Intelligent Reflecting Surface–Assisted Wireless Secret Key Generation against Multiple Eavesdroppers

Ya Liu 1,2*, Kaizhi Huang 1,2, Xiaoli Sun 1, Shaochuan Yang 1 and Liang Wang 1,2

1 Wireless Communication Technology Office, Information Engineering University, Zhengzhou 450002, China; liuya2014@zua.edu.cn (Y.L.); lgdxsunxiaoli@sina.com (X.S.); yangsc@zua.edu.cn (S.Y.); jym@ndsc.com.cn (L.W.)

2 School of Intelligent Engineering, Zhengzhou University of Aeronautics, Zhengzhou 450015, China

* Correspondence: huangkaizhi@tsinghua.org.cn

Abstract: In this paper, we propose an improved physical layer key generation scheme that can maximize the secret key capacity by deploying intelligent reflecting surface (IRS) near the legitimate user aiming at improving its signal-to-noise ratio (SNR). We consider the scenario of multiple input single output (MISO) against multiple relevant eavesdroppers. We elaborately design and optimize the reflection coefficient matrix of IRS elements that can improve the legitimate user’s SNR through IRS passive beamforming and deteriorate the channel quality of eavesdroppers at the same time. We first derive the lower bound expression of the achievable key capacity, then solve the optimization problem based on semi-definite relaxation (SDR) and the convex–concave procedure (CCP) to maximize the secret key capacity. Simulation results show that our proposed scheme can significantly improve the secret key capacity and reduce hardware costs compared with other benchmark schemes.

Keywords: intelligent reflecting surface; physical layer secret key generation; semi-definite relaxation; convex–concave procedure

1. Introduction

The tremendous growth in extensive connectivity, ubiquity, and diversity of the sixth generation (6G) wireless communication networks will result in unpredictable security threats [1]. Traditionally, data confidentiality is guaranteed by the high-layer encryption mechanism based on computational complexity. However, the key distribution for massive devices is complicated. Furthermore, the public key cryptography may be completely cracked by the emerging quantum computers in the future [2]. As a powerful supplement to the existing high-layer encryption, the physical layer key generation (PKG) technology [3] makes use of the inherent characteristics of wireless channels (i.e., temporal variation, uniqueness, and reciprocity). The PKG extracts the key from the channel characteristics, which are considered as the natural shared random source [4–6]. It is information-theoretically secure and lightweight and is considered to be one of the enhanced technologies of 6G secure communication [7].

Key generation usually consists of four main steps: acquisition of shared random source, quantization, information reconciliation, and privacy amplification. First, two legitimate users, namely Alice and Bob, transmit pilots to each other in turn, and they estimate the channels between them to obtain correlated channel measurements. Then, these measurements are converted into binary bits by using quantization algorithms [8]. Next, information reconciliation is used to correct inconsistent bits between Alice and Bob [9]. Finally, the privacy amplification phase is employed to eliminate possible information leakage in the previous phases [10]. However, the channel estimation can have low accuracy due to the poor quality of the received signal in the acquisition of shared random source, introducing a high key inconsistency rate and low key entropy after quantization.
In [11], the authors consider the scenario that the base station uses the maximum ratio transmission (MRT) to maximize the SNR of the received signal, but this scheme results in limited improvement of the SNR. We also use preprocessing methods to remove the non-reciprocity caused by noise. However, part of the channel characteristic information will be abandoned, which reduces the key generation rate (KGR), increases the complexity of baseband algorithm processing, and introduces poor real-time performance.

Recently, intelligent reflecting surfaces (IRSs) that can flexibly control the electromagnetic characteristics of wireless channels have received much attention and are considered as a significant technology for 6G [12,13]. An IRS is typically constructed by using a printed circuit board (PCB), which consists of a reflective unit layer, a copper plate, and a control circuit board. The reflecting elements are equally spaced on a two-dimensional plane and are composed of full metal sheets on the bottom layers and metal patches on the top layers of the PCB dielectric substrates [14]. Moreover, a semiconductor device can vary the impedance of the reflecting element by controlling its biasing voltage so that the electromagnetic response can be dynamically tuned in real time without changing the geometrical parameters [15]. IRSs can achieve real-time configuration of various parameters of the reflected electromagnetic wave, including phase, amplitude, and polarization direction, and can artificially control the radio wave transmission. In addition, IRSs can smartly program and reconstruct electromagnetic waves in real time to customize the wireless environment with passive characteristics. IRSs are used to preprocess the wavefront of reflected electromagnetic waves; specifically, the polarization direction of the received signal is adjusted to match the polarization of the antenna of the legitimate receiver [16], which enhances the received signal strength.

Complex algorithm design is not required in our IRS-assisted PKG, which effectively reduces the key inconsistency and improves the SNR of the legitimate receiver and the key entropy. Research on IRS-assisted PKG has emerged recently. In Ref. [17], the authors design an IRS reflecting coefficient matrix to maximize the SNR received by the legitimate user in the single input single output (SISO) network. An IRS is utilized to introduce artificial randomness for boosting the secret key rate by adjusting the IRS phase switching to modify the propagation environment in [18–20]. In Ref. [19], the authors optimized the switching states of the IRS elements to maximize the secret key rate. A limited number of IRS elements were turned on, which corresponded to the largest variances of the IRS channels. However, the analysis of the secret key rate was greatly simplified, because the eavesdroppers’ channels were assumed to be independent of the legitimate users’. In Ref. [20], the authors further use IRSs and Wi-Fi equipment to build a prototype system to achieve any adjustable key rate. To sum up, IRSs can be utilized to improve the SNR or enhance the randomness as an artificial random source in the research of PKG. An IRS is used to improve the SNR in this paper, and the relationship between the number of IRS elements and transmitting antennas is not further explored in the current research. IRS-assisted PKG in multi-antenna networks remains unexplored; however, this is more relevant for the actual communication scenarios.

