Enhancing Secret Key Generation in Block Fading Channels using Reconfigurable Intelligent Surfaces

Hibatallah Alwazani, Student Member, IEEE, Anas Chaaban, Senior Member, IEEE

Abstract-Physical-layer security (PLS) is superior to classical cryptography techniques due to its notion of perfect secrecy and independence to an eavesdropper's computational power. One form of PLS arises when Alice and Bob (the legitimate users) exchange signals to extract a common key from the random common channels. The drawback of extracting keys from wireless channels is the ample dependence on the dynamicity and fluctuations of the radio channel. However, some radio channels are constant such as line-of-sight (LoS) and can be estimated by Eve (an illegitimate user), or can be quite static in behavior due to the presence low-mobility users thus restricting the amount of randomness. This in turn lowers the secret key rate (SKR) defined as the number of bits of key generated per channel use. In this work, we aim to address this challenge by using a reconfigurable intelligent surface (RIS) to produce random phases at certain carefully curated intervals such that it disrupts the channel in low-entropy environments. We propose an RIS assisted key generation method, study its performance, and compare with benchmarks to observe the benefit of using an RIS while considering various important metrics such as key mismatch rate and average secret key throughput. Simulations are made to validate our theoretical findings showing an improvement in performance when an RIS is deployed.

I. INTRODUCTION

Physical layer security (PLS) provides means for information transmission that is provably secure. It is more desirable than classical cryptography [1] for several reasons [2]. First, there is no assumption made on the eavesdropper's computational power, they could have, in principle, unlimited computation power and still not be able to decipher the message in some scenarios. Second, it gives rise to the notion of perfect secrecy, where knowing the ciphertext at an eavesdropper tells it nothing about the message being exchanged. Finally, it is highly scalable [?], which is necessary for future generation networks as devices connected to the nodes may have varying power and computation capabilities.

Generally, for key-based secrecy, we face a fundamental question in cryptography: how do two parties share a secret key without compromising the key? In PLS, a key can be extracted from the wireless channel which acts as a common and unique source of randomness for Alice (the transmitter) and Bob (the receiver). This idea of generating random, common, and secret keys at two legitimate points from wireless channels is not new [3], [4]. It has been explored before but



Fig. 1: System model with an access point Alice, receiver Bob, RIS Rose, and eavesdropper Eve.

largely abandoned because of the fundamental limitation of low-entropy environments where channels vary slowly thereby producing low secret key rates (SKR) [5]. However, with the emergence of a smart radio environment enabled by the practical implementation of the reconfigurable intelligent surfaces (RIS)s, this limitation may be overcome [6]. Here, the RIS is abstracted as a large number of passive, scattering elements, where each element can be reconfigured to change the amplitude and/or phase of the impinging electromagnetic (EM) waves to achieve a desired objective, such as inducing channel variations in our case. Essentially, the RIS becomes a building block for a programmable and software-defined wireless environment [?]. Thus, this aspect in physical layer security (PLS) is undergoing a resurgence, with a focus on smart radio environment enabled secret key generation.

The authors in [7] present a novel wireless key generation architecture based on randomized channel responses from an RIS which act as the shared random source to Alice and Bob. They present their results using two metrics which are SKR and key mismatch rate (KMR). The authors in [8] propose a joint user allocation scheme and an RIS reflection parameter adjustment scheme to enhance key generation efficiency in a multi-user communication scenario. They compare the result against a scheme without an RIS and find that the RIS indeed boosts performance by reducing channel similarities between adjacent users and thus the enhancing efficiency of key generation.

The authors in [9] derive an upper bound on the SKR using

The authors are with the School of Engineering, the University of British Columbia, 1137 Alumni Ave., Kelowna, BC V1V1V7, Canada (email: {hibat97,anas.chaaban}@ubc.ca)

[2] and compare with another SKR upper bound without the presence of an RIS in the system. The work in [10] studies the minimum achievable SKR in the presence of an RIS and multiple passive eavesdroppers, where the authors optimize the minimum SKR by choosing appropriate RIS phase shifts. Here, the RIS works in a capacity to combat deleterious wireless channel conditions such as co-channel interference and dead zones. Moreover, [10] consider an RIS as a new degree of freedom in the channel, where the aim of the RIS is increasing correlation between legitimate nodes' channels and decreasing correlation with eavesdropping channels. However, [10] assumes that channel state information (CSI) is known at Alice and the RIS which is not practical.

In this paper, we study a practical secret key generation protocol, where CSI is initially unknown at all nodes. The RIS perturbs the block fading channel to induce more randomness in the channel. Then, channels are estimated and keys are generated over multiple blocks using the perturbed channel which changes faster than the original block fading channel, thanks to the RIS. The contributions of the paper can be summarized as follows:

- We formulate a theoretical achievable SKR lower bound for the proposed protocol.
- For a practical implementation of the protocol, we study the key mismatch rate (KMR) and the key throughput defined as the average number of key bits generated per transmission.
- We study the effect of the RIS in terms of several parameters such as the number of elements and the RIS switching rate.

In general, we notice a significant improvement in performance compared to the scenario without an RIS, where the key rate is limited due to the static nature of the channels within a fading block. To delve deeper into the results, we start by formulating the system model studied in this paper.

II. SYSTEM MODEL

Consider the setup depicted in Fig. 1, where a single antenna access point (Alice) serves a single-antenna user (Bob), in the presence of a passive eavesdropper (Eve) and an RIS (Rose) equipped with N elements controlled by Alice through a control link. To secure the communication, Alice and Bob generate a key through exchanging signals over the wireless channel, and use the key to encrypt the message to be transmitted. Eve knows the cryptosystem and the key generation protocol, and aims to discover the information exchanged between Alice and Bob.

As can be seen in Fig. 1, we denote by $h_{\rm ab}, h_{\rm ba} \in \mathbb{C}$ the channels from Alice to Bob and from Bob to Alice, respectively, by $h_{\rm ae}, h_{\rm be} \in \mathbb{C}$ the channels from Alice and Bob to Eve, respectively, by $\mathbf{h}_{\rm ar}, \mathbf{h}_{\rm br} \in \mathbb{C}^N$ the channels from Alice and Bob to Rose, respectively, and by $\mathbf{h}_{\rm ra}, \mathbf{h}_{\rm rb} \in \mathbb{C}^N$ the channels from Alice constraints from Rose to Alice, Bob, and Eve, respectively.

We assume block-fading channels in which all channels maintain constant values for T symbols and vary independently between blocks based on their respective distributions.



Generate secret keys from estimates

Fig. 2: Key generation time T_k split into multiple RIS switching periods with duration T_s from each of which a channel estimate is obtained at Alice (A) and Bob (B). The estimates are then put through a process to generate a common key.

We also assume a time-division duplexing (TDD) scheme, which implies that $h_{ba} = h_{ab}$, $\mathbf{h}_{ra} = (\mathbf{h}_{ar}^H)^T$, and $\mathbf{h}_{rb} = (\mathbf{h}_{br}^H)^T$ (reciprocal channels). Moreover, we assume independent Rayleigh fading so that

$$h_{ij} \sim \mathcal{CN}(0, \beta_{ij}) \tag{1}$$

$$\mathbf{h}_{\mathrm{r}i} \sim \mathcal{CN}(0, \beta_{\mathrm{r}i} \mathbf{I}_N) \tag{2}$$

for $i, j \in \{a, b, e\}$, where $\mathcal{CN}(0, \mathbf{Q})$ denotes a circularly symmetric complex Gaussian distribution with mean 0 and covariance matrix \mathbf{Q} .

The transmission time is divided between Alice and Bob for the sake of key generation and information transmission as shown in Fig. 2. To realize secure transmission, a transmission block of length T symbols representing a coherence interval is divided into T_k symbols used for key generation, and T_d symbols used for data transmission. We focus on the key generation phase in this work. During the key generation phase, Alice transmits during odd time slots, while Bob transmits during even time slots. Denoting the transmitted symbols by Alice and Bob by $x_{a,t} \in \mathbb{C}$ and $x_{b,t} \in \mathbb{C}$, respectively, which satisfy the power constraints $\sum_{t \text{ odd}} |x_{a,t}|^2 \leq \frac{T_k}{2}P$ and $\sum_{t \text{ even}} |x_{b,t}|^2 \leq \frac{T_k}{2}P$, the received signals can be written as

$$y_{i,t} = (h_{\mathrm{a}i} + \mathbf{h}_{\mathrm{a}r}^H \boldsymbol{\Phi}_t \mathbf{h}_{ri}) x_{\mathrm{a},t} + n_{i,t}, \quad i \in \{\mathrm{b},\mathrm{e}\}, \ t \text{ odd}, \quad (3)$$

$$y_{i,t} = (h_{\mathrm{b}i} + \mathbf{h}_{\mathrm{br}}^H \boldsymbol{\Phi}_t \mathbf{h}_{\mathrm{r}i}) x_{\mathrm{b},t} + n_{i,t}, \quad i \in \{\mathrm{a},\mathrm{e}\}, \ t \text{ even, (4)}$$

where

$$\mathbf{\Phi}_t = \operatorname{diag}([e^{j\theta_{t,1}}, \dots, e^{j\theta_{t,N}}]) \in \mathbb{C}^{N \times N},$$
(5)

is the reflection matrix for Rose in time slot $t, \theta_{t,n} \in [0, 2\pi]$ is the random phase-shift applied by element n, and $n_{a,t}, n_{b,t}, n_{e,t} \in \mathbb{C}$ are noise samples at Alice, Bob, and Eve, respectively, which are independent of each other, and are independent and identically distributed over time with distribution $\mathcal{CN}(0, \sigma^2)$. Using this transmission, Alice and Bob can generate a shared key $\mathbf{k} = (k_1, \ldots, k_r) \in \{0, 1\}^r$ where r is the total number of key bits. Since T_k is defined as the total number of symbols reserved for key generation at the two nodes, Alice and Bob split this portion in half for their

respective key generation as $\frac{T_k}{2}$. Thus, the secret key rate (SKR) in bits per symbol is defined as $R_k = \frac{r}{T_k/2}$, which is desired to be large. The end goal of Alice and Bob is to perform this key generation and extract k while preventing Eve from being able to discover the key.

III. KEY GENERATION AND SECRET KEY RATE

Alice and Bob use the random channel between them as a source of shared randomness to generate a key. Since the channel remains constant during a coherence interval of length T symbols, the RIS can help disrupt the channel by embedding additional randomness during a coherence interval. [18] introduces the concept of random reconfigurable surfaces (RRS) accounting for RISs that whose elements induce a timevariant phase shift on the reflected signals and present it as the diffusion function of an RIS. This is the same functionality we use for the RIS implementation detailed next.

A. Channel Estimation

Alice and Bob generate keys by estimating their channels (Fig. 2) and using the channel estimates as common randomness. To randomize the channel during a coherence interval, we consider an RIS which switches its phase-shift matrix Φ_t randomly every T_s symbols, with $T_s \leq T_k$ and $\theta_{t,n} \sim \text{Uniform}[0, 2\pi]$. Let the RIS phase shift matrix during switching period ℓ be represented by Φ_ℓ . Alice and Bob estimate the channel for each switching interval $\ell \in \{1, \ldots, \frac{T_k}{T_s}\}$. Alice and Bob send pilot signals $\mathbf{x}_{a,\ell}, \mathbf{x}_{b,\ell} \in \mathbb{C}^{T_s/2}$ in switching period ℓ during odd-indexed and even-indexed symbols, respectively, such that $\|\mathbf{x}_{a,\ell}\|^2 = \|\mathbf{x}_{a,\ell}\|^2 = \frac{T_s}{2}P$. Alice and Bob receive

$$\mathbf{y}_{\mathrm{a},\ell} = g_{\mathrm{ba}} \mathbf{x}_{\mathrm{b},\ell} + \mathbf{n}_{\mathrm{a},\ell},\tag{6}$$

$$\mathbf{y}_{\mathrm{b},\ell} = g_{\mathrm{ab}} \mathbf{x}_{\mathrm{a},\ell} + \mathbf{n}_{\mathrm{b},\ell},\tag{7}$$

where $g_{ba,\ell} = h_{ba} + \mathbf{h}_{br}^H \boldsymbol{\Phi}_{\ell} \mathbf{h}_{ra}$ and $g_{ab,\ell} = h_{ab} + \mathbf{h}_{ar}^H \boldsymbol{\Phi}_{\ell} \mathbf{h}_{rb} = g_{ba,\ell}$, and $\mathbf{n}_{a,\ell}$ and $\mathbf{n}_{b,\ell}$ collect the noise instances during switching period ℓ during odd-indexed and even -indexed symbols, respectively. Alice and Bob then estimate the channels $g_{ba,\ell}$ and $g_{ab,\ell}$ to be used as shared randomness as follows (using least-squares estimation)

$$\bar{g}_{\mathrm{ba},\ell} = \mathbf{y}_{\mathrm{a},\ell}^{H} \frac{\mathbf{x}_{\mathrm{b},\ell}}{\|\mathbf{x}_{\mathrm{b},\ell}\|^{2}} = g_{\mathrm{ba},\ell} + \bar{n}_{\mathrm{ba},\ell}, \qquad (8)$$

$$\bar{g}_{\mathrm{ab},\ell} = \mathbf{y}_{\mathrm{b},\ell}^H \frac{\mathbf{x}_{\mathrm{a},\ell}}{\|\mathbf{x}_{\mathrm{a},\ell}\|^2} = g_{\mathrm{ab},\ell} + \bar{n}_{\mathrm{ab},\ell},\tag{9}$$

where $\bar{n}_{\mathrm{ba},\ell} = \frac{\mathbf{n}_{\mathrm{a},\ell}^{\mathbf{n}} \mathbf{x}_{\mathrm{b},\ell}}{\|\mathbf{x}_{\mathrm{b},\ell}\|^2}$ and $\bar{n}_{\mathrm{ab},\ell} = \frac{\mathbf{n}_{\mathrm{b},\ell}^{\mathbf{H}} \mathbf{x}_{\mathrm{a},\ell}}{\|\mathbf{x}_{\mathrm{a},\ell}\|^2}$ are independent $\mathcal{CN}(0,\bar{\sigma}^2)$ noises with $\bar{\sigma}^2 = \frac{2\sigma^2}{T_{\mathrm{s}}P}$. During the same time, Eve obtains the following estimates similarly

$$\bar{g}_{\mathrm{be},\ell} = g_{\mathrm{be},\ell} + \bar{n}_{\mathrm{