The structure of the proposed PKG-Net is shown in Fig. 2. In particular, the input is the location information of Bob (x_b, y_b, z_b), which is a 3×1 tensor. Then two fully connected (FC) layers are adopted as hidden layers for feature extraction with ReLu as the activation function. The output layer consists of two FC layers. Since neural networks only support real-valued outputs, the first $2 \times M \times M$ FC layer outputs a real-valued tensor $\mathbf{p}^{'} \in \mathbb{R}^{2M^2 \times 1}$ and the second $2 \times L$ FC layer outputs a real-valued tensor $\boldsymbol{\theta}^{'} \in \mathbb{R}^{2L \times 1}$. To obtain the precoding matrix and satisfy the total power constraint, the first normalization layer converts $\mathbf{p}^{'}$ to a complex-valued matrix $\mathbf{P}$ and performs the following normalization step:

$$\mathbf{P} = \sqrt{MP_a}\frac{\mathbf{P}}{\|\mathbf{P}\|_F^2}. \tag{27}$$

Similarly, to satisfy the unit modulus constraint, the second normalization layer performs

$$\boldsymbol{\theta}_l = \frac{\boldsymbol{\theta}_l^{'}}{\sqrt{\left(\boldsymbol{\theta}_l^{'}\right)^2 + \left(\boldsymbol{\theta}_{l+L}^{'}\right)^2}} + j\frac{\boldsymbol{\theta}_{l+L}^{'}}{\sqrt{\left(\boldsymbol{\theta}_l^{'}\right)^2 + \left(\boldsymbol{\theta}_{l+L}^{'}\right)^2}}, \forall l. \tag{28}$$

During the training phase, the PKG-Net learns to update its parameters in an unsupervised manner. The goal is to maximize the SKR, namely, minimize the following loss function:

$$\mathcal{L}_{\text{loss}} = -\frac{1}{K}\sum_{k=1}^{K} I\left(\widetilde{\mathbf{y}}_{a,k}; \widetilde{\mathbf{y}}_{b,k}^T\right), \tag{29}$$

where K is the number of training samples, and $\widetilde{\mathbf{y}}_{a,k}$ and $\widetilde{\mathbf{y}}_{b,k}^T$ are the channel estimations in the k-th training. It is clear that the smaller the loss function, the higher the average SKR. The DNN is updated using the stochastic gradient descent method and implemented by Adam optimizer with a learning rate of 0.001. The training phase is performed offline, and thus the computational complexity is less a concern.

During the online inference phase, the BS directly designs the precoding matrix and IRS reflecting coefficients according to the output of the trained neural network as soon as it gets the location information of Bob.

VI. Simulation Results

In this section, we numerically evaluate the SKR performance of the proposed PKG-Net in comparison with the benchmark methods.

A. Simulation Setup

The coordinates of the BS and the IRS in meters are set as (5, -35, 0) and (0, 0 , 0), respectively. The large-scale path loss in dB is computed by

$$\beta_i = \beta_0 - 10\alpha_i \log_{10}\left(d/d_0\right), \tag{30}$$

where $\beta_0 = -30$ dB is the path loss at the reference distance, $d_0 = 1$ m is the reference distance, d is the transmission distance, and α_i is the path-loss exponent. For the direct link, i.e., $i = \text{h}$, we set $\alpha_i = 3.67$; for the reflecting links, i.e., $i = \text{G}$ or f, we set $\alpha_i = 2$. The noise power is set to $\delta^2 = -90$ dBm. The IRS is assumed to be a uniform square array, i.e., $L_{\text{H}} = L_{\text{V}}$. Unless otherwise specified, the default spatial correlation coefficient at the BS is set to $\eta = 0.3$ and the IRS element spacing is half a wavelength, i.e., $\Delta = \frac{\lambda}{2}$. We assume that the uplink and downlink channel probings use the same transmit power, i.e., $P_a = P_b = P$.

During the training of the proposed PKG-Net, the UE location is uniformly distributed in the xy-plane with $x \in [5, 15]$ and $y \in [5, 15]$ to achieve generalization ability to various UE locations. Each hidden layer of the PKG-Net has 200 neurons. We train the neural network with 100 epochs. In each epoch, 1000 random UE locations are used as training samples with a batch size of 100.