In this paper, we mainly consider an IRS-assisted MISO system model against multiple non-colluding eavesdroppers (non-colluding eavesdropping is practical in the IoT scenario, where nodes exist independently and do not cooperate. Partially colluding and fully colluding eavesdroppers will be discussed in Section 4), who gather around the legitimate user, targeting to obtain private information. We deploy an IRS near the legitimate user and elaborately design an IRS reflection coefficient matrix that can improve the legitimate user’s SNR through IRS passive beamforming, and thereby the legitimate user’s channel estimation accuracy is improved. At the same time, multiple eavesdroppers around the legitimate user, after IRS tuning, offset the reflected signals with the direct link signals from the base station, therefore deteriorating the channel quality and effectively reducing information leakage. In the presence of multiple passive eavesdroppers, we formulate the secret key capacity of the system and optimize the IRS reflection coefficient to maximize the secret key capacity under the constraint that the modulus square of the IRS reflection
coefficient is less than one. Due to the non-convexity of this optimization problem, we employ SDR and CCP to solve it. Simulation results show that our scheme significantly improves the secret key capacity compared with MRT and IRS with random phase shifts.

The rest of the paper is organized as follows. Section 2 describes the system model discussed in this paper and signal representation. In Section 3, we discuss the IRS-assisted secret key rate and derive the expression of key generation capacity. In Section 4, the proposed optimization scheme and solution are presented. Section 5 presents the simulation results. Section 6 draws the conclusions.

2. System Model and Signal Representation

As shown in Figure 1, a base station Alice and a single antenna user Bob are legitimate communication nodes aiming to extract the shared secret keys from their reciprocal wireless channel with the assistance of an IRS (Rose). K non-colluding eavesdroppers (Eves) attempt to acquire the transmitted information generated by Alice and Bob based on their own channel observations. All the eavesdroppers are non-colluding, meaning that each eavesdropper performs independent decoding to retrieve signals without relying on other eavesdroppers [21]. Suppose that all Eves are equipped with a single antenna, while the number of antennas at Alice are denoted by M. Rose is composed of N reflecting elements deployed in a uniform planar array (UPA), with X vertical elements and Y horizontal elements, and can change its reflection coefficients to minimize the information leaked to Eve.

![Figure 1. System model for IRS-assisted network against multiple Eves.](image)

2.1. Channel Model

The equivalent channels from Alice to Rose, Bob, and Eve k (the k-th eavesdropper) are denoted by $h_{ae} \in \mathbb{C}^{N \times M}$, $h_{ab} \in \mathbb{C}^{1 \times M}$, and $h_{ae_k} \in \mathbb{C}^{1 \times M}$, respectively, while the equivalent channels from Rose to Bob and Eve k are denoted by $h_{rb} \in \mathbb{C}^{1 \times N}$ and $h_{re_k} \in \mathbb{C}^{1 \times N}$, respectively.

Let $\Phi = \text{diag}(\beta_1 e^{j\theta_1}, \beta_2 e^{j\theta_2}, \ldots, \beta_N e^{j\theta_N})$ represent the diagonal phase-shifting matrix of Rose, where in its main diagonal, $\beta_n \in [0, 1]$ and $\theta_n \in [0, 2\pi]$ denote the amplitude and phase shift on the incident signal by Rose’s n-th element, for $n = 1, \ldots, N$. The reflecting coefficient vector of Rose $v = [v_1, v_2, \ldots, v_N]^T$ is defined, where the n-th element of v is $v_n = \beta_n e^{j\theta_n}$, which is the n-th diagonal element of $\Phi$.

We consider the case where the light of sight (LOS) path between the base station and Bob/Eve is blocked, and the Rayleigh fading model is considered due to plenty of scatters in this wireless channel, i.e., each element of $h_{ab}$ and $h_{ae_k}$ is independent and identically
We use Rician fading to model the channel where $\alpha$ which remains unchanged within the channel coherence time; and $\kappa$ and $\eta$ where $\alpha$ is the Rician distribution. The LoS component

between the IRS and Bob/Eve, LoS components exist in practical implementation. Both set as half wavelength, i.e., we have

where $\theta_{\text{IRS}} \in [0, \pi]$ and $\gamma_{\text{IRS}} \in [0, \pi]$ represent the elevation and azimuth angles of arrival (AOA) at IRS, respectively, and $\varphi_{\text{BS}} \in [0, 2\pi]$ is the azimuth angle of departure (AOD) from the BS and IRS. $\lambda$ is the wavelength, and $d_R$ and $d_B$ denote the element spacing at the IRS and the antenna spacing at the BS, respectively, and in this paper, they are both set as half wavelength, i.e., we have $d_R = d_B = \frac{\lambda}{2}$. The path loss can be derived as $\text{PL}(d) [\text{dB}] = \text{PL}_0 + 10c \log_{10}(d)$, where $d$, $\text{PL}_0$ and $c$ denote the distance between transmitter and receiver, constant path loss term, and path loss exponent, respectively. For the channels between the IRS and Bob/Eve, LoS components exist in practical implementation. We use Rician fading to model the channel $h_{br}$ and $h_{er}$, which can be denoted by

where $\kappa_2$ and $\kappa_3$ is the Rician $\kappa$-factor of $h_{br}$ and $h_{er}$; $\tilde{h}_{ru} \in \mathbb{C}^{1 \times N}$ is the LoS component, which remains unchanged within the channel coherence time; and $\tilde{h}_{ru} \in \mathbb{C}^{1 \times N}$ is the non-LoS (NLoS) component, whose elements follow the zero-mean complex Gaussian distribution. The LoS component $\tilde{h}_{ru}$ is expressed as

where $\alpha_{\text{IRS,u}}(\varphi_{\text{IRS,u}}, \omega_{\text{IRS,u}})$ is the normalized array response vector of the UPA at IRS, $\varphi_{\text{IRS,u}} \in [0, \pi]$ and $\omega_{\text{IRS,u}} \in [0, \pi]$ denote the elevation and azimuth AOD from IRS to Bob/Eve $k$, respectively, where $\eta_2$ and $\eta_3$ are the complex gain of IRS-to-Bob and IRS-to-Eve channels, respectively. To generate the shared secret keys, Alice and Bob will alternatively exchange pilots and perform channel estimations. In the downlink channel probing, the BS broadcasts the orthogonal pilot signal $S_1 \in \mathbb{C}^{M \times T_1}$, where $T_1$ is the length of pilot, $S_1^H = I_{M \times M}$, and $I$ is an $M \times M$ identity matrix. Assuming that the transmitting power of the base station (BS) is $P$, the received signal of Bob or the $k$-th Eve is given by

where $G_u = \text{diag}(h_{ru})h_{ar}$ and $N_{u}^{DL}$ and $N_{u}^{DL}$ follow complex additive white Gaussian noise (AWGN) with variance $\sigma_1^2$ and $\sigma_2^2$ of each element. Similarly, Bob sends the
orthogonal pilot signal $S_2 \in \mathbb{C}^{M \times T_2}$ in the uplink channel probing, where $T_2$ is the length of pilot and $S_2(S_2)^\dagger = I_{M \times M}$. Bob’s transmit power is also $P$. Thus Alice and Eve $k$ receive

$$Y_a^{UL} = \sqrt{P} \left( h_{ba} + h_{ar}^T \Phi h_{rb}^T \right) S_2 + N_a^{UL} = \sqrt{P} \left( h_{ab}^T + G_b v \right) S_2 + N_a^{UL}$$

