Secret Key Generation Assisted by Intelligent Reflecting Surface with Discrete Phase Shift in Static Environment

Xiaoyan Hu, Liang Jin*, Kaizhi Huang, Xiaoli Sun and Keming ma
PLA Strategic Support Force Information Engineering University,
Zhengzhou, China
Email: {liangjin}@263.net

Abstract—Physical layer secret key generation is a promising candidate to achieve one-time-pad encryption approach for wireless communication system. The main issue of this method is the insufficient secret key rate. Especially in a static environment, the entropy of the channel complex coefficient is limited due to the lack of channel time-variation. To solve the problem, this paper proposes a novel secret key generation scheme assisted by intelligent reflecting surface (IRS) with discrete phase. We construct a dynamic time-varying channel by switching the phase of the reflection elements rapidly and randomly, and use channel estimation samples to update the secret key. Based on the common IRS channel model, we derive the expression of secret key rate. Monte Carlo simulation and numerical results show that the scheme can update secret key even if the channel coefficient is constant, and the secret key rate is higher than schemes based on artificial random signal. In addition, we comprehensively analyze the influence of various factors, such as the number of reflection elements and the IRS switching frequency on the secret key rate.

Keywords—wireless communication, physical layer security, secret key generation, intelligent reflecting surface, secret key rate

I. INTRODUCTION

Wireless communication is vulnerable to be eavesdropped due to broadcasting. As a supplement to the existing symmetric-key encryption schemes, the physical layer secret key generation (SKG) technology has attracted wide research [1]. The SKG use channel characteristics, such as Channel State Information (CSI), Received Signal Strength (RSS) and Channel Impulse Response (CIR) as common random sources to generate secret keys [2]. Due to the inherent characteristics of wireless channels (i.e., reciprocity, spatial decorrelation, and temporal variation), the key generated from CSI at two legitimate nodes is highly correlated and changing quickly, and is unknown to eavesdroppers outside the half wavelength. However, in the static environment with a long channel coherence time, the time-varying nature of the channel may be insufficient, resulting in a low secret key rate [3].

To solve this problem, the methods of deploying more communication devices (e.g., more relays [4] or antennas[5]) to obtain more CSI samples have been widely proposed, but they obviously increase the cost. In other work, artificial randomness (e.g., random precoding matrix [6] [7] or random signal [8] [9]) is introduced to improve the entropy of CSI samples. However, since the channel coefficient is constant, the artificial random signal is easy to be predicted by eavesdroppers, and the key rate is still limited [10]. Therefore, it is still an open issue to update keys rapidly with low cost in static environment.

The intelligent reflecting surface (IRS) assisted wireless communication has been proved to be a promising solution to ameliorate the channel environment [11]. By adjusting the phase shift of low-cost reconfigurable passive elements (e.g., printed dipoles) in IRS, the signals of multiple reflected paths

at the receiver are coherently added, thereby improving the received signal-to-noise ratio (SNR) [12]. However, the existing IRS-assisted communication methods only increases the received power, but does not fundamentally change the fact of static channels, so they have limited contribution to SKG. Different from the traditional usage, this paper focuses on developing a novel IRS utilization method for SKG, that is, using IRS to construct a dynamic channel to overcome the problem of low secret key rate in static environment. The phase shift of the IRS elements switch rapidly and randomly, and legitimate nodes send pilots to obtain fast-changing CSI. We designed the SKG process for two different scenarios, and then derive the expressions of the exact secret key rate, and the asymptotic secret key rate when the number of IRS elements tends to infinity. Finally, we perform Monte Carlo simulation to verify the derivation. The results show that our scheme is superior to the comparison schemes in [8] and [9] based on artificial random signal, and the optimal switching time should be adjusted according to pilot power.

The rest of this paper is organized as follows. Section II introduces the system model and the IRS configuration of the proposed scheme. Section III evaluates the secret key rate. Section IV presents simulation and numerical results. Section V concludes the paper

II. SYSTEM MODEL

A. Channel Model

As shown in Fig. 1, we consider a common SKG channel model in static environment, where Alice, Bob and Carlo are legal nodes. The main difference of this channel model is that there is an IRS composed of N reflection elements, and the reflective elements of the IRS can be programmed by the IRS controller Carol through a wired control link. There is also a passive eavesdropper named Eve, who eavesdrops on a wiretap channel independent of the legitimate channel. They all equipped with a single antenna, and the wireless channels are modeled as quasi-static flat block fading channels [4], which means channel coefficients are independent and identically distributed (i.i.d.) circularly symmetric complex Gaussian random variables with zero mean, and they remain constant over each period of the coherence time T_c . For ease of analysis, the channel between U and V is denoted as h_{UV} , where $U, V \in \{A, B, C, E\}$ and $\{A, B, C, E\}$ denote Alice, Bob, Carol and Eve, respectively.

