Reconfigurable Intelligent Surface Assisted Secret Key Generation in Quasi-Static Environments

Tianyu Lu, Liquan Chen, *Member, IEEE,* Junqing Zhang, Kailin Cao, and Aiqun Hu, *Member, IEEE*

***Abstract*—We propose a key generation protocol with the aid of a reconfigurable intelligent surface (RIS) to boost secret key rate (SKR) in quasi-static environments. Considering a passive eavesdropper, we derive the closed-form expression of the lower and upper bounds of the SKR. Our findings indicate the SKR is determined by the number of RIS elements, the correlation coefficient, the pilot length and the quality of the reflecting channel. Our protocol fully exploits the randomness from the direct channel and the reflecting channel. Monte Carlo simulations validate the analytical expression of the SKR and demonstrate our protocol outperforms existing work.**

***Index Terms*—Physical layer security, reconfigurable intelligent surface, secret key rate.**

I. Introduction

KEY generation is a promising technology for establishing cryptographic keys for Internet of Things (IoT) [1]. Secret key rate (SKR) describes how fast the protocol can generate keys securely [2]. SKR highly relies on channel variation, hence it is limited in quasi-static environments where the coherence time is quite long. Artificial randomness has been introduced in such scenarios for increasing SKR [3], where the transmitter manipulates the artificial channel characteristics observed by the receiver.

Reconfigurable intelligent surface (RIS) can also be used to introduce artificial randomness. RIS can adjust the amplitudes and phase shifts of incident waves using tunable reflectors, which can be used to modify the propagation environment and induce randomness to boost SKR. The passive beamforming design is optimized in a RIS-assisted key generation system in [4]. The optimal selection of RIS units is proposed in [5] to maximize the SKR. These works focused on designing the phase matrix to maximize the signal-to-noise ratio (SNR), lacking in the solution to the slow variation of the channel in quasi-static environments. Two-way probing (TWP) and one-way probing (OWP) is employed in [6] but the information leaked to eavesdroppers is not considered. Including the spatially-correlated direct channel, the correlation between legitimate and eavesdropping reflecting channels severely degrades the SKR. Considering multiple eavesdroppers, the work in [7] introduced a one-time pad communication protocol by utilizing random phase shifts of RIS elements, where the derivation of the upper bound (UB) on the SKR is rigorous but the lower bound (LB) is not analyzed.

This research is supported by National key research and development program of China, Joint research of IoT security system and key technologies based on quantum key (2020YFE0200600). (Corresponding author: L. Chen)

T. Lu, L. Chen and K. Cao are with the School of Cyber Science and Engineering, Southeast University, Nanjing, 210096, China. (e-mail: effronlu@seu.edu.cn; lqchen@seu.edu.cn; caokl@seu.edu.cn)

J. Zhang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom. (email: junqing.zhang@liverpool.ac.uk.)

A. Hu is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China. (e-mail: aqhu@seu.edu.cn)

L. Chen and A. Hu are also with the Purple Mountain Laboratories for Network and Communication Security, Nanjing, 211111, China.

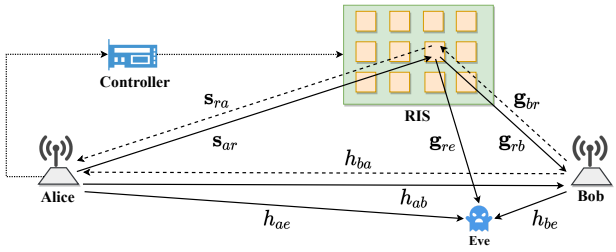

Fig. 1. System model of the RIS-assisted secret key generation

A complete analysis of the information-theory security of RIS-assisted key generation in quasi-static environments is still missing. Our main technical contributions are as follows:

- A four-step channel probing for RIS-assisted key generation is designed. Instead of improving the SNR by the passive beamforming, the RIS introduces artificial randomness by random phase matrix in quasi-static environments. Our protocol fully exploits the randomness from the direct channel and reflecting channels.
- The lower bound and upper bound on the analytical expression of the SKR are derived with the presence of a passive eavesdropper.
- Our protocol is validated by Monte Carlo simulations. We find that the SKR is determined by the pilot length, the correlation between measurements, the quality of the reflecting channel, and the number of RIS elements.

Notations: Lower-case, boldface lower-case and boldface upper-case letters denote scalars, vectors and matrices, respectively. $(\cdot)^{-1}$, $\bar{(\cdot)}$ and $(\cdot)^H$ are the inverse, conjugate and conjugate transpose, respectively. $\|\cdot\|$ is the Euclidean norm, $\mathbb{E}\{\cdot\}$ is the expectation, and $\circ$ is the Hadamard product.

II. System and Channel Model

The RIS-assisted key generation system consists of two legitimate users, Alice and Bob, a RIS, as well as a passive eavesdropper, Eve, as shown in Fig. 1. Alice, Bob and Eve are all equipped with a single antenna. Alice and Bob aim to agree on a common key and keep it secure from Eve. They probe the channel in a time-division duplex (TDD) mode and extract secret keys from their correlated measurements. Eve

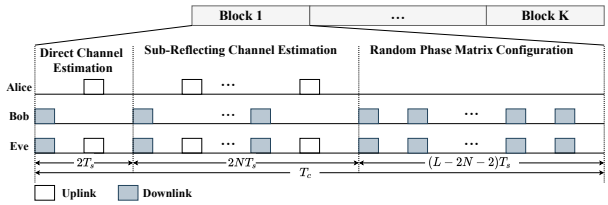

Fig. 2. Channel probing in one coherence block

listens to transmissions over the public channel and wants to infer the keys from the measurements. A RIS equipped with N reflection elements serves as a trust third party. It applies random phase matrix to mimic movement-induced fast fading.