(7)

$$Y_e^{UL} = \sqrt{P} \left( h_{be} + h_{re}^T \Phi h_{rb}^T \right) S_2 + N_e^{UL},$$

(8)

where $N_a^{UL}$ is complex AWGN with variance $\sigma_1^2$ of each element due to channel reciprocity, and $N_e^{UL}$ follows complex additive white Gaussian noise (AWGN) $\sigma_2^2$ of each element.

Assuming that the sampling interval is adequately small, the channel reciprocity preserves between the bidirectional pilot transmissions within the coherent time. By the least square (LS) estimation, the combined channels at each respective node after normalization can be expressed as

$$Z_b^{DL} = h_{ab} + v^T G_b + N_b^{DL'},$$

$$Z_e^{UL} = h_{ae}^T + G_b v + N_e^{UL'},$$

(9)

$$Z_{e_1}^{DL} = h_{ae_1} + v^T G_{e_1} + N_{e_1}^{DL'},$$

$$Z_{e_2}^{UL} = h_{be_2} + h_{re}^T \Phi h_{rb}^T + N_{e_2}^{UL'},$$

where the variance of each element in AWGN $N_b^{DL'}$ and $N_e^{UL'}$ are $\sigma_1^2/P$, and in AWGN $N_{e_1}^{DL'}$ and $N_{e_2}^{UL'}$ are $\sigma_2^2/P$ and $\sigma_3^2/P$, respectively. After channel probing, BS and UT vectorize the estimated channel matrices $h_B = \text{vec}(Z_b^{DL})$ and $h_A = \text{vec}(Z_e^{UL})$ to generate the secret key. After employing quantization, information reconciliation and privacy amplification, the BS and UT finally generate the consistent secret key. Similarly, Eves vectorize the estimated channel matrices $h_{E_{e_1}} = \text{vec}(Z_{e_1}^{DL})$, $h_{E_{e_2}} = \text{vec}(Z_{e_2}^{UL})$ to guess the same key.

2.2. Spatial Correlation

When the eavesdropper $k$ is located at least several wavelengths away from the legitimate user, the channels from the IRS to them, $h_{rb}$ and $h_{re}$, are assumed to be independent with each other [23]. Furthermore, when the number of IRS elements is large, the IRS-induced channels $h_{rb} \Phi h_{ar}$ and $h_{re} \Phi h_{ar}$ are statistically independent [24]. However, with the rapid development of communication technology, more and more unattended sensor terminals are put into use in the Internet of Things scenarios, and illegal terminals try to get close to legitimate ones, resulting in the difficulty of ensuring the security of legitimate users at all times. When eavesdroppers are located close to the legitimate users, the corresponding channels $h_{rb}$ and $h_{re}$ may be correlated. We define the correlation coefficient between them as

$$\rho_k = \frac{\mathbb{E} \{ h_{rk} h_{re_k}^H \}}{\sqrt{\mathbb{E} \{ h_{rk} h_{rb}^H \} \mathbb{E} \{ h_{re} h_{re_k}^H \} }$$

(10)

where a larger value of $\rho_k$ implies a higher correlation between channels of the eavesdropper $k$ and legitimate user. The channel correlation in (10) implies that IRS-induced channels $h_{rb} \Phi h_{ar}$ and $h_{re} \Phi h_{ar}$ may be correlated. When eavesdroppers have the same ability, the closer Eve $k$ is to Bob, the higher the correlation between them.

The cross-correlation between the channels corresponding to Eve $k$ and Bob can be expressed as

$$R_k = \mathbb{E} \left\{ \left( h_{ab} + h_{rb} \Phi h_{ar} \right)^T \left( h_{ae} + h_{re} \Phi h_{ar} \right) \right\}$$

$$= \mathbb{E} \left\{ h_{ab}^T h_{ar} \Phi h_{ar} \right\} + \mathbb{E} \left\{ h_{ae}^T \Phi h_{ar} \right\} + \mathbb{E} \left\{ h_{ab}^T \Phi h_{ar} \Phi h_{ar}^T \right\}$$

$$= \mathbb{E} \left\{ h_{ab}^T \Phi h_{ar} \Phi h_{ar}^T \right\}$$

(11)

which will be further analyzed in Section 3 to derive its expression.
3. IRS-Assisted Secret Key Rate Analysis

In this section, a closed-form expression of the secret key capacity for a lower bound is derived. We conservatively take the lower bound capacity as the minimum achievable secret key rate. The lower bound of the key capacity [25] can be expressed as

\[
C(h_A; h_B | h_{E_1}, h_{E_2}) \geq \max \left\{ I(h_A; h_B) - I(h_A; h_{E_1}, h_{E_2}), I(h_A; h_B) - I(h_B; h_{E_1}, h_{E_2}) \right\}
\]

(12)

where \( I( ; ) \) denotes the mutual information.