Fig. 1. Channel model

To accommodate different types of communication, we consider two SKG modes. Fig. 1(a) and Fig. 1(b) respectively show the process of pilots transmission between Alice and Bob, Alice and Carlo for SKG. Let $h_{UV,d}$, $\mathbf{g}_{Ur} = [g_{Ur,1}, \dots, g_{Ur,N}]^T \in \mathbb{C}^{1 \times N}$, $\mathbf{h}_{rV}^H = [h_{rV,1}^*, \dots, h_{rV,N}^*] \in \mathbb{C}^{N \times 1}$ denote the channels from the communicating party U to V , from U to IRS, and from the IRS to V , respectively, where $\mathbb{C}^{x \times y}$ represents a $x \times y$ complex matrix. Then, the channel between any two communicating parties is given by

$$\begin{aligned} h_{UV} &= h_{UV,d} + \mathbf{h}_{rV}^H \mathbf{\Theta} \mathbf{g}_{Ur} \\ &= \sum_n e^{j\theta_n} g_{Ur,n} h_{rV,n}^* + h_{UV,d} \end{aligned} \quad (1)$$

where $\mathbf{\Theta} = \text{diag}(\beta e^{j\theta_1}, \beta e^{j\theta_2}, \dots, \beta e^{j\theta_N})$ denotes the reflection coefficient vector of the IRS. Due to channel reciprocity, we have $h_{UV} = h_{VU}$ and $\mathbf{h}_{rU} = \mathbf{g}_{Ur}$. Assumed that the power gain of the combined channel h_{UV} is $2\sigma_h^2$, the power gain of $h_{UV,d}$ is $2\sigma_h^2(1-\rho)$, and the power gain of the $\mathbf{h}_{rV}^H \mathbf{\Theta} \mathbf{g}_{Ur}$ is $2\sigma_h^2\rho$, where ρ is the power ratio of the IRS reflection channel. Note that the cascade channel, i.e. $\mathbf{h}_{rV}^H \mathbf{\Theta} \mathbf{g}_{Ur}$, is equally divided into N reflection channels. Since the path loss is space-related and is easy to be predicted by eavesdroppers, it is ignored as many SKG studies [2] [13].

Note that different from the traditional SKG model, we deploy Carlo to change $\mathbf{\Theta}$ by switching the phase of the IRS elements quickly and randomly, and increase the entropy of the combined channel, i.e., h_{UV} .

B. IRS Configuration

We consider a common discrete phase shift IRS model with $\beta = 1$, and the phase shift has K values to be adjusted, which can be obtained by uniformly quantifying the interval $[0, 2\pi)$. Then the sets of discrete reflection phase shifts at each element of IRS can be expressed as

$$\mathcal{K}_\theta = \left\{ 0, \frac{2\pi}{K}, \dots, \frac{2\pi(k-1)}{K}, \dots, \frac{2\pi(K-1)}{K} \right\} \quad (2)$$

where $k = 1, 2, \dots, K$. When K tends to infinity, it can be approximately considered that the value of the phase shift is continuous. According to [14], the switching frequency of the discrete phase can be performed within 1 microsecond at the fastest, which is conducive to the construction of dynamic channel with low cost.

III. SECRET KEY GENERATION SCHEMES

In this section, we design two IRS-assisted SKG schemes for the communication scenarios shown in Fig. 1. Scheme 1 is an improvement of the classic point-to-point SKG in Fig. 1(a) based on the common IRS channel model. Scheme 2 is a novel SKG scheme for the communication process dominated by the IRS controller Carlo in Fig. 1(b).