We compare the proposed PKG-Net with the following benchmark methods:

$$\widehat{I}\left(\widetilde{\mathbf{y}}_a;\widetilde{\mathbf{y}}_b^T\right)=\log_2\left(\frac{\left|P_bP_a\delta_h^2\mathbf{U}\mathbf{\Lambda}^T\mathbf{\Lambda}\mathbf{U}^H+\delta^2P_a\mathbf{I}_M\right|\left|P_a\delta_h^2\mathbf{U}\mathbf{\Lambda}^T\mathbf{\Lambda}\mathbf{U}^H+\delta^2\mathbf{I}_M\right|}{\left|\delta^2P_bP_a\delta_h^2\mathbf{U}\mathbf{\Lambda}^T\mathbf{\Lambda}\mathbf{U}^H+\delta^2P_a\left(P_a\delta_h^2\mathbf{U}\mathbf{\Lambda}^T\mathbf{\Lambda}\mathbf{U}^H+\delta^2\mathbf{I}_M\right)\right|}\right)$$
$$=\sum_{i=1}^{M}\log_2\left(\frac{\left(P_bP_a\delta_h^2p_i^2+\delta^2P_a\right)\left(P_a\delta_h^2p_i^2+\delta^2\right)}{\delta^2P_bP_a\delta_h^2p_i^2+\delta^2P_a^2\delta_h^2p_i^2+\delta^4P_a}\right),\tag{25}$$

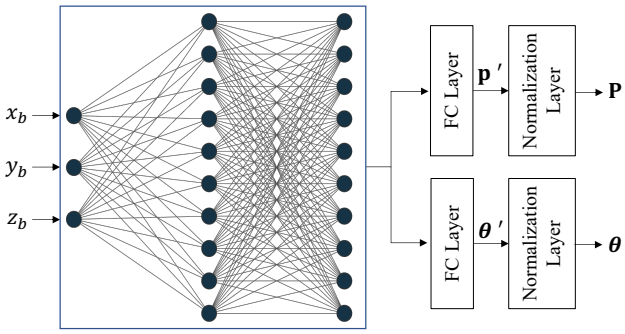

Fig. 2. Structure of the proposed PKG-Net.

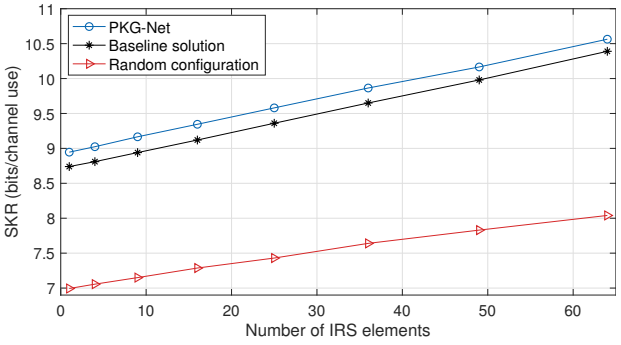

Fig. 4. SKR versus L with $P=10$ dBm and $M=4$.

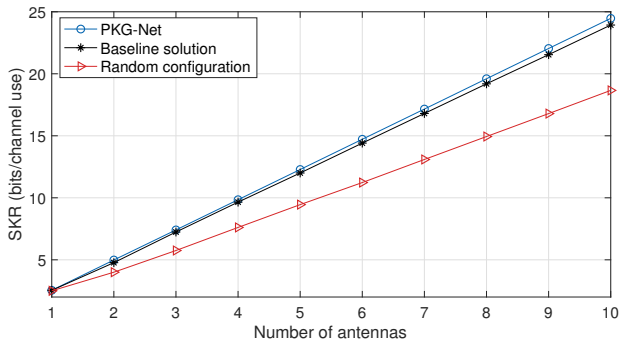

Fig. 3. SKR versus M with $P=10$ dBm and $L=36$.

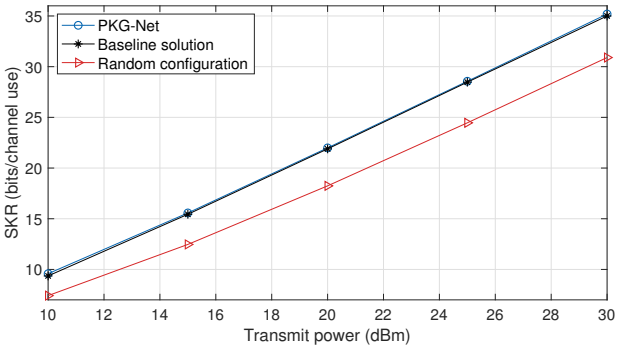

Fig. 5. SKR versus P with $M=4$ and $L=25$.

- Baseline solution: Represent the water-filling algorithm based solution proposed in Section IV.
- Random configuration: Represent a non-optimized scheme, where both the precoding matrix $\mathbf{P}$ and the IRS reflecting coefficient vector $\boldsymbol{\theta}$ are randomly configured.