We assume that Alice and Rose know the statistics of the channel state information (CSI) of all channels. This is a recognized assumption in large-scale wireless networks, in which the eavesdropper is an authorized but untrusted user trying to obtain the information of other users [26]. Below, we derive the lower bound of IRS-assisted secret key capacity. Considering the uplink channel estimation at the Eve side is scalar and poses a small threat to information leakage, we only consider the impact of downlink channel estimations, i.e., \( h_{E_1} \) of Eve on key capacity in this paper. We set \( h_{E_1} = h_{E_2} \). The lower bound is expressed as the maximum of \( C_{k,1} = I(h_A; h_B) - I(h_A; h_{E_1}) \) and \( C_{k,2} = I(h_A; h_B) - I(h_B; h_{E_1}) \), so we derive closed form expressions of \( C_{k,1} \) and \( C_{k,2} \), then select the maximum value as the final expression. First, we express the first term \( C_{k,1} \) as

\[
C_{k,1} = I(h_A; h_B) - I(h_A; h_{E_1}) = H(h_A / h_{E_1}) - H(h_A / h_B) = \log_2 \frac{\det(W_{A E_1}) \det(K_{B B})}{\det(W_{E_1 E_2}) \det(W_{A B})}
\]

(13)

where \( H( ) \) is the information entropy, \( W_{xy} = E\{[h_x, h_y]^T [h_x^H, h_y^H]\} \), \( x, y \in \{A, B, E\} \), and \( K_{xy} = E\{[h_x, h_y]^H\} \) are correlation matrices, and \( \det( ) \) is the determinant of matrix. Furthermore, we can derive

\[
K_{AA} = \mathbb{E}\{h_A h_A^H\}
\]

\[
= \mathbb{E}\left\{ h_{a b}^T h_{a b}^* + h_{a r}^T \Phi h_{a r}^* \Phi H h_{a r}^* + N_a^{U L'} \left( N_a^{U L'} \right)^H \right\}
\]

\[
\overset{②}{=} \frac{\kappa_2}{\kappa_2 + 1} \mathbb{E}\left\{ \left( h_{a r}^T \Phi h_{a r}^* \right) \left( h_{a r}^T \Phi H h_{a r}^* \right) \right\} + \sigma_A^2 I
\]

\[
\overset{③}{=} \frac{\kappa_2}{\kappa_2 + 1} \mathbb{E}\left\{ \left( h_{a r}^T \Phi h_{a r}^* \right) \left( h_{a r}^T \Phi H h_{a r}^* \right) \right\} + \sigma_A^2 I
\]

\[
\overset{④}{=} Q_A(\nu) R_{B S} + \sigma_A^2 I
\]

In Equation (1), we can substitute the expression of \( h_A \). In Equation (2), we substitute \( h_{rb} \) according to Equation (4), and the mean value of NLOS component \( h_{rb} \) is 0. In Equation (4), \( h_{ar} \) and \( \bar{h}_{rb} \) according to Equations (1) and (5) are substituted and calculated by matrix multiplication. \( \sigma_A^2 = \sigma_{h_{rb}}^2 + \sigma_1^2 / P \) and \( Q_A(\nu) \) can be expressed as

\[
Q_A(\nu) = \frac{\kappa_2}{\kappa_2 + 1} \left| \eta_1 \eta_2 \right|^2 \nu^H \beta^H \beta \nu
\]

(15)

The vector \( \beta \) is given as

\[
\beta = [1, \ldots, e^{T_{x,y}(\theta_{IRS} + \gamma_{IRS})} + T_{x,y}(\gamma_{IRS} + \theta_{IRS}), \ldots, e^{T_{x,y}(\theta_{IRS} + \gamma_{IRS})} + T_{x,y}(\gamma_{IRS} + \theta_{IRS})]
\]

(16)

where \( T_{x,y}(\theta, \gamma) \) is defined as

\[
T_{x,y}(\theta, \gamma) = e^{2 \pi \frac{\pi}{2} \left( x - 1 \right) \sin \delta \sin \gamma + (y - 1) \cos \gamma}.
\]

(17)
We define matrix $\mathbf{R}_{BS} = \mathbb{E}\left\{[\mathbf{a}_{BS}(\mathbf{q}_{BS})^*\mathbf{a}_{BS}(\mathbf{q}_{BS})]^T\right\}$, the rank of which is equal to 1.

It can also be derived that $\mathbf{K}_{BB} = \mathbf{K}_{AA} = Q_{A}(\mathbf{v})\mathbf{R}_{BS} + \sigma_{A}^2\mathbf{I}, \mathbf{K}_{AB} = \mathbf{K}_{BA} = Q_{A}(\mathbf{v})\mathbf{R}_{BS} + \sigma_{AB}^2\mathbf{I}.$

Similarly, we can get $\mathbf{K}_{E_{i}A} = \mathbf{K}_{AE_{i}} = \mathbb{E}\{\mathbf{h}_{E_{i}}\mathbf{h}_{E_{i}}^H\} = \mathbf{R}_{E_{i}}$, where $\mathbf{R}_{E_{i}}$ is the cross-correlation between the channels corresponding to Eve $k$ and Bob. We derive $\mathbf{R}_{E_{i}}$ as

$$\mathbf{K}_{E_{i}A} = \mathbf{K}_{AE_{i}} = \mathbf{R}_{E_{i}} = R_{AE_{i}}(\mathbf{v})\mathbf{R}_{BS} \tag{18}$$

where $R_{AE_{i}}(\mathbf{v})$ and $\psi$ can be denoted as

$$R_{AE_{i}}(\mathbf{v}) = \sqrt{\frac{k_2 \cdot k_3}{(k_2 + 1)(k_3 + 1)}}\eta_1^2\eta_2^2\mathbf{v}^H\psi\mathbf{v} \tag{19}$$

$$\psi = [1, \cdots, e^{-r_{v,k}(\mathbf{q}_{BS}/\mathbf{R}_{BS})}, e^{-r_{E_{i},k}(\mathbf{q}_{IRS,E_{i}})}, \cdots]^T \tag{20}$$

Similarly, we get $\mathbf{K}_{E_{i}E_{i}} = \mathbb{E}\{\mathbf{h}_{E_{i}}\mathbf{h}_{E_{i}}^H\} = Q_{E_{i}}(\mathbf{v})\mathbf{R}_{BS} + \sigma_{E_{i}}^2\mathbf{I},$ where $Q_{E_{i}}(\mathbf{v}) = \frac{k_2}{k_2 + 1}|\eta_1\eta_3|^2\mathbf{v}^H\psi\mathbf{v}, \sigma_{E_{i}}^2 = \sigma_{AB}^2 + \sigma_{E_{i}}^2/\delta$. Thus, the determinant of matrix terms $\mathbf{W}_{AE_{i}}$ and $\mathbf{W}_{AB}$ in (11) can be expressed as

$$\det(\mathbf{W}_{AE_{i}}) = \det(\mathbf{K}_{AA}) \cdot \det(\mathbf{K}_{E_{i}E_{i}} - \mathbf{K}_{AE_{i}}\mathbf{K}_{AA}^{-1}\mathbf{K}_{AE_{i}}) \tag{21}$$

$$\det(\mathbf{W}_{AB}) = \det(\mathbf{K}_{AA}) \cdot \det(\mathbf{K}_{BB} - \mathbf{K}_{AB}\mathbf{K}_{AA}^{-1}\mathbf{K}_{AB}) \tag{22}$$