A. Scheme 1

In scheme 1, the legitimate communication parties Alice and Bob send pilot signals to estimate the channel coefficients and cooperatively generate secret keys. As the controller of the IRS, Carlo does not participate in this process, only change the phase of the IRS randomly to construct a dynamic channel. The specific step is as follows: (i) Alice and Bob send pilots to each other in the same coherent time. Meanwhile, Carlo randomly switches the IRS phase and ensures that the interval of switching is less than the interval of each round of pilot transmission, i.e., the phase of the IRS is different during each channel estimation. (ii) Alice and Bob estimate the wireless channel coefficients of the combined channel based on pilots. Then, due to (1) and the channel reciprocity, the estimation results of Alice and Bob can be expressed as

$$\begin{cases} \hat{h}_A = h_{AB} + n_A = \sum_n e^{j\theta_n} g_{Ar,n} h_{rB,n}^* + h_{AB,d} + n_A \\ \hat{h}_B = h_{AB} + n_B = \sum_n e^{j\theta_n} g_{Ar,n} h_{rB,n}^* + h_{AB,d} + n_B \end{cases} \quad (3)$$

where $n_A \sim \mathcal{CN}(0, 2\sigma_n^2 / P_B T_s)$ and $n_B \sim \mathcal{CN}(0, 2\sigma_n^2 / P_A T_s)$ denotes the estimation error of employing zero forcing channel estimation [4] [13], P_A and P_B are the pilot power of Alice and Bob, and T_s is the time of channel estimation. (iii) Alice and Bob repeat (i) and (ii) throughout the coherent time, and implement quantization, information reconciliation and privacy amplification to generate the secret key.

B. Scheme 2

In scheme 2, the legitimate communication parties Alice and Carlo generate secret keys cooperatively. The specific step is as follows: (i) By applying the pilots sent by Alice and the channel estimation methods proposed in [12], Carlo estimates all the CSI exactly in advance. (ii) In the same coherent time, Carlo sends pilots to Alice, and randomly changes the phase of the IRS elements in the same way as scheme 1. (iii) Carlo calculates Alice's channel coefficients based on the CSI and the phase shift of IRS, while Alice estimates channel coefficients based on the pilots. Then, we have

$$\begin{cases} \tilde{h}_A = h_{CA} + n'_A = \sum_n e^{j\theta_n} g_{Cr,n} h_{rA,n}^* + h_{CA,d} + n'_A \\ \tilde{h}_C = h_{CA} = \sum_n e^{j\theta_n} g_{Cr,n} h_{rA,n}^* + h_{CA,d} \end{cases} \quad (4)$$

where $n'_A \sim \mathcal{CN}(0, 2\sigma_n^2 / P_C T_s)$, $\tilde{h}_C$ denotes the calculation of Carlo. (iv) Alice and Carlo repeat (ii) and (iii) throughout the coherent time T_c . Then, implement quantization, information reconciliation and privacy amplification to generate the secret key.

IV. SECRET KEY RATE ANALYSIS

To evaluate the performance, we study both the exact secret key rate and the approximate values in the following. Due to the eavesdropper channels are independent from the legitimate channels (verified in section V), and according to the result of [4], the instantaneous secret key rate for scheme 1 and 2 can be respectively expressed as

$$\begin{aligned} R_{s1} &= \frac{1}{T_s} I(\hat{h}_A; \hat{h}_B) \quad (\text{bit/s}) \\ R_{s2} &= \frac{1}{T_s} I(\tilde{h}_A; \tilde{h}_C) \quad (\text{bit/s}) \end{aligned} \quad (5)$$

A. Exact Secret Key Rate

For the convenience of analysis, we decouple the complex variable into the i.i.d. real and imaginary parts in the same way as [4] and [13]. For example, we decouple h_{UV} as h_{UV}^R and h_{UV}^I respectively. Let $\sigma_a^2 = \sigma_n^2 / P_B T_s$, $\sigma_b^2 = \sigma_n^2 / P_A T_s$, $\sigma_c^2 = \sigma_n^2 / P_C T_s$, $\xi_i \in \mathcal{H}_{AB}$, $\zeta_i \in \mathcal{H}_{CA}$, where $\mathcal{H}_{AB}$ and $\mathcal{H}_{CA}$ represent the value space of h_{AB}^R and h_{CA}^R , respectively.

Proposition 1: The exact secret key rate of scheme 1 and 2 are given by

$$\begin{aligned} R_{s1} &= \frac{2}{T_s K^N} \iint \text{tr}(\mathbf{AB}) \log_2 \frac{K^N \text{tr}(\mathbf{AB})}{\text{tr}(\mathbf{A}) \text{tr}(\mathbf{B})} dx dy \\ R_{s2} &= -\frac{2}{T_s K^N} \int \text{tr}(\mathbf{C}) \log_2 \frac{K^N}{\text{tr}(\mathbf{C})} dz - \frac{1}{T_s} \log_2(2\pi e \sigma_c^2) \end{aligned} \quad (6)$$

where $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ are defined as

$$\begin{aligned} \mathbf{A} &= \text{diag} \left(\Phi \left(\frac{(x - \xi_i)}{\sigma_a} \right), \dots \right), \quad i = 1, 2, \dots, K^N \\ \mathbf{B} &= \text{diag} \left(\Phi \left(\frac{(y - \xi_i)}{\sigma_b} \right), \dots \right), \quad i = 1, 2, \dots, K^N \\ \mathbf{C} &= \text{diag} \left(\Phi \left(\frac{(z - \zeta_i)}{\sigma_c} \right), \dots \right), \quad i = 1, 2, \dots, K^N \end{aligned} \quad (7)$$