B. Results

In the following numerical evaluation, the UE location is set as $(x_b, y_b, z_b)=(10,10,0)$ unless otherwise stated.

In Fig. 3, we show the effect of the number of antennas on the SKR. First, it is observed that the SKR increases linearly with the number of antennas, as more antennas introduce more sub-channels to extract secure keys. Moreover, we can see that regardless of the number of antennas, the proposed PKG-Net achieves a higher SKR than the two benchmark methods, demonstrating the effectiveness of the proposed DNN-based algorithm. The gap in terms of SKR between the proposed PKG-Net and other benchmark methods increases with the number of antennas, indicating that using more antennas requires a more sophisticated design of BS precoding.

Fig. 4 illustrates the effect of the number of IRS elements on the SKR. As can be observed, the SKR monotonically increases with the number of IRS elements, since more IRS elements provide more reflection links that improve the received signals during channel probings. It is noticed that the SKR gain of increasing IRS elements is not as significant as that of increasing BS antennas. This is because in the proposed PKG system, the downlink pilot length is proportional to the number of antennas. It is expected to achieve a higher SKR when the entire cascaded channel is estimated with a minimum pilot length of $M(L+1)$, which requires a new design of IRS phase shifting and will be of interest in our future work.

In Fig. 5, the SKR versus the transmit power is displayed. It is shown that the SKR monotonically increases with the transmit power for all the considered optimization methods, which is straightforward due to the fact that a higher transmit power leads to a higher SNR, thereby improving the reciprocity of channel observations at Alice and Bob.

Fig. 6 shows the SKR versus the spatial correlation coefficient at the BS for different UE locations. We can see

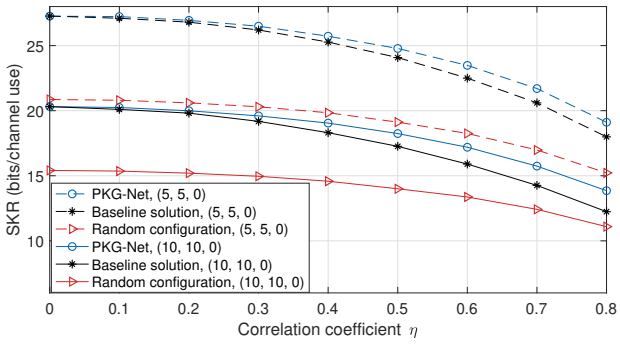

Fig. 6. SKR versus η with $P = 10$ dBm, $M = 8$ and $L = 36$.

that the SKR monotonically decreases with the correlation coefficient, which illustrates that the existence of spatial correlation degrades the performance of PKG in terms of SKR. In comparison with the benchmark methods, the proposed PKG-Net can effectively design the BS precoding and IRS phase shifting under different spatial correlation conditions. Interestingly, when the correlation coefficient increases, the SKR gain of the proposed PKG-Net becomes more significant compared to the baseline solution. Furthermore, the proposed PKG-Net shows good generalization to UE locations.

VII. Conclusion

In this paper, we have studied the PKG in an IRS-assisted multi-antenna system. We have developed a new PKG framework and derived the closed-form expression of SKR. To maximize the SKR, we proposed a novel DNN-based algorithm, PKG-Net, to jointly configure the precoding matrix at the BS and the reflecting coefficient vector at the IRS. Simulation results show that under various system parameters, the proposed PKG-Net achieves a higher SKR than the benchmark methods. Additionally, it is observed that the spatial correlation among BS antennas degrades the PKG performance in terms of SKR, and that the proposed PKG-Net can address the spatial correlation more effectively than other benchmark methods. In our future work, we will extend the proposed PKG system to a multi-user scenario and solve the multi-user precoding problem.

Appendix A
Proof of Theorem 1

Following [13], (12) can be further derived as

$$I\left(\widetilde{\mathbf{y}}_a;\widetilde{\mathbf{y}}_b^T\right) = H\left(\widetilde{\mathbf{y}}_a\right) + H\left(\widetilde{\mathbf{y}}_b^T\right) - H\left(\widetilde{\mathbf{y}}_a,\widetilde{\mathbf{y}}_b^T\right) = \log_2\left(\frac{|\mathbf{R}_a||\mathbf{R}_b|}{|\boldsymbol{\mathcal{R}}_{a,b}|}\right), \tag{31}$$

where

$$\mathbf{R}_a = \mathbb{E}\left\{\widetilde{\mathbf{y}}_a\widetilde{\mathbf{y}}_a^H\right\} = P_b\left(\widetilde{\boldsymbol{\theta}}\otimes\mathbf{P}\right)^T\mathbf{R}_c\left(\widetilde{\boldsymbol{\theta}}\otimes\mathbf{P}\right)^* + \delta^2\mathbf{P}^T\mathbf{P}^*, \tag{32}$$