We substitute $\det(\mathbf{W}_{AE_{i}}), \det(\mathbf{W}_{BB}), \det(\mathbf{W}_{E_{i}E_{i}})$ and $\det(\mathbf{W}_{AB})$ into Equation (11) above. Because $Q_{A}(\mathbf{v}), R_{AE_{i}}(\mathbf{v}),$ and $Q_{E_{i}}(\mathbf{v})$ are all scalars, the ranks of $Q_{A}(\mathbf{v})\mathbf{R}_{BS}, R_{AE_{i}}(\mathbf{v})\mathbf{R}_{BS},$ and $Q_{E_{i}}(\mathbf{v})\mathbf{R}_{BS}$ are also equal to 1, which means that they all have, at most, one non-zero eigenvalue. Therefore, we can take advantage of this property that the determinant of a determined matrix is equal to the product of all eigenvalues of the matrix.

**Theorem 1.** For Eve $k$, the achievable secret key capacity $C_{k,1}$ in IRS-assisted wireless networks is calculated as

$$C_{k,1} = \log_2 \left( \frac{(MQ_{E_{i}}(\mathbf{v}) + \sigma_{E_{i}}^2)(MQ_{E_{i}}(\mathbf{v}) + \sigma_{E_{i}}^2)^2 - M^2R_{AE_{i}}(\mathbf{v})^2(MQ_{A}(\mathbf{v}) + \sigma_{A}^2)}{(MQ_{E_{i}}(\mathbf{v}) + \sigma_{E_{i}}^2)(2MQ_{A}(\mathbf{v}) + \sigma_{A}^2 + \sigma_{AB}^2)} \right) \tag{23}$$

where $f_{E_{i}}(\mathbf{v}) = M^3Q_{A}(\mathbf{v})^2Q_{E_{i}}(\mathbf{v}) - M^2Q_{A}(\mathbf{v})Q_{E_{i}}(\mathbf{v})^2 + 2M^2\sigma_{A}^2Q_{A}(\mathbf{v})Q_{E_{i}}(\mathbf{v}) + M^2\sigma_{E_{i}}^2Q_{A}(\mathbf{v})^2 - M^2\sigma_{A}^2R_{AE_{i}}(\mathbf{v})^2 + 2M\sigma_{A}^2\sigma_{E_{i}}^2Q_{A}(\mathbf{v}) + M\sigma_{A}^4Q_{E_{i}}(\mathbf{v}) + \sigma_{A}^4\sigma_{E_{i}}^2$ and $h_{E}(\mathbf{v}) = 2M^2Q_{A}(\mathbf{v})Q_{E_{i}}(\mathbf{v}) + M(c_{A}^2 + \sigma_{AB}^2)Q_{E_{i}}(\mathbf{v})^2 + 2M\sigma_{A}\sigma_{E_{i}}^2Q_{A}(\mathbf{v}) + (c_{A}^2 + \sigma_{AB}^2)\sigma_{E_{i}}^2$.

**Proof of Theorem 1.** Because the rank of $\mathbf{R}_{BS}$ is 1, it has only one non-zero eigenvalue, which can be denoted as $\lambda_{M}(\mathbf{R}_{BS}), \lambda_{M}(\mathbf{R}_{BS}) = \lambda_{M}(\mathbf{R}_{BS}) = M$. Therefore, we can have $\sum_{i=1}^{M} \lambda_{i}(Q_{A}(\mathbf{v})\mathbf{R}_{BS}) = \lambda_{M}(Q_{A}(\mathbf{v})\mathbf{R}_{BS}) = MQ_{A}(\mathbf{v})$, and thus we can deduce that the matrix $Q_{A}(\mathbf{v})\mathbf{R}_{BS} + \sigma_{A}^2\mathbf{I}$ has $M - 1$ identical eigenvalue $\sigma_{A}^2$, the $M$ eigenvalue is $MQ_{A}(\mathbf{v}) + \sigma_{A}^2$. Then we utilize the properties that the determinant of a given matrix can be expressed as the product of all eigenvalues of the matrix. Therefore, $\det(Q_{A}(\mathbf{v})\mathbf{R}_{BS} + \sigma_{A}^2\mathbf{I}) = \prod_{i=1}^{M} \lambda_{i}(Q_{A}(\mathbf{v})\mathbf{R}_{BS} + \sigma_{A}^2\mathbf{I}) = (\sigma_{A}^2)^{M-1}(MQ_{A}(\mathbf{v}) + \sigma_{A}^2)$, where $\lambda_{i}(\cdot)$ means the $i$-th eigen-
value of the matrix. The determinant of the other three matrix terms can be calculated similarly, which completes the verification. □

We can prove that $C_{k,2} = C_{k,1}$ due to the reciprocal assumption of uplink and downlink.

4. Proposed Optimization Scheme and Solution

4.1. Optimization Analysis

From the above analysis, we can see the reflection coefficient vector $v$ of IRS leads to the correlation between the legitimate channel and the eavesdropping channel. Therefore, we can design $v$ to maximize the secret key capacity. We can see that key capacity is the minimum secret key capacity $C_{k,1}$ against all the eavesdroppers. A low-complexity optimization scheme is designed to decide the $N$-element reflecting coefficients of Rose to maximize the key capacity. We can formulate the optimization problem as follows:

$$\max_{v} \min_{k \in K} C_{k,1} \quad s.t. \quad |v_n|^2 \leq 1, n = 1, \cdots, N,$$

(24)

where $K = \{1, \cdots, K\}$. The function $\log_2(\cdot)$ is monotonically increasing in (23). Accordingly, the optimization formulation (23) can be further described as

$$\max_{v} \min_{k \in K} \frac{f_k(v)}{h_k(v)} s.t. |v_n|^2 \leq 1, n = 1, \cdots, N.$$

(25)

Due to the max–min operations, the objective function in (25) is non-convex. As described below, we use an auxiliary variable $Q$ to transform the optimization problem as

$$\max_{v, Q} \min_{k \in K} f_k(v) - h_k(v) \leq 0, k = 1, \cdots, K.$$

(26)

We can transform $h_k(v)$ and $f_k(v)$ into function expressions $f_k(V)$ and $h_k(V)$. We can now see that $f_k(V)$ and $h_k(V)$ are both convex with regard to variable $V$. The optimization problem can be re-formulated as

$$\max_{v, Q} \min_{k \in K} f_k(V) - h_k(V) \leq 0, k = 1, \cdots, K.$$

(27)
wireless transmission, it is easier to expose eavesdroppers’ identities. We consider partially which can be solved by alternatively optimizing $Q$. Therefore, the original constraint condition $Q \cdot h_k(V) - f_k(V) \leq 0$ can be decomposed into multiple convex subproblems by linearizing the concave term $-f_k(V)$. We successfully transformed the IRS optimization problem in (27) into a convex optimization problem, which can be solved by alternatively optimizing $Q$ and $V$.