We consider Rayleigh block-fading channels where the channel effects remain constant during the coherence time T_c. Each block is further divided into $L = T_c/T_s$ slots, which is denoted as uplink (downlink) slot when it is assigned for uplink (downlink). The RIS configures phase shifts to modify the channel as a function of slots $t = 1, 2, \ldots, L$. The channel modified by RIS can be estimated by sending a public pilot signal $\mathbf{x} \in \mathbb{C}^{T_l \times 1}$ from the transmitter u to the receiver v, where T_l is the length of the pilot signal. In the t-th slot of the k-th block, the received signal can be given as

$$\begin{aligned}\mathbf{y}_v(t,k) &= (h_{uv}(k) + \mathbf{g}_{rv}^T(k)(\boldsymbol{\phi}(t,k) \circ \mathbf{s}_{ur}(k)))\mathbf{x} + \mathbf{n}_{uv}(t,k) \\ &= (h_{uv}(k) + \boldsymbol{\phi}^T(t,k)(\mathbf{g}_{rv}(k) \circ \mathbf{s}_{ur}(k)))\mathbf{x} + \mathbf{n}_{uv}(t,k),\end{aligned} \tag{1}$$

where $h_{uv}(k)$ is the direct channel from the transmitter u to the receiver v, $\{u, v\} = \{a, b, e\}$, $\mathbf{s}_{ur}(k) \in \mathbb{C}^{N\times 1}$ is the channel from the transmitter u to the RIS, r, $\mathbf{g}_{rv}(k) \in \mathbb{C}^{N\times 1}$ is the channel from the RIS to the receiver v, $\mathbf{n}_{uv}(t,k)$ is an additive white Gaussian noise (AWGN) vector, and $\boldsymbol{\phi}(t,k) = [\phi_1(t,k), \ldots, \phi_N(t,k)]^T$ is the reflection vector that models the phase shifts of RIS where $\phi_n(t,k) = e^{j\theta_n(t,k)}$ is the reflection coefficient of n-th element. The phase shift $\theta_n(t,k)$ is configured from the uniform quantization of the interval $[0, 2\pi)$, i.e., $\mathcal{K} = \{0, \frac{2\pi}{K}, \ldots, \frac{2\pi(K-1)}{K}\}$, where $K = 2^B$ is the phase-shift level and B is the controlling bits [8]. The index k is dropped for clarity in the following context.

According to (1), the n-th element can dynamically adjust its reflection coefficient to modify the n-th channel of $\mathbf{g}_{rv} \circ \mathbf{s}_{ur}$. Define $\mathbf{r}_{uv} = [r_{uv,1}, \ldots, r_{uv,N}] \equiv \mathbf{g}_{rv} \circ \mathbf{s}_{ur}$ as the reflecting channel, where $r_{uv,n}$, $n \in 1, \ldots, N$, is the n-th sub-reflecting channel. The received signal (1) can be rewritten as

$$\mathbf{y}_v(t) = (h_{uv} + \boldsymbol{\phi}(t)^T\mathbf{r}_{uv})\mathbf{x} + \mathbf{n}_{uv}(t). \tag{2}$$

We assume that $h_{uv} \sim \mathcal{CN}(0, \sigma_{uv}^2)$, $s_{ur,n} \sim \mathcal{CN}(0, \sigma_{ur,n}^2)$, $g_{rv,n} \sim \mathcal{CN}(0, \sigma_{rv,n}^2)$, and $\mathbf{n}_{uv}(t) \sim \mathcal{CN}(\mathbf{0}, \sigma_{n_{uv}}^2\mathbf{I})$, where $s_{ur,n}$ ($g_{rv,n}$) is the n-th entry of $\mathbf{s}_{ur}$ ($\mathbf{g}_{rv}$). The channels are reciprocal, i.e., $h_{vu} = h_{uv}$, $s_{ur,n} = s_{ru,n}$ and $g_{rv,n} = g_{vr,n}$.

III. Protocol Design

As shown in Fig. 2, in order to fully exploit the artificial randomness induced by the RIS, we designed a four-step protocol, namely direct channel estimation, sub-reflecting channel estimation, random phase matrix configuration and channel state information (CSI) reconstruction. Specifically, we first estimate the direct channel to exploit its randomness; the measurements will also be used in steps 2 and 3 to mitigate the influence of the direct channel. Secondly, we estimate the sub-reflecting channels to exploit its randomness; the measurements will also be used in step 4 to reconstruct Alice's CSI. Thirdly, to induce fast-fading effects in a block, RIS configures random phase matrix and Bob probes the channel in downlink slots. Finally, Alice reconstruct the CSI based on the measurements from the former steps and the controlled reflection vector. Notably, the measurements in OWP scheme is twice the quantity of that in TWP scheme.

A. Step 1: Direct Channel Estimation

The direct channel varies from block to block whose randomness can be extracted. At the first two slots, Alice and Bob turn off the RIS and send the public pilot to each other. Eve also receives two pilot signals. The receiver v measures the CSI by the least square (LS) method [9] as

$$\hat{h}_{uv} = \frac{\mathbf{x}^H}{||\mathbf{x}||^2}\mathbf{y}_v(t) = h_{uv} + \frac{\mathbf{x}^H}{PT_l}\mathbf{n}_{uv}(t), \tag{3}$$

where P is the average transmit power. Note that $\hat{h}_{uv} \sim \mathcal{CN}(0, \hat{\sigma}_{uv,0}^2)$ with $\hat{\sigma}_{uv,0}^2 = \sigma_{uv}^2 + \sigma_{n_{uv}}^2/(PT_l)$ and the estimation noise is $\hat{n}_{uv}(t)$ with $\hat{\sigma}_{n_{uv,0}}^2 = \sigma_{n_{uv}}^2/(PT_l)$.