$$\mathbf{R}_b = \mathbb{E}\left\{\widetilde{\mathbf{y}}_b^T\widetilde{\mathbf{y}}_b^*\right\} = \left(\widetilde{\boldsymbol{\theta}}\otimes\mathbf{P}\right)^T\mathbf{R}_c\left(\widetilde{\boldsymbol{\theta}}\otimes\mathbf{P}\right)^* + \delta^2\mathbf{I}_M, \tag{33}$$

and

$$\boldsymbol{\mathcal{R}}_{a,b} = \begin{bmatrix}\mathbf{R}_a & \mathbf{R}_{a,b}\\ \mathbf{R}_{b,a} & \mathbf{R}_b\end{bmatrix}, \tag{34}$$

where $\mathbf{R}_c = \mathbb{E}\left\{\mathbf{h}_c\mathbf{h}_c^H\right\} = \begin{bmatrix}\beta_{\mathrm{h}}\mathbf{R}_{\mathrm{B}} & \mathbf{0}^T\\ \mathbf{0} & \beta_{\mathrm{G}}\beta_{\mathrm{f}}\mathbf{R}_{\mathrm{I}}\odot\mathbf{R}_{\mathrm{I}}\otimes\mathbf{R}_{\mathrm{B}}\end{bmatrix}$ and

$$\mathbf{R}_{a,b} = \mathbf{R}_{b,a} = \mathbb{E}\left\{\widetilde{\mathbf{y}}_a\widetilde{\mathbf{y}}_b^*\right\} = \sqrt{P_b}\left(\widetilde{\boldsymbol{\theta}}\otimes\mathbf{P}\right)^T\mathbf{R}_c\left(\widetilde{\boldsymbol{\theta}}\otimes\mathbf{P}\right)^*. \tag{35}$$

This completes the proof.

Acknowledgement

This work was supported in part by the UK EPSRC under grant ID EP/V027697/1; in part by the National Key Research, Development Program of China under grant ID 2020YFE0200600; and in part by the National Natural Science Foundation of China under Grant 62171121.

References

[1] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6g wireless: the role of physical layer security," *IEEE Commun. Stand. Mag.*, vol. 6, no. 1, pp. 102–108, 2022.

[2] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for iot security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138 406–138 446, 2020.

[3] T. Lu, L. Chen, J. Zhang, K. Cao, and A. Hu, "Reconfigurable intelligent surface assisted secret key generation in quasi-static environments," *IEEE Commun. Lett.*, vol. 26, no. 2, pp. 244–248, Feb. 2022.

[4] Z. Ji, P. L. Yeoh, D. Zhang, G. Chen, Z. He, H. Yin, and Y. li, "Secret key generation for intelligent reflecting surface assisted wireless communication networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 1030–1034, Jan. 2021.

[5] 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 Trans. Inf. Forensics Security*, vol. 17, pp. 211–225, Jan. 2022.

[6] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless communications: A tutorial," *IEEE Trans Commun.*, vol. 69, no. 5, pp. 3313–3351, 2021.

[7] J. Wang, C. Jiang, H. Zhang, Y. Ren, K.-C. Chen, and L. Hanzo, "Thirty years of machine learning: The road to pareto-optimal wireless networks," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1472–1514, 2020.

[8] A. Taha, M. Alrabeiah, and A. Alkhateeb, "Enabling large intelligent surfaces with compressive sensing and deep learning," *IEEE Access*, vol. 9, pp. 44 304–44 321, 2021.

[9] C. Huang, R. Mo, and C. Yuen, "Reconfigurable intelligent surface assisted multiuser miso systems exploiting deep reinforcement learning," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1839–1850, 2020.

[10] L. Jiao, G. Sun, J. Le, and K. Zeng, "Machine learning-assisted wireless phy key generation with reconfigurable intelligent surfaces," in *Proc. of the 3rd ACM Workshop on Wireless Security and Mach. Learning*, 2021, pp. 61–66.

[11] 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. 2020.

[12] Q. Zhu and Y. Hua, "Optimal pilots for maximal capacity of secret key generation," in *Proc. IEEE GLOBECOM 2019*, Hawaii, USA, Dec. 2019, pp. 0–5.

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

[14] C. Xing, Y. Jing, S. Wang, S. Ma, and H. V. Poor, "New viewpoint and algorithms for water-filling solutions in wireless communications," *IEEE Trans. Signal Process.*, vol. 68, pp. 1618–1634, Feb. 2020.