Algorithm 1 presents the details of the proposed SDR and CCP based algorithm. The matrix $V$ we obtain is not necessarily rank-1, so we can recover $v$ from $V$ with the help of the Gaussian randomization method. $\epsilon$ denotes a small convergence threshold, and $Q_{\text{max}}$ is a sufficiently large number. Note that the proposed SDR-CCP based algorithm can solve the problem with a worst-case complexity of $O\left(\max\{N, K\}^4 N^{1/2} \bar{L} \log(Q_{\text{max}}/\epsilon)\right)$, where $\bar{L}$ is the average number of iterations. The SDR-CCP algorithm is more efficient than the standard branch-and-bound algorithm with the exponential complexity of $O\left((1/\delta_A\delta_\beta)^{KN}\right)$ in solving problem (27), where $\delta_A$ and $\delta_\beta$ are the discrete quantization intervals of amplitude and phase, respectively.

Algorithm 1 Our algorithm based on SDR and CCP.

Input: $\sigma_A^2, \sigma_E^2, \sigma_{\theta_k}^2, \eta_1, \eta_2, \eta_3, \beta, \Psi, M, \epsilon, Q_{\text{max}}$

Output: $V, Q$

1: Initialize $Q_{\text{min}} = 0$, and Set $Q^{(1)} = (Q_{\text{max}} + Q_{\text{min}})/2$.
2: repeat (Bisection Search for $Q$)
3: \quad repeat (Our algorithm based on SDR and CCP)
4: \quad \quad For given $Q^{(t)}$, when $q = 1$, initialize a positive semi-definite matrix $V^{(1)}$ randomly; when
5: \quad \quad $q > 1$, given $V^{(q)}$, solve the above optimization problem (28) for $V^{q+1}$.
6: \quad \quad Update $q = q + 1$.
7: \quad until the optimization variable $V$ reaches convergence.
8: \quad Record $V_{\text{opt}} = V^{(q)}$ of the current iteration if the above problem can be solved, then update
9: \quad $Q_{\text{min}} = Q^{(q)}$; if $Q^{(q)}$ is unreachable, then update $Q_{\text{max}} = Q^{(q)}$
10: until $Q_{\text{max}} - Q_{\text{min}} < \epsilon$.
11: Recover $v$ from $V_{\text{opt}}$ by Gaussian randomization.

4.2. Partially Colluding and Fully Colluding Cases

For colluding eavesdropping, all colluding eavesdroppers transmit signals wirelessly to an additional channel signal processor, which also incurs high costs. In the process of wireless transmission, it is easier to expose eavesdroppers’ identities. We consider partially and fully colluding cases, in which the SNR received by the signal processor is the sum of all eavesdroppers’ SNRs. The optimization objective is $\max \sum_{k=1}^{X} C_{k,1}$, where $X$ is the number of colluding eavesdroppers. When $X = K$, it is fully colluding. We solve this optimization problem based on the SDR and successive convex approximation (SCA) methods [24].

4.3. Discussion on Active Pilot Attacks

We studied an IRS-assisted key generation scheme against multiple correlated eavesdroppers under the assumption of passive attacks. Next, we discuss the possibility of the
The proposed scheme to resist a simple active attack, where the eavesdroppers transmit pilots at the same time that the legitated user is transmitting [27]. In this case, eavesdroppers transmit the same probing signals as those of the legitated user in the uplink to prevent Alice and Bob from obtaining similar channel estimates. Under this attack, Alice obtains the uplink channel estimation as

$$Z_a^{UL} = h_{ab}^T + G_b^T v + \sum_k \left( h_{aq_k}^T + G_{q_k}^T v \right) + N_a^{UL}$$  \hspace{1cm} (29)$$

while in the downlink, Bob estimates the channel as

$$Z_b^{DL} = h_{ab} + v^T G_b + N_b^{DL}$$  \hspace{1cm} (30)$$

From (29) and (30), the channel estimates of Alice and Bob are different, leading to the failure of consistent keys generated. However, as mentioned above, we deploy the IRS to enhance the legitimate user’s channel and deteriorate the channel quality of eavesdroppers. We elaborate on designing the reflection coefficient matrix of the IRS, greatly weakening the eavesdropping channels. Thus, the eavesdroppers’ signals can be ignored. Alice and Bob can still obtain similar channel estimates and generate secret keys under the pilot spoofing attack. To summarize, the proposed scheme can counteract this attack by elaborately designing the IRS phase shift.

5. Simulation Analysis

As shown in Figure 2, a network deployment where Alice, Bob, and the central point of IRS are located at $(5, 0, 25)$, $(2, 100, 0)$, and $(0, 100, 25)$ is considered. We set up the following simulation parameters according to [17,28]. $K$ Eves are randomly distributed in a circle of radius $R$ centered on Bob. The carrier frequency is set to 1 GHz. IRS configuration is a uniform planar rectangular array (URA) with 5 rows and $N/5$ columns, and $\lambda/2$ spacing. The constant path loss term is $PL_0 = -20$ dB at reference distance $d_0 = 1$ m. Since there are extensive obstacles as well as scatters in the channel links from the BS to the user, we set the path loss exponent $c_{ab} = c_{ae_k} = 4.5$; meanwhile, we set $c_{ar} = 3.7$, $c_{rh} = c_{re_k} = c_{be_k} = 2.2$. The other parameters are set as $\sigma_A^2 = \sigma_{b_k}^2 = -80$ dB, $\sigma_{h_{ab}}^2 = -50$ dB, $M = 4$, $N = 20$, $K = 3$, $R = \lambda$, and Rician $\kappa$-factor $\kappa = 1$, if not specified otherwise. The maximum correlation coefficient $\rho$ among all Eves is 0.5 unless otherwise specified. Three benchmark schemes are presented: (1) the secret key capacity of key generation from correlated wireless channels without IRS (N-IRS) [29]; (2) an IRS-aided system with on-off switching states (On-off IRS) [19]; (3) an IRS-aided system with random phase shifts (R-IRS) [20].