Proof: R_{s1} in (6) can be rewritten as

$$\begin{aligned} R_{s1} &= \frac{1}{T_s} I(\hat{h}_A; \hat{h}_B) = \frac{1}{T_s} I(\hat{h}_A^I; \hat{h}_B^I) + \frac{1}{T_s} I(\hat{h}_A^R; \hat{h}_B^R) \\ &\stackrel{(a)}{=} \frac{2}{T_s} \iint f_{\hat{h}_A^R, \hat{h}_B^R}(x, y) \log_2 \frac{f_{\hat{h}_A^R, \hat{h}_B^R}(x, y)}{f_{\hat{h}_A^R}(x) f_{\hat{h}_B^R}(y)} dx dy \end{aligned} \quad (8)$$

where $f(\cdot)$ is the probability density function (PDF), $f(\cdot, \cdot)$ is the joint PDF, and (a) holds due to the real and imaginary parts of channel gain are i.i.d. random variables. For a given $\xi_i \in \mathcal{H}$, the probability distribution of h_{AB}^R is given by

$$\begin{aligned} P(\xi_i) &\equiv P(h_{AB}^R = \xi_i) \\ &= P \left(\sum_n \beta_{g_{Ar,n}} \beta_{h_{B,n}}^* \cos(\theta_n + \theta_{g_{Ar,n}} + \theta_{h_{B,n}}^*) + h_{AB,d}^R = \xi_i \right) \\ &\stackrel{(a)}{=} P \left(\theta_1 = \frac{2\pi(k_1-1)}{K}, \theta_2 = \frac{2\pi(k_2-1)}{K}, \dots, \right. \\ &\quad \left. \theta_N = \frac{2\pi(k_N-1)}{K} \right) \\ &\stackrel{(b)}{=} \frac{1}{K^N} \end{aligned} \quad (9)$$

where $k_1, k_2, \dots, k_N \in \{1, 2, \dots, K\}$, β and θ denote the amplitude and phase of reflection channel $\mathbf{G}_{Ar}$ and $\mathbf{h}_{rB}$, respectively. (a) holds due to θ_n follows Discrete Uniform Distribution, and the number of the values of h_{AB}^R is a permutation with repetition of size K^N . In addition, n_A^R and n_B^R are i.i.d. Gaussian random variables with variance σ_a^2 and σ_b^2 , $\hat{h}_A^R$ and $\hat{h}_B^R$ follow the Gaussian Mixture Distribution. Then, the PDF and joint PDF of $\hat{h}_A^R$ and $\hat{h}_B^R$ in (8) can be expressed as

$$\begin{aligned} f_{\hat{h}_A^R}(x) &= \sum_i P(\xi_i) f_{\hat{h}_A^R | h_{AB}^R}(x | \xi_i) = \sum_i \frac{1}{K^N} \Phi \left(\frac{(x - \xi_i)}{\sigma_a} \right) \\ f_{\hat{h}_B^R}(y) &= \sum_i P(\xi_i) f_{\hat{h}_B^R | h_{AB}^R}(y | \xi_i) = \sum_i \frac{1}{K^N} \Phi \left(\frac{(y - \xi_i)}{\sigma_b} \right) \\ f_{\hat{h}_A^R, \hat{h}_B^R}(x, y) &= \sum_i P(\xi_i) f_{\hat{h}_A^R, \hat{h}_B^R}(x, y | \xi_i) \\ &\stackrel{(a)}{=} \sum_i P(\xi_i) f_{\hat{h}_A^R | h_{AB}^R}(x | \xi_i) f_{\hat{h}_B^R | h_{AB}^R}(y | \xi_i) \\ &= \sum_i \frac{1}{K^N} \Phi \left(\frac{(x - \xi_i)}{\sigma_a} \right) \Phi \left(\frac{(y - \xi_i)}{\sigma_b} \right) \end{aligned} \quad (10)$$

where (a) holds due to $\hat{h}_A^R \rightarrow h_{AB}^R \rightarrow \hat{h}_B^R$ is a Markov chain. Then substituting (10) in (8) concludes the proof of R_{s1} .

Similarly to the above derivation, we can obtain

$$\begin{aligned} P(\zeta_i) &\equiv P(h_{CA}^R = \zeta_i) = \frac{1}{K^N} \\ f_{\hat{h}_A^R | h_{CA}^R}(z | \zeta_i) &= \Phi \left(\frac{(z - \zeta_i)}{\sigma_c} \right) \end{aligned} \quad (11)$$

And R_{s2} in (6) can be rewritten as

$$\begin{aligned} R_{s2} &= \frac{2}{T_s} \left[H(\tilde{h}_A^R) - H(\tilde{h}_A^R | h_{CA}^R) \right] \\ &= \frac{2}{T_s} \left[-\sum_i P(\zeta_i) H(\tilde{h}_A^R | \zeta_i) - \frac{1}{2} \log_2(2\pi e \sigma_c^2) \right] \end{aligned} \quad (12)$$

Then substituting (11) and (12) in (6) concludes the proof of R_{s2} .

Since the closed-form expression in (6) are difficult to be derived directly, we can obtain the value of (6) by numerical integration.

B. Asymptotic Secret Key Rate

We consider two extreme conditions to evaluate the asymptotic solutions of the secret key rate of the proposed scheme.

1) High SNR

Let the SNR of Alice, Bob in scheme 1 are expressed as $\gamma_a = \sigma_h^2 / \sigma_a^2$ and $\gamma_b = \sigma_h^2 / \sigma_b^2$, and the SNR of Alice in scheme 2 is $\gamma_c = \sigma_h^2 / \sigma_c^2$, then we have the following corollary.

Corollary 1: Let $\mathbb{E}_{h_{AB}}\{R_{s1}\}$ and $\mathbb{E}_{h_{AC}}\{R_{s2}\}$ denote the ergodic secret key rate (bit/s) in multiple coherent times, then we have

$$\mathbb{E}_{h_{AB}}\{R_{s1}\} \leq \mathbb{E}_{h_{AC}}\{R_{s2}\} \leq \frac{2K^N}{T_s} \text{ (bit/s)} \dots\dots\dots (13)$$

The first equal sign holds when $\gamma_a = \gamma_c$ and $\gamma_b \rightarrow \infty$, and the second equal sign holds when γ_a, γ_b and $\gamma_c \rightarrow \infty$.

Proof:

$$\begin{aligned} \mathbb{E}_{h_{AB}}\{R_{s1}\} &\stackrel{(a)}{=} \frac{2}{T_s} \mathbb{E}_{h_{AB}}\{I(\hat{h}_A^R; \hat{h}_B^R)\} \\ &\stackrel{(b)}{=} \frac{2}{T_s} \mathbb{E}_{h_{AB}}\{I(h_{AB}^R; \hat{h}_A^R) + I(h_{AB}^R; \hat{h}_B^R | \hat{h}_A^R)\} \\ &\stackrel{(c)}{\leq} \frac{2}{T_s} \mathbb{E}_{h_{AB}}\{I(h_{AB}^R; \hat{h}_A^R)\} \\ &\stackrel{(d)}{=} \frac{2}{T_s} \mathbb{E}_{h_{AC}}\{I(h_{AC}^R; \tilde{h}_C^R)\} = \mathbb{E}_{h_{AC}}\{R_{s2}\} \\ &\stackrel{(f)}{=} \frac{2}{T_s} \mathbb{E}_{h_{AC}}\{H(h_{AC}^R) - H(h_{AC}^R | \tilde{h}_C^R)\} \\ &\stackrel{(g)}{\leq} \frac{2}{T_s} \mathbb{E}_{h_{AC}}\{H(h_{AC}^R)\} = \frac{2K^N}{T_s} \text{ (bit/s)} \end{aligned} \dots\dots\dots (14)$$

where (a) and (e) hold due to (5) and the independence of real part and imaginary part. (b) holds due to the mutual information chain rule and $\hat{h}_A^R \rightarrow h_{AB}^R \rightarrow \hat{h}_B^R$ is a Markov chain, (c) and (g) hold due to the conditional mutual information and conditional entropy of discrete random variables are not negative, (d) holds due to $\gamma_a = \gamma_c$ and the channel coefficients in different coherence times are i.i.d. random variables. (f) holds due to $I(h_{AC}^R; \tilde{h}_C^R) = H(h_{AC}^R) - H(h_{AC}^R | \tilde{h}_C^R)$.