B. Step 2: Sub-Reflecting Channel Estimation

The sub-reflecting channels are sources of randomness which are however hard to extract directly from a single channel probing since the channel observed by a receiver at the t-th slot is a superposition of the direct and sub-reflecting channels. Also, because Bob conducts OWP in step 3, Alice needs to know the CSI of sub-reflecting channels so that Alice can observe the same artificially-randomized channel to Bob by combining it with the controlled $\boldsymbol{\phi}(t)$ in step 4.

Alice and Bob implement overall N rounds of channel probings alternatively in uplink and downlink slots and then repeat the LS algorithm N times. Eve eavesdrops on transmissions and conducts the LS estimation. Alice will configure the $\boldsymbol{\phi}(t)$ same for the two slots but different for different rounds of probing. After that, they stack N reflection vectors to form an orthogonal matrix and perform the inverse operation to recover N sub-reflecting channels. The direct-channel component in measurements can be wiped off based on $\hat{h}_{uv}$.

Define two same reflection pattern matrices whose rows should be orthogonal as $\boldsymbol{\Phi} = [\boldsymbol{\phi}(t), \ldots, \boldsymbol{\phi}(t + 2(N-1))]^T$, where $t = 3$ for downlink slots and $t = 4$ for uplink slots. RIS chooses a Hadamard-matrix truncation reflection pattern $\boldsymbol{\Phi}$ to decompose $\mathbf{r}_{uv}$ [8], which is public to Eve. After N rounds of channel probings, the receiver v collects the received signals and stack the measurements as $\hat{\mathbf{H}}_{uv} = [\hat{h}_{uv}(t), \ldots, \hat{h}_{uv}(t + 2(N-1))]^T$, where $\hat{h}_{uv}(t) = \boldsymbol{\phi}_{uv}^T(t)\mathbf{r}_{uv} + h_{uv} + \frac{\mathbf{x}^H}{\|\mathbf{x}\|}\mathbf{n}_{uv}(t)$. We have $\hat{\mathbf{H}}_{uv} = \boldsymbol{\Phi}\mathbf{r}_{uv} + h_{uv} + \hat{\mathbf{N}}_{uv}(t)$, where $\hat{\mathbf{N}}_{uv} = [\hat{\mathbf{n}}_{uv}(t), \ldots, \hat{\mathbf{n}}_{uv}(t + 2(N-1))]^T$ and $\hat{\mathbf{n}}_{uv}(t) = \frac{\mathbf{x}^H}{PT_l}\mathbf{n}_{uv}(t)$. Given $\hat{\mathbf{H}}_{uv}$ and $\hat{h}_{uv}$, the receiver v measures $\mathbf{r}_{uv}$ as

$$\hat{\mathbf{r}}_{uv} = \boldsymbol{\Phi}^{-1}\hat{\mathbf{H}}_{uv} - \hat{h}_{uv} = \mathbf{r}_{uv} + \boldsymbol{\Phi}^{-1}(\hat{\mathbf{n}}_{uv}(t) - \hat{\mathbf{n}}_{uv}(t-2)). \tag{4}$$

Notably, $\hat{\mathbf{r}}_{uv} \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Sigma})$, where $\boldsymbol{\Sigma} = \sigma_{rv,n}^2\sigma_{ur,n}^2 + \sigma_{n_{uv}}^2(\boldsymbol{\Phi}^H\boldsymbol{\Phi})^{-1}/(PT_l) + \boldsymbol{\Delta}$. Here, $\boldsymbol{\Delta}$ is a matrix with one

element δ at the upper-left corner because $\mathbf{\Phi}^{-1}$ centralizes the estimation noise from step 1 to the first measurement in step 2. The estimation noise variance is $\hat{\sigma}^2_{n_{uv,n}} = \sigma^2_{n_{uv}}/(NPT_l) + \delta\sigma^2_{n_{uv}}/(PT_l)$, where $\delta = 1$ for $t = 3$ and 4, otherwise $\delta = 0$. Specially, the autocorrelation $\rho_{l,2}$ of the measurements in step 2 is not affected by the estimation noise accumulated from step 1 and they can be viewed as independent random variables (RVs). In practice, there exists spatial correlation between sub-reflecting channels, which is affected by the element size and wavelength [10]. The large-size case is applied here, where the spatial correlation between sub-reflecting channels is weak. We will validate the effect from the spatial correlation in the simulation. In small-size case, several elements can be grouped into a sub-surface that is equivalent to a large-size element.

C. Step 3: Random Phase Matrix Configuration

One Rayleigh-fading block maintains a long coherence time in quasi-static environments, so this source of randomness is limited. To mimic the same fast-fading physical effects, RIS applies random phase matrix in the remaining $L - 2(N + 1)$ slots. In TWP scheme, Alice and Bob both measure the channel in two slots alternatively. Here, we introduce OWP scheme, where Bob measures the channel in downlink slots and then Alice reconstruct the CSI based on the information from step 1, step 2 and the controlled $\boldsymbol{\phi}(t)$.

From Fig 2, there are only transmissions from Alice to Bob. Different from the fixed pattern in step 2, $\boldsymbol{\phi}(t)$ is generated based on selecting $\theta_{n,t}$ randomly from $\mathcal{K}$ in discrete uniform distribution. After Alice adjusts a random $\boldsymbol{\phi}(t)$ and sends a pilot, Bob and Eve estimate the channel as $\hat{h}_{av}(t) = h_{av} + f_{av}(t) + \frac{\mathbf{x}^H}{||\mathbf{x}||^2}\mathbf{n}_{av}(t)$, where $f_{av}(t) = \boldsymbol{\phi}^T(t)\mathbf{r}_{av}$ is the equivalent channel. According to the central limit theorem (CLT), $f_{av}(t)$ converges to the normal distribution when N is sufficient large, i.e., $N \gg 1$ [11]. In practice, $f_{av}(t)$ is not Gaussian distributed when N is small. However, there is no need to set N too large. $f_{av}(t)$ is approximately a complex Gaussian RV if $N \geq 10$ [12]. Bob and Eve modify measurements by removing the direct channel component as

$$\hat{f}_{av}(t) = \boldsymbol{\phi}^T(t)\mathbf{r}_{av} + \frac{\mathbf{x}^H}{||\mathbf{x}||^2}(\mathbf{n}_{av}(t) - \mathbf{n}_{av}(1)), \tag{5}$$

where $\hat{f}_{av}(t) \sim \mathcal{CN}(0, \hat{\sigma}_{av,r})$ with $\hat{\sigma}_{av,r} = \sum_n \sigma^2_{rv,n}\sigma^2_{ar,n} + \hat{\sigma}_{n_{av,r}}$ and $\hat{\sigma}_{n_{av,r}} = 2\sigma^2_{n_{av}}/(PT_l)$.

D. Step 4: CSI Reconstruction

Alice needs to reconstruct the CSI of the artificially-randomized channel since Alice does not probe the channel directly in OWP scheme. Because Alice controls RIS and knows $\boldsymbol{\phi}(t)$ in advance, Alice combines $\hat{\mathbf{r}}_{ba}$ which is measured in step 2 with $\boldsymbol{\phi}(t)$ as $\hat{f}_{ba}(t) = \boldsymbol{\phi}^T(t)\hat{\mathbf{r}}_{ba}$. Although Eve cannot capture Bob's pilots, Eve knows partial information from step 2, i.e. $\hat{f}_{be}(t) = \sum_n \hat{r}_{be,n}$. Notably, $\hat{\sigma}^2_{n_{bv,r}} = \sigma^2_{n_{bv}}\text{tr}((\mathbf{\Phi}^H\mathbf{\Phi})^{-1})/(PT_l) + \sigma^2_{n_{bv}}/(PT_l) = 2\sigma^2_{n_{bv}}/(PT_l)$.

In a block, the receiver v gets overall $L - (N + 1)$ measurements and stack them as $\tilde{\mathbf{h}}_{uv} = [\tilde{h}^{(1)}_{uv}, \tilde{h}^{(2)}_{uv}, \ldots, \tilde{h}^{(Q)}_{uv}]^T \equiv [\hat{h}_{uv}, \hat{\mathbf{r}}^T_{uv}, \hat{f}_{uv}(2N + 3), \ldots, \hat{f}_{uv}(L)]^T$. Next, we will analyze how much secrets keys Alice and Bob can extract from their measurements in the presence of Eve.

IV. Secret Key Rate Analysis

The SKR is defined as the maximal key bits generated from an observation, which can be lower and upper bounded as [2]

$$\begin{aligned} C_{sk} \geq \max\{&I(\tilde{\mathbf{h}}_{ab}; \tilde{\mathbf{h}}_{ba}) - I(\tilde{\mathbf{h}}_{ab}; \tilde{\mathbf{h}}_{ae}, \tilde{\mathbf{h}}_{be}), \\ &I(\tilde{\mathbf{h}}_{ba}; \tilde{\mathbf{h}}_{ab}) - I(\tilde{\mathbf{h}}_{ba}; \tilde{\mathbf{h}}_{ae}, \tilde{\mathbf{h}}_{be})\}, \\ C_{sk} \leq \min\{&I(\tilde{\mathbf{h}}_{ab}; \tilde{\mathbf{h}}_{ba}), I(\tilde{\mathbf{h}}_{ab}; \tilde{\mathbf{h}}_{ba} \mid \tilde{\mathbf{h}}_{ae}, \tilde{\mathbf{h}}_{be})\}. \end{aligned} \tag{6}$$

A. Lower Bound

For $q = 1$, Alice and Bob extract secret keys from their K measurements of $\tilde{h}^{(1)}_{uv}$. Eve gets as close as possible from Bob to maximize the correlation between his channel h_{ae} with h_{ab}. Therefore, h_{be} is independent with h_{ab} and h_{ae} [13], so the SKR of $\tilde{h}^{(1)}_{uv}$ is $C(\tilde{h}^{(1)}_{ab}, \tilde{h}^{(1)}_{ba}||\tilde{h}^{(1)}_{ae})$ and is lower bounded by

$$C^{(1)}_{l_1} = \log_2\left(1 + \frac{(\eta_{ae} + 1) - |\rho|^2(\eta^* + 1)}{(\eta_{ab} + 1)(\eta_{ba} + 1)(\eta_{ae} + 1) - (\eta_{ae} + 1)}\right), \tag{7}$$

where $\eta^* = \min(\eta_{ab}, \eta_{ba})$, $\rho = \mathbb{E}\{h_{ab}\bar{h}_{ae}\}/(\sigma_{ab}\sigma_{ae})$ is the spatial correlation coefficient between the channel of Alice-Bob and the one of Alice-Eve. The equation (7) is affected by ρ and η_{uv}, where $\eta_{uv} = \hat{\sigma}^2_{n_{uv,0}}/\sigma^2_{uv} = 1/(T_l\gamma_{uv})$ is the mean-square error (MSE) of the direct channel and $\gamma_{uv} = P\sigma^2_{uv}/\sigma^2_{n_{uv}}$ is the signal-to-noise ratio (SNR). The MSE is inversely proportional to the SNR and T_l.

To ensure a positive LB, the argument of $\log(x)$ should be greater than 1. Given a ρ, the requirement $\eta^* < \frac{\eta_{ae} - |\rho|^2 + 1}{|\rho|^2} = \tau$ should be satisfied, i.e., when Alice's or Bob's MSE is lower than the threshold τ, secret keys can be generated securely from the direct channel. In the worst situation $\rho = 1$, Alice's or Bob's MSE should be lower than Eve's.

For $q = 2, \ldots, N + 1$, Alice and Bob extract secret keys from their measurements of sub-reflecting channels. Although h_{be} is independent with h_{ba} and h_{ab}, $\tilde{h}^{(q)}_{be}$ contains the information of $\mathbf{\Phi}$ and $\mathbf{g}_{br}$, so some information is leaked to Eve. According to (6), we derive $C^{(q)}_{l_2,b}$ which is expanded at the bottom of the next page, where $k_1 = 1 - |\rho_1|^2 - |\rho_2|^2$, $k_2 = |\rho_1|^2 + |\rho_2|^2$, $k_3 = 1 - |\rho_1|^2$, $k_4 = |\rho_1|^2$, $k_5 = 1 - |\rho_2|^2$, $k_6 = |\rho_2|^2$, $W^n_{uv} = \mathbb{E}\{r_{uv,n}\bar{r}_{uv,n}\}$ is the variance of the n-th sub-reflecting channel, and ρ_1 (ρ_2) is the spatial correlation coefficients between $r_{ae,n}$ ($r_{be,n}$) and $r_{ab,n}$ ($r_{ba,n}$). $C^{(q)}_{l_2,a} = I(\tilde{h}^{(q)}_{ab}; \tilde{h}^{(q)}_{ba}) - I(\tilde{h}^{(q)}_{ab}; \tilde{h}^{(q)}_{ae}, \tilde{h}^{(q)}_{be})$ can be similarly calculated by replacing the subscript ab in (8) with ba. Therefore, we obtain the LB of $C^{(q)}_{l_2} = \max(C^{(q)}_{l_2,a}, C^{(q)}_{l_2,b})$ as

$$C^{(q)}_{l_2} = \log_2\left(1 + \frac{k_1 + k_3\eta^n_{be} + k_5\eta^n_{ae} + \eta^n_{ae}\eta^n_{be} - (k_2 + k_4\eta^n_{be} + k_6\eta^n_{ae})\eta^*_n}{(\eta^n_{ae}\eta^n_{be} + \eta^n_{ae} + \eta^n_{be} + 1)(\eta^n_{ab} + \eta^n_{ba} + \eta^n_{ab}\eta^n_{ba})}\right), \tag{9}$$

where $\eta^*_n = \min(\eta^n_{ab}, \eta^n_{ba})$. The equation (9) is affected by ρ_1, ρ_2 and η^n_{uv}, where $\eta^n_{uv} = \hat{\sigma}^2_{n_{uv,n}}/W^n_{uv} = 1/(NT_l\gamma^n_{uv}) + \delta/(T_l\gamma^n_{uv})$ is the MSE of the n-th sub-reflecting channel and is determined by N, T_l and $\gamma^n_{uv} = PW^n_{uv}/\sigma^2_{n_{uv,n}}$.

In order to obtain a positive LB, the MSE in step 2 should meet the condition $\eta^*_n < \frac{k_1 + k_3\eta^n_{be} + k_5\eta^n_{ae} + \eta^n_{ae}\eta^n_{be}}{k_2 + k_4\eta^n_{be} + k_6\eta^n_{ae}}$. The inequality can be inverted as $|\rho_1|^2 + |\rho_2|^2 < \frac{\eta_e + 1}{\eta^*_n + 1}$ if $\hat{\sigma}^2_{n_{ae,n}} = \hat{\sigma}^2_{n_{be,n}} = \hat{\sigma}^2_{n_{e,n}}$. Given the same channel quality and noise power, i.e., $\eta^n_{ab} = \eta^n_{ba} = \eta_e$, the system should meet the requirement of $|\rho_1|^2 + |\rho_2|^2 < 1$ to generate secret keys.

For $q = N+2, \ldots, Q$, Alice and Bob extract secret keys from the artificially-randomized channel. Due to $\hat{\sigma}_{n_{ab,r}} \leq \hat{\sigma}_{n_{ba,r}}$, we derive the LB of $C_{l_3}^{(q)}$ as

$$C_{l_3}^{(q)} = \log_2\left(1+\frac{g_1+g_3\eta_{be}^r+g_5\eta_{ae}^r+\eta_{ae}^r\eta_{be}^r-(g_2+g_4\eta_{be}^r+g_6\eta_{ae}^r)\eta_{ab}^r}{(\eta_{ae}^r\eta_{be}^r+\eta_{ae}^r+\eta_{be}^r+1)(\eta_{ab}^r+\eta_{ba}^r+\eta_{ab}^r\eta_{ba}^r)}\right), \tag{10}$$

where $g_1 = 1-|\rho_3|^2-|\rho_4|^2$, $g_2 = |\rho_3|^2+|\rho_4|^2$, $g_3 = 1-|\rho_3|^2$, $g_4 = |\rho_3|^2$, $g_5 = 1-|\rho_4|^2$, $g_6 = |\rho_4|^2$, $\eta_{uv}^r = \hat{\sigma}_{uv,r}/M_{uv} = 2/(T_l\gamma_{uv}^r)$ is the MSE of the artificially-randomized channel, $\gamma_{uv}^r = PM_{uv}/\sigma_{n_{be}}^2$ is the SNR, $M_{uv} = \mathbb{E}\left\{f_{uv}(t)\bar{f}_{uv}(t)\right\}$ is the channel variance, and ρ_3 (ρ_4) is the spatial correlation coefficients between $f_{ae}(t)$ ($f_{be}(t)$) and $f_{ab}(t)$ ($f_{ba}(t)$). To ensure a positive LB, the MSE should meet the condition of $\eta_{ab}^r < \frac{g_1+g_3\eta_{be}^r+g_5\eta_{ae}^r+\eta_{ae}^r\eta_{be}^r}{g_2+g_4\eta_{be}^r+g_6\eta_{ae}^r}$.

Next, we calculate the autocorrelation $\rho_{l,b}^{(q_3,q_4)}$ between Bob's q_3-th and q_4-th measurements from step 3 as

$$\rho_{l,b}^{(q_3,q_4)} = \frac{\frac{\sum_{n=1}^{q_1}\sigma_{br,n}^2\sigma_{ar,n}^2\mathbb{E}\{e^{j\theta_{n,q_3}}\}\mathbb{E}\{e^{-j\theta_{n,q_4}}\}}{\sum_{n=1}^{q_1}\sigma_{br,n}^2\sigma_{ar,n}^2}+\frac{\eta_{ab}^r}{2}}{\eta_{ab}^r+1}. \tag{11}$$

Due to $\theta_{n,q} \sim \mathcal{U}(0, 2\pi)$, $\mathbb{E}\{e^{-j\theta_{n,q}}\} \to 0$. Thus, $\rho_{l,b}^{(q_3,q_4)} \to 0$, when $\eta_{ab}^r \to 0$. As for Alice, the autocorrelation is given as

$$\rho_{l,a}^{(q_3,q_4)} = \frac{(\eta_{ba}^r+1)\mathbb{E}\{e^{j\theta_{n,q_3}}\}\mathbb{E}\{e^{-j\theta_{n,q_4}}\}}{\eta_{ba}^r+1}. \tag{12}$$

Thus, $\rho_{l,a}^{(q_3,q_4)} \to 0$, when $\mathbb{E}\{e^{-j\theta_{n,q}}\} \to 0$. The measurements from steps 3 and 4 can be viewed as independent RVs. The SKR is lower bounded as $C_{sk} \geq \frac{1}{T_c}\sum_q C_{l_1}^{(1)} + C_{l_2}^{(q)} + C_{l_3}^{(q)}$.

B. Upper Bound

For $q = 1$, according to [13], the UB of $C_{u_1}^{(1)}$ is given as

$$\log_2\left(\frac{\left((\eta_{ba}+1)(\eta_{ae}+1)-|\rho|^2\right)\left((\eta_{ab}+1)(\eta_{ae}+1)-|\rho|^2\right)}{(\eta_{ae}+1)\left((\eta_{ae}+1)\left((\eta_{ab}+\eta_{ba})+\eta_{ab}\eta_{ba}\right)-|\rho|^2(\eta_{ab}+\eta_{ba})\right)}\right). \tag{13}$$

For $q = 2, \ldots, N+1$, according to (6), we calculate the conditional mutual information given $\tilde{h}_{ae}^{(q)}$ and $\tilde{h}_{be}^{(q)}$ as

$$C_{u_2}^{(q)} = \log_2\left(1+\frac{(1-\frac{|\rho_1|^2}{\eta_{ae}^n+1}-\frac{|\rho_2|^2}{\eta_{be}^n+1})^2}{(\eta_{ba}^n+\eta_{ab}^n)(1-\frac{|\rho_1|^2}{\eta_{ae}^n+1}-\frac{|\rho_2|^2}{\eta_{be}^n+1})+\eta_{ba}^n\eta_{ab}^n}\right). \tag{14}$$

Next, we prove $I(\tilde{h}_{ba}^{(q)}, \tilde{h}_{ab}^{(q)} \mid \tilde{h}_{ae}^{(q)}, \tilde{h}_{be}^{(q)}) \leqslant I(\tilde{h}_{ab}^{(q)}, \tilde{h}_{ba}^{(q)})$. We firstly derive that $I(\tilde{h}_{ab}^{(q)}, \tilde{h}_{ba}^{(q)}) = \log_2\left(1+\frac{1}{\eta_{ba}^n+\eta_{ab}^n+\eta_{ba}^n\eta_{ab}^n}\right)$. Clearly, $I(\tilde{h}_{ab}^{(q)}, \tilde{h}_{ba}^{(q)} \mid \tilde{h}_{ae}^{(q)}, \tilde{h}_{be}^{(q)}) = I(\tilde{h}_{ba}^{(q)}, \tilde{h}_{ab}^{(q)})$ if $\eta_{ae}^n = +\infty$ and $\eta_{be}^n = +\infty$. Besides, $I(\tilde{h}_{ba}^{(q)}, \tilde{h}_{ab}^{(q)} \mid \tilde{h}_{ae}^{(q)}, \tilde{h}_{be}^{(q)})$ monotonically increases with η_{ae}^n and η_{be}^n, if they are positive.

For $q = N+2, \ldots, Q$, we similarly derive $C_{u_3}^{(q)}$ as

$$C_{u_3}^{(q)} = \log_2\left(1+\frac{(1-\frac{|\rho_3|^2}{\eta_{ae}^r+1}-\frac{|\rho_4|^2}{\eta_{be}^r+1})^2}{(\eta_{ab}^r+\eta_{ba}^r)(1-\frac{|\rho_3|^2}{\eta_{ae}^r+1}-\frac{|\rho_4|^2}{\eta_{be}^r+1})+\eta_{ab}^r\eta_{ba}^r}\right). \tag{15}$$

The SKR is upper bounded as $C_{sk} \leq \frac{1}{T_c}\sum_q C_{u_1}^{(1)} + C_{u_2}^{(q)} + C_{u_3}^{(q)}$. The UB and LB on the SKR are derived in the case of a single eavesdropper, but it can be expanded to the case of non-colluding multi-eavesdroppers by calculating the SKRs related to them and finding the minimum.

V. Simulation Results

This section presents the numerical results of the SKR analytical expression and validates it by Monte Carlo simulations. We use *ITE* toolbox [14] to calculate the mutual information. In all the following figures, markers denote the numerical results and different solid or dashed lines represent simulation results. The channel variance is $\sigma_{uv}^2 = \beta_0(d/d_0)^{-\zeta}$, where $\beta_0 = -30$ dB is the path loss at $d_0 = 1$ m, d is the link distance and ζ is the path-loss exponent that is set as 4 in indoor environments. The variance of the reflecting channel is $P_r = \sum_n \sigma_{ar,n}^2\sigma_{br,n}^2$ and that of the direct channel is $P_d = \sigma_{ab}^2$. Normalize P_r and P_d as $P_d + P_r = 1$, and set $\alpha = P_r/P_d$. The eavesdropping channel is modeled as $h_{ae} = 1/\sqrt{\beta}\rho h_{ab} + \sqrt{1-\rho^2}\omega$, so are $r_{ue,n}$ and $f_{ue}(t)$, where $\beta = \sigma_{ab}^2/\sigma_{ae}^2$, $\rho = J_0(2\pi d_{be}/\lambda)$, $\omega \sim \mathcal{CN}(0, \sigma_{ae}^2)$, $J_0(\cdot)$ is a zeroth-order Bessel function of the first kind and λ is the wavelength [3], [9]. Other parameters: $\lambda = 0.3$ m, $T = 300$, $B = 8$, $P_t = 20$ dBm and all noise power is -96 dBm. Two benchmarks are considered, i.e., no-RIS and TWP schemes.

Fig. 3 shows the SKR versus Alice's (Bob's) SNR when Eve's SNR = 20 dB. Also, two curves show the impact of the T_l on the SKR. When $T_l = 1$, the LB is less than 0 in a low SNR (equivalently high MSE) condition since the MSE is greater than the threshold. Another observation is $T_l = 5$ exhibits a larger performance gain compared to $T_l = 1$, because the MSE is suppressed by the longer pilot. When $T_l = 5$, the secret keys can be extracted securely though Alice's (Bob's) channel quality is poorer than Eve's, i.e., SNR < 20, since the ρ guarantees that the MSE is less than the threshold. What's more, Eve's passive eavesdropping induces the gap between the UB and the $I(\tilde{\mathbf{h}}_{ab}; \tilde{\mathbf{h}}_{ba})$ about 0.28 bit (13.5%) and 0.37 bit (11.3%) at $T_l = 1$ and $T_l = 5$, respectively, where $I(\tilde{\mathbf{h}}_{ab}; \tilde{\mathbf{h}}_{ba})$ is the SKR without the presence of Eve.

Fig. 4 investigates the impact of the ρ. As $|\rho| \to 1$, the LB and UB deviate from the $I(\tilde{\mathbf{h}}_{ab}; \tilde{\mathbf{h}}_{ba})$. If Eve gets close to Bob and the $|\rho|$ rises, the UB and LB decreases gradually and become loose. There is a trade-off between the LS estimation error in step 2 and the slots assigned for step 3. With the increment of N, the SKR increases initially and then decreases since the larger N increases the slots consumed in step 2 but reduces the slots for step 3. In Fig. 5, we perform the one-dimensional search and find $N^* = 48$ to maximize the UB.

Fig. 5 also demonstrates the $|\rho_l|$ versus N when the spatial correlation model in [10] is applied with the $\lambda/2$ element size.

$$C_{l_2,b}^{(q)} = \log_2\left(1+\frac{\frac{W_{ab}^n}{\hat{\sigma}_{n_{ba,n}}^2}\left[\frac{k_1W_{ab}^nW_{ae}^nW_{be}^n}{\hat{\sigma}_{n_{ab,n}}^2\hat{\sigma}_{n_{ae,n}}^2\hat{\sigma}_{n_{be,n}}^2}-\frac{k_2W_{ae}^nW_{be}^n}{\hat{\sigma}_{n_{ae,n}}^2\hat{\sigma}_{n_{be,n}}^2}+\frac{k_3W_{ab}^nW_{ae}^n}{\hat{\sigma}_{n_{ab,n}}^2\hat{\sigma}_{n_{ae,n}}^2}-\frac{k_4W_{ae}^n}{\hat{\sigma}_{n_{ae,n}}^2}+\frac{k_5W_{ab}^nW_{be}^n}{\hat{\sigma}_{n_{ab,n}}^2\hat{\sigma}_{n_{be,n}}^2}-\frac{k_6W_{be}^n}{\hat{\sigma}_{n_{be,n}}^2}+\frac{W_{ab}^n}{\hat{\sigma}_{n_{ab,n}}^2}\right]}{\left(\frac{W_{ae}^nW_{be}^n}{\hat{\sigma}_{n_{ae,n}}^2\hat{\sigma}_{n_{be,n}}^2}+\frac{W_{ae}^n}{\hat{\sigma}_{n_{ae}}^2}+\frac{W_{be}^n}{\hat{\sigma}_{n_{be,n}}^2}+1\right)\left(\frac{W_{ab}^n}{\hat{\sigma}_{ab,n}^2}+\frac{W_{ab}^n}{\hat{\sigma}_{ba,n}^2}+1\right)}\right). \tag{8}$$

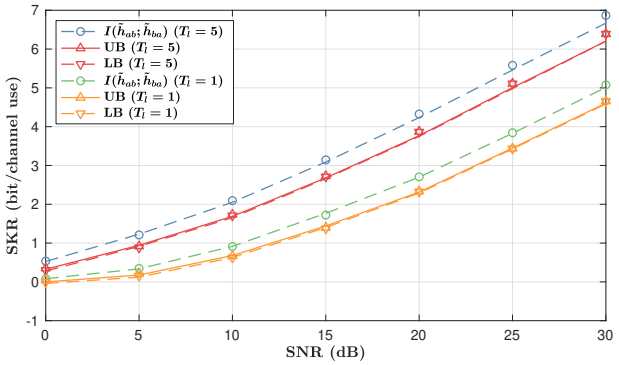

Fig. 3. SKR versus SNR ($d_{be}=0.064$ m, $N=64$, $\alpha=9$).

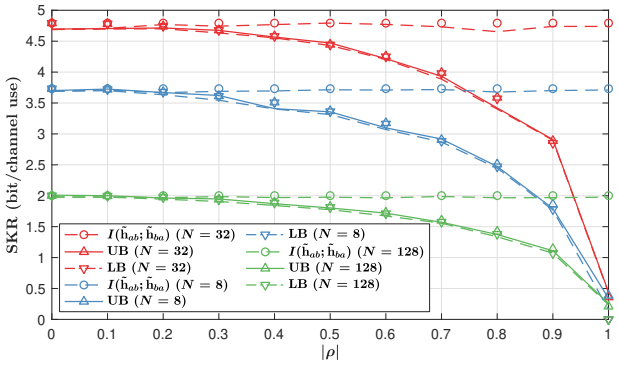

Fig. 4. SKR versus $|\rho|$ (SNR $=30$ dB, $\frac{P_r}{N}=-21$ dB, $T_l=1$, $\beta=1$).

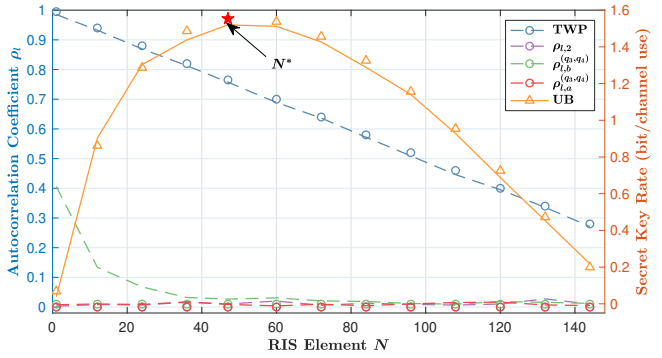

Fig. 5. ρ_l versus N ($d_{be}=0.064$ m, SNR = 20 dB, $\frac{P_r}{N}=-23$ dB, $\beta=1$, $T_l=1$).

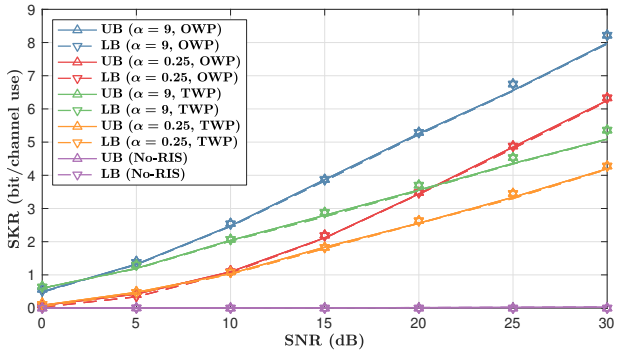

Fig. 6. Comparison with benchmarks ($d_{be}=0.072$ m, $N=32$, $T_l=5$).

The first observation is $\rho_{l,2}$ and $\rho_{l,a}^{(q_3,q_4)}$ are approximately equal to 0 in OWP scheme, which means the spatial correlation will not affect the autocorrelation coefficient seriously if the elements size equals $\lambda/2$. Also, $\rho_{l,b}^{(q_3,q_4)}$ decreases with N since the MSE is suppressed by the quality of the reflecting channel. In contrast, it is difficult for the TWP scheme in [7] to approach the UB when N is small, because the direct channel component results in the redundancy between channel measurements in one T_c.

Fig. 6 compares the proposed protocol with other benchmarks versus SNR with different α. TWP and OWP schemes outperform no-RIS scheme. Compared to TWP scheme, the UB and LB on the SKR of OWP scheme rises by an average of 0.64 bit (32.9%) and 1.15 bit (39.7%) when $\alpha=0.25$ and $\alpha=9$, respectively. If the direct component dominates the channel, i.e. $\alpha<1$, the performance of TWP scheme will get close to or exceed OWP scheme. The direct channel component increases the SNR in TWP scheme but leads to the autocorrelation of measurements.

VI. Conclusion

This letter proposed a RIS-assisted key generation protocol based on OWP scheme and investigated the SKR in the presence of an eavesdropper. We found the pilot length should ensure the MSE is small enough to generate secret keys. Also, we found the SKR is determined by the RIS elements, the correlation coefficient and the reflecting channel quality which impacts the autocorrelation of channel samples. Simulations validated that our protocol outperforms existing work.

References

[1] J. Zhang *et al.*, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138 406–138 446, Jul. 2020.
[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.
[3] N. Aldaghri *et al.*, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2692–2705, Feb. 2020.
[4] Z. Ji *et al.*, "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] X. Lu *et al.*, "Intelligent reflecting surface assisted secret key generation," *IEEE Signal Process. Lett.*, vol. 28, pp. 1036–1040, Feb. 2021.
[6] X. Hu *et al.*, "Intelligent reflecting surface-assisted secret key generation with discrete phase shifts in static environment," *IEEE Wireless Commun. Lett.*, May 2021, to be published.
[7] Z. Ji *et al.*, "Random shifting intelligent reflecting surface for OTP encrypted data transmission," *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1192–1196, Feb. 2021.
[8] C. You *et al.*, "Intelligent reflecting surface with discrete phase shifts: Channel estimation and passive beamforming," in *Proc. IEEE ICC 2020*, Dublin, Ireland, Jun. 2020, pp. 1–6.
[9] J. Zhang *et al.*, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, Jan. 2017.
[10] E. Björnson *et al.*, "Rayleigh fading modeling and channel hardening for reconfigurable intelligent surfaces," *IEEE Commun. Lett.*, vol. 10, no. 4, pp. 830–834, Apr. 2021.
[11] P. Staat *et al.*, "Intelligent reflecting surface-assisted wireless key generation for low-entropy environments," 2020, arXiv:2010.06613v2.
[12] J. Yang *et al.*, "RIS antenna aided secret key generation for static environment," 2021, techrxiv.14972196.v1.
[13] F. Rottenberg *et al.*, "CSI-based versus RSS-based secret-key generation under correlated eavesdropping," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1868–1881, Mar. 2021.
[14] Z. Szabó, "Information theoretical estimators toolbox," *Journal of Machine Learning Research*, vol. 15, pp. 283–287, Jan. 2014.