![Figure 2. Simulation setup.](image-url)

Figure 3 shows the secret key capacity versus the number of IRS elements $N$. We see that increasing the size of the IRS results in a significant improvement in the secret key capacity of our SDR-CCP scheme. Furthermore, we observe that our scheme with optimal IRS phase shifting outperforms the three benchmark schemes for the entire range.
of $N$, because the SNR of the legitimate user is improved by elaborately designing the phase shift matrix of the IRS. Secret key capacity increases with decreasing Rician $\kappa$-factor $\kappa_{rb} = \kappa_{re} = \kappa$ because a lower $\kappa$ corresponding to a stronger NLoS path provides more randomness in the wireless channels.

![Figure 3](image-url)  
**Figure 3.** Achievable secret key capacity versus the number of IRS reflecting elements $N$ with $P = 20$ dBm.

In Figure 4, we note that the achievable secret key capacity reduces with an increasing number of Eves. We also see that our proposed scheme significantly outperforms the three benchmark schemes by at least 0.3 bps. We observe that the increasing number of Eves has only a small negative impact on the performance of our SDR-CCP scheme. As we know, due to a greater average distance between the eavesdroppers with $R = \lambda$, the secret key capacity increases.

![Figure 4](image-url)  
**Figure 4.** Achievable secret key capacity versus the number of eavesdroppers.

In Figure 5, the secret key capacity of our proposed SDR-CCP scheme is significantly improved with the increase of transmission power $P$, because the channel estimation accuracy at Bob is greatly improved; instead, Eve’s SNR is severely reduced through the design of the IRS phase shift. We consider the MRT precoding strategy used by the
transmitting antenna for Bob as a comparison. The MRT scheme without an IRS (N-IRS-MRT) can increase the system’s secret key capacity compared with N-IRS and R-IRS because the base station uses MRT to improve Bob’s SNR. Even if the IRS phase shift is randomly set, MRT (R-IRS-MRT) can improve Bob’s SNR and secret key capacity compared with R-IRS. For the N-IRS and R-IRS, the SNR of Eve is also improved with the increase of $P$, which increases the risk of information leakage. It can be seen that the increase of secret key capacity based on MRT and SDR-CCP is not significant, because IRS has brought a great increase to Bob’s SNR.

![Figure 5. Achievable secret key capacity versus different transmission power $P$.](image)

Figure 6 compares the secret key capacity obtained as a function of the channel correlation coefficient $\rho$. The solutions of the algorithm in [18] are obtained by optimizing the IRS configuration under the assumption of independent channels. Then, the optimal solutions obtained are substituted into the expression of (23). As expected, our SDR-CCP outperforms the algorithm in [18], which assumes independent Eves, in the considered range. In particular, as the channel correlation coefficient increases from 0.2 to 0.8, the key capacity becomes smaller. Figure 6 confirms that the secret key capacity can be enhanced if the channel correlation is considered at the design stage.
In Figure 7, it is assumed that the transmission power of each antenna is 5dBm. It can be seen that the secret key capacity can be improved by increasing the number of transmitting antennas and IRS elements with our proposed SDR-CCP scheme. For example, the case of $M = 4$, $N = 40$ and $M = 6$, $N = 30$ can achieve the same secret key capacity, which means we can reduce the number of transmitting antennas by increasing IRS elements and reduce the hardware costs of transmitting antennas.

Figure 7. Achievable secret key capacity versus $N$ with different $M$.

Figure 8 demonstrates the comparison over the non-colluding, partially colluding, and fully colluding cases. We assume $K = 6$ eavesdroppers exist. We consider the influence of the number of colluding eavesdroppers on the secret key capacity in the colluding eavesdropping scenario. It is observed that the risk of leakage becomes larger for a greater number of colluding eavesdroppers, where $X = 2, 4, 6$ (fully colluding), which causes a greater security threat than non-colluding eavesdroppers. In particular, the secret key...
capacity gap becomes more distinct over the non-colluding, partially colluding, and fully colluding cases for higher transmitting power $P$.

![Figure 8. Comparison of the secret key capacity for different numbers of colluding eavesdroppers with different $P$.](image)

6. Conclusions

This paper proposes an IRS-assisted key generation scheme in a MISO system against multiple correlated eavesdroppers. The secret key capacity of the system is maximized by elaborately optimizing the reflection coefficient matrix of IRS. We formulate and solve an optimization problem to obtain the optimal IRS configuration based on SDR and CCP. We find that the same secret key capacity is obtained by reducing the number of transmitting antennas at the cost of increasing the number of IRS elements, which reduced the hardware costs of antennas. The numerical results demonstrated that the proposed scheme provides the highest secret key capacity as compared with other existing benchmark schemes.

Author Contributions: Conceptualization, K.H.; methodology, X.S.; software, Y.L.; validation, X.S., Y.L. and S.Y.; writing—original draft preparation, Y.L.; writing—review and editing, Y.L. and L.W.; funding acquisition, K.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China, grant number 61871404.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ylianttila, M.; Kantola, R.; Gurtov, A.; Mucchi, L.; Oppermann, I.; Yan, Z.; Nguyen, T.H.; Liu, F.; Hewa, T.; Liyanage, M.; et al. 6G white paper: Research challenges for trust, security and privacy. arXiv 2020, arXiv:2004.11665.
2. Zhang, H.; Ji, Z.; Wang, H.; Wu, W. Survey on quantum information security. China Commun. 2019, 16, 1–36. [CrossRef]
3. Maurer, U.M. Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory 1993, 39, 733–742. [CrossRef]
4. Li, G.; Zhang, Z.; Zhang, J.; Hu, A. Encrypting Wireless Communications on the Fly Using One-Time Pad and Key Generation. IEEE Internet Things J. 2021, 8, 357–369. [CrossRef]
5. Li, G.; Sun, C.; Zhang, J.; Jorswieck, E.; Xiao, B.; Hu, A. Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities. Entropy 2019, 21, 497. [CrossRef]
6. Zeng, K. Physical layer key generation in wireless networks: Challenges and opportunities. IEEE Commun. Mag. 2015, 53, 33–39. [CrossRef]
7. You, X.; Wang, C.-X.; Huang, J.; Gao, X.; Zhang, Z.; Wang, M.; Huang, Y.; Zhang, C.; Jiang, Y.; Wang, J.; et al. Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. Sci. China Inf. Sci. 2021, 64, 110301. [CrossRef]
8. Wallace, J. Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits. In Proceedings of the 2009 IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009; pp. 1–5. [CrossRef]
9. Huth, C.; Guillaume, R.; Strohm, T.; Duplys, P.; Samuel, I.A.; Güneysu, T. Information reconciliation schemes in physical-layer security: A survey. Comput. Netw. 2016, 109, 84–104. [CrossRef]
10. Bennett, C.; Brassard, G.; Crepeau, C.; Maurer, U. Generalized privacy amplification. IEEE Trans. Inf. Theory 1995, 41, 1915–1923. [CrossRef]
11. Wang, Z.; Cao, Y.; Zhang, D.; Hua, X.; Gao, P.; Jiang, T. User Selection for MIMO Downlink With Digital and Hybrid Maximum Ratio Transmission. IEEE Trans. Veh. Technol. 2021, 70, 11101–11105. [CrossRef]
12. Wu, Q.; Zhang, R. Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network. IEEE Commun. Mag. 2020, 58, 106–112. [CrossRef]
13. Wu, Q.; Zhang, R. Beamforming Optimization for Wireless Network Aided by Intelligent Reflecting Surface with Discrete Phase Shifts. IEEE Trans. Commun. 2020, 68, 1838–1851. [CrossRef]
14. Abeywickrama, S.; Zhang, R.; Wu, Q.; Yuen, C. Intelligent Reflecting Surface: Practical Phase Shift Model and Beamforming Optimization. IEEE Trans. Commun. 2020, 68, 5849–5863. [CrossRef]
15. Liu, F.; Tsilipakos, O.; Pitilakis, A.; Tasolamprou, A.C.; Mirmoosa, M.S.; Kantartzis, N.V.; Kwon, D.-H.; Georgiou, J.; Kossifos, K.; Antoniades, M.A.; et al. Intelligent metasurfaces with continuously tunable local surface impedance for multiple reconfigurable functions. Phys. Rev. Appl. 2019, 11, 044024. [CrossRef]
16. Chen, L.; Hu, W.; Jamieson, K.; Chen, X.; Fang, D.; Gummerson, J. Pushing the physical limits of IoT devices with pro-grammable metasurfaces. In Proceedings of the 18th Symposium on Networked Systems Design and Implementation, Boston, MA, USA, 12–14 April 2021.
17. Ji, Z.; Yeoh, P.L.; Zhang, D.; Chen, G.; Zhang, Y.; He, Z.; Yin, H.; Li, Y. Secret Key Generation for Intelligent Reflecting Surface Assisted Wireless Communication Networks. IEEE Trans. Veh. Technol. 2021, 70, 1030–1034. [CrossRef]
18. Hu, X.; Jin, L.; Huang, K.; Sun, X.; Zhou, Y.; Qu, J. Intelligent Reflecting Surface-Assisted Secret Key Generation With Discrete Phase Shifts in Static Environment. IEEE Wirel. Commun. Lett. 2021, 10, 1867–1870. [CrossRef]
19. Lu, X.; Lei, J.; Shi, Y.; Li, W. Intelligent Reflecting Surface Assisted Secret Key Generation. IEEE Signal Process. Lett. 2021, 28, 1036–1040. [CrossRef]
20. Staat, P.; Elders-Boll, H.; Heinrichs, M.; Kronberger, R.; Zenger, C.; Paar, C. Intelligent Reflecting Surface-Assisted Wireless Key Generation for Low-Entropy Environments. In Proceedings of the 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Helsinki, Finland, 13–16 September 2021; pp. 745–751. [CrossRef]
21. Hoang, T.M.; Dung, L.T.; Nguyen, B.C.; Tran, X.N.; Kim, T. Secrecy Outage Performance of FD-NOMA Relay System With Multiple Non-Colluding Eavesdroppers. IEEE Trans. Veh. Technol. 2021, 70, 12985–12997. [CrossRef]
22. Wang, P.; Fang, J.; Duan, H.; Li, H. Compressed Channel Estimation for Intelligent Reflecting Surface-Assisted Millimeter Wave Systems. IEEE Signal Process. Lett. 2020, 27, 905–909. [CrossRef]
23. Li, G.; Hu, A.; Zhang, J.; Peng, L.; Sun, C.; Cao, D. High-Agreement Uncorrelated Secret Key Generation Based on Principal Component Analysis Preprocessing. IEEE Trans. Commun. 2018, 66, 3022–3034. [CrossRef]
24. Li, G.; Sun, C.; Xu, W.; Di Renzo, M.; Hu, A. On Maximizing the Sum Secret Key Rate for Reconfigurable Intelligent Surface-Assisted Multiuser Systems. IEEE Trans. Inf. Forensics Secur. 2022, 17, 211–225. [CrossRef]
25. Thai, C.D.T.; Lee, J.; Quek, T.Q.S. Physical-Layer Secret Key Generation with Colluding Untrusted Relays. IEEE Trans. Wirel. Commun. 2016, 15, 1517–1530. [CrossRef]
26. Chen, G.; Gong, Y.; Xiao, P.; Chambers, J.A. Physical Layer Network Security in the Full-Duplex Relay System. IEEE Trans. Inf. Forensics Secur. 2015, 10, 574–583. [CrossRef]
27. Sun, C.; Li, G. Power Allocation and Beam Scheduling for Multi-User Massive MIMO Secret Key Generation. IEEE Access 2020, 8, 164580–164592. [CrossRef]
28. Guan, X.; Wu, Q.; Zhang, R. Intelligent Reflecting Surface Assisted Secrecy Communication: Is Artificial Noise Helpful or Not? IEEE Wirel. Commun. Lett. 2020, 9, 778–782. [CrossRef]
29. Zhang, J.; He, B.; Duong, T.Q.; Woods, R. On the Key Generation from Correlated Wireless Channels. IEEE Commun. Lett. 2017, 21, 961–964. [CrossRef]