Corollary 1 shows that when the SNR is large, R_{s1} and R_{s2} are limited to N, K and T_s . It inspired us to further increase the secret key rate by configuring IRS appropriately.

2) Massive IRS Elements

For the IRS with finite number of the discrete phase shift, i.e., K , we can deploy more IRS elements to obtain larger key rate. In this subsection, we prove that the R_{s1} and R_{s2} in Proposition 1 have closed-form upper bound when N tends to infinity

Corollary 2: When $N \rightarrow \infty$, $h_{AB}^R, h_{AB}^I, h_{CA}^R$ and h_{CA}^I approximately follow Gaussian distribution, and the exact secret key rate of scheme 1 and 2 are given by

$$\begin{aligned} \lim_{N \rightarrow \infty} \mathbb{E}_{h_{AB}}\{R_{s1}\} &= -\frac{1}{T_s} \log_2 \left(1 - \frac{\rho^2 \sigma_h^4}{(\rho \sigma_h^2 + \sigma_a^2)(\rho \sigma_h^2 + \sigma_b^2)} \right) \\ \lim_{N \rightarrow \infty} \mathbb{E}_{h_{AC}}\{R_{s2}\} &= -\frac{1}{T_s} \log_2 \left(1 - \frac{\rho \sigma_h^2}{(\rho \sigma_h^2 + \sigma_c^2)} \right) \end{aligned} \dots\dots\dots (15)$$

Proof: Based on the system model, we have $E(h_{AB}^R - h_{AB,d}^R) = E(h_{AB}^I - h_{AB,d}^I) = E(h_{CA}^R - h_{CA,d}^R) = E(h_{CA}^I - h_{CA,d}^I) = 0$, and $D(h_{AB}^R - h_{AB,d}^R) = D(h_{AB}^I - h_{AB,d}^I) = D(h_{CA}^R - h_{CA,d}^R) = D(h_{CA}^I - h_{CA,d}^I) = \rho \sigma_h^2$. Then, according to the Lemma 2 and 3 (i.e. Lyapunov theorem) in [10], when $N \rightarrow \infty$, the distribution of $h_{AB}^R, h_{AB}^I, h_{CA}^R$ and h_{CA}^I converges weakly to Gaussian random variables with variance $\rho \sigma_h^2$. Finally, according to the well-known Gaussian PDF, a derivation similar to [10] can be carried out to obtain $\lim_{N \rightarrow \infty} \mathbb{E}_{h_{AB}}\{I(\hat{h}_A; \hat{h}_B)\}$ and $\lim_{N \rightarrow \infty} \mathbb{E}_{h_{AC}}\{I(\tilde{h}_A; \tilde{h}_C)\}$. Such that Corollary 2 is proved.

In addition, from (5), (13) and (15), it can be observed that reducing T_s can obtain more channel estimation samples in a short time and generate keys faster. However, transmitting pilot in such a short time amplifies the error of the channel estimation, thereby reducing the number of key bits that can be extracted for each estimation sample. Therefore, the selection of T_s is crucial for the increasing of R_{s1} and R_{s2} . In general, it is difficult to obtain the closed form expressions of optimal T_s . We will use a one-dimensional search to find the optimal value in Section V.

V. SIMULATION AND NUMERICAL RESULTS

In this section, we present numerical results and Monte Carlo simulation results to evaluate the performance of the proposed IRS assisted SKG scheme. To ensure the accuracy of the results, we perform Monte Carlo simulation method to generate 10000 random channel gains at different coherent time. For ease of analysis, we assume that $K=2$.

First, we plot 1000 channel estimation samples in Fig. 2. From Fig. 2(a1) and Fig. 2(a2), one can see that when N is small, the channel coefficients approximately follow complex Gaussian Mixture Distribution, and the real part of the IRS, i.e. h_{AB}^R has K^N different values. Fig. 2(b3) and Fig. 2(a3) are normal probability plots, which show that when $N=20$, the real parts of the channel coefficient approximately follow the Gaussian distribution, which shows that the approximate secret key rate is also valid for most general IRS channel models. In addition, the channel coefficients of Alice and Bob are very similar, but are quite different from Eve's, which verifies that the eavesdropping channel and the legal channel are independent.

Fig. 2. The complex plane diagram of 1000 channel estimation samples, and the Normal Probability Plot (NPP) of the real parts of $\hat{h}_A$: $\gamma = 30\text{dB}$, $K=2$, $N=5$, for (a) and $N=20$ for (b).

To verify the derivation results, we use the MATLAB *Information Theoretical Estimator* Toolbox as [4] to calculate the simulation value of R_{s1} and R_{s2} in (6), and calculate the theoretical value according to *Proposition 1* and *Corollary 1*. Unless otherwise noted, the solid lines in the following figures represent the theoretical value, and the dashed lines represent the simulated value. Fig. 3 plots the R_{s1} and R_{s2} versus γ and N , where several colored lines are calculated by *Proposition 1*, and the black lines are calculated by *Corollary 2*. It can be seen that even in static environment, R_{s1} and R_{s2} increases with the increase of SNR and N due to the dynamic channel. Moreover, R_{s1} and R_{s2} do not exceed the upper bound derived from *Corollary 2* as N continues to increase. And when the number of reflection elements is limited, i.e., $N=20$, R_{s1} and R_{s2} is very close to the upper bound. For most IRS, it is easy to deploy such a few reflection elements. In addition, it can be observed that R_{s2} is always larger than R_{s1} . This is because Carlo knows all the CSI and the switched phase, which eliminates uncertainties of $\tilde{h}_A$. Due to the similar trend of their curves, we only analyze R_{s1} for simplification in the following.

Fig. 3. The secret key rate versus γ and N with $K=2$, $T_s=1$.

Fig. 4. Comparison of the condition mutual information between scheme 1 and other schemes with $K=2$, $T_s=1$.

In Fig.4 shows the condition mutual information of scheme 1 when Eve performs the same method, where $\hat{h}_E$ is obtained in the same way as $\hat{h}_A$ and $\hat{h}_B$. As comparisons, Zhang's scheme [8] and Aldaghri's scheme [9] are considered, both of which are designed for static environment. From Fig. 4, one can see that the secret key rate of our scheme is restricted by ρ , which shows that it has better performance when the reflected channel is the main component of the combined channel. In addition, It can be observed that the conditional mutual information of proposed scheme in Fig.4 is very close to that of Fig. 3, which indicates that Eve hardly knows $\hat{h}_A$ and $\hat{h}_B$ by passive eavesdropping. This is because the legitimate channel is independent from the eavesdropping channel, so almost no information about IRS reflection channel is leaked to Eve. However, schemes in [8] and [9] only induce the randomness of the signal artificially, without increasing the uncertainty of the channel. From the analysis in [10], the information of random signal may partially leak to Eve when channels are static. Therefore, the proposed scheme has advantages over the other two schemes in terms of secret key rate, especially in high SNR.

Fig. 5. R_{s1} versus transmission power $P_t = P_A = P_B$ and T_s with $N=20$.

Fig. 5 shows the R_{s1} versus transmission power P_t and T_s , where the purple dots are the optimal T_s corresponding to the maximum R_{s1} for a given P_t , and they are obtained by numerical search. Of note is that the R_{s1} is lower when T_s is smaller due to the larger error of the channel estimation according to (3). Moreover, a larger T_s means that a lower switching frequency of the IRS phase shift and a smaller number of channel estimation samples in the coherent time, resulting in a lower R_{s1} . Therefore, it can be observed that the

optimal T_s decreases with the increase of P_t , which means to obtain a larger R_{s1} , T_s should be reduced when the transmission power is increasing.

VI. CONCLUSION

In this paper we proposed a novel secret key generation scheme based on the intelligent reflecting surface with discrete phase shift. The phase of reflection elements switches randomly and rapidly to change the CSI of combined channel in static environment. At the same time, the legitimate communication parties estimate the time-varying channel coefficients for SKG. Furthermore, we derive the expressions of secret key rate, and analyze them versus the number of reflection element, the switching frequency of phase shift and transmission power. Simulation and numerical results show that legitimate communication parties can update the secret key in static environment. Moreover, when ρ is large, the secret key rate is higher than [8] and [9] due to the independence of the CSI of the legitimate node and the eavesdropper. In addition, the results show that the key rate can be increased by increasing N , or reducing T_s while increasing the power.

ACKNOWLEDGMENT

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0801903, in part by the National Natural Science Foundation of China under Grant 61701538, Grant 61601514, Grant 61501516, and Grant 61521003, in part by Doctoral Fund of Ministry of Education of China (2019M663994), and in part by National Defense Science and Technology Innovation Special Zone of China.

REFERENCES

- [1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," in *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679-695, April 2018.
- [2] J. Zhang, B. He, T. Q. Duong and R. Woods, "On the Key Generation From Correlated Wireless Channels," in *IEEE Communications Letters*, vol. 21, no. 4, pp. 961-964, April 2017.
- [3] J. Wallace, "Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits," 2009 *IEEE International Conference on Communications*, Dresden, 2009, pp. 1-5.
- [4] S. Xiao, Y. Guo, K. Huang and L. Jin, "Cooperative Group Secret Key Generation Based on Secure Network Coding," in *IEEE Communications Letters*, vol. 22, no. 7, pp. 1466-1469, July 2018.
- [5] S. Bakshi and D. C. Popescu, "Secret Key Generation With Precoding and Role Reversal in MIMO Wireless Systems," in *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, pp. 3104-3112, June 2019.
- [6] H. Taha and E. Alsusa, "Secret Key Exchange Using Private Random Precoding in MIMO FDD and TDD Systems," in *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 4823-4833, June 2017.
- [7] Y. Lou, L. Jin, Z. Zhong, K. Huang, and S. Zhang, "Secret key generation scheme based on MIMO received signal spaces (in Chinese)," *SCIENTIA SINICA Informationis*, vol. 47, no. 3, pp. 362-373, 2017.
- [8] S. Zhang, L. Jin, Y. Lou and Z. Zhong, "Secret key generation based on two-way randomness for TDD-SISO system," in *China Communications*, vol. 15, no. 7, pp. 202-216, July 2018.
- [9] N. Aldaghri and H. Mahdavi, "Physical Layer Secret Key Generation in Static Environments," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692-2705, 2020.
- [10] L. Jin, S. Zhang, Y. Lou, X. Xu and Z. Zhong, "Secret Key Generation With Cross Multiplication of Two-Way Random Signals," in *IEEE Access*, vol. 7, pp. 113065-113080, 2019.
- [11] T. J. Cui, M. Q. Qi, X. Wan, J. Zhao, and Q. Cheng, "Coding metamaterials, digital metamaterials and programmable metamaterials," *Light: Science & Applications*, vol. 3, e218, Oct. 2014.
- [12] C. You, B. Zheng and R. Zhang, "Channel Estimation and Passive Beamforming for Intelligent Reflecting Surface: Discrete Phase Shift and Progressive Refinement," in *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2604-2620, Nov. 2020.
- [13] Q. Xu and P. Ren, "Channel-Aware Key Generation Under Wireless Fading Environment," in *IEEE Communications Letters*, vol. 24, no. 8, pp. 1636-1640, Aug. 2020.
- [14] L. Zhang et al., "Space-time-coding digital metasurfaces," *Nature Communications*, vol. 9, no. 1, p. 4334, Oct. 2018.

Xiaoyan Hu received the M.S. degree in Information and Communication Engineering from PLA Strategic Support Force Information Engineering University, Zhengzhou, China, in 2018 and now he is pursuing the Ph.D. degree. His research interests include wireless network security, physical layer security, and information theory.

Liang Jin received the Ph.D. degree from Xi'an Jiaotong University, Xi'an, China. He is a Professor and a Ph.D. Supervisor with the National Digital Switching System Engineering and Technological Research Center (NDSC), which is an affiliate of the PLA Strategic Support Force Information Engineering University, Zhengzhou, China. He is also a Visiting Researcher with Purple Mountain Laboratories: Networking, Communications and Security, Nanjing, China. His research interests include wireless communication, physical layer security, and smart antenna.

Kaizhi Huang received the Ph.D. degree from Tsinghua University, Beijing, China. She has been a Faculty Member of NDSC, which is an affiliate of the PLA Strategic Support Force Information Engineering University, Zhengzhou, China. She is currently a Professor and a Visiting Researcher with Purple Mountain Laboratories: Networking, Communications and Security. Her research interests include wireless network security, physical layer security and signal processing

Keming Ma received the Ph.D. degree from the PLA Strategic Support Force Information Engineering University, where he is currently a Lecturer and a Faculty Member of NDSC. He is also a Visiting Researcher with Purple Mountain Laboratories: Networking, Communications and Security. His research interests include wireless signal processing, channel coding, and channel estimation and equalization.

Shuaifang Xiao received the B.S. degree in electronic science and technology from Tsinghua University, Beijing, China, and the Ph.D. degree from the PLA Strategic Support Force Information Engineering University. He is currently a Research Associate with NDSC. His research interests include physical layer security, cooperative communications, and the internet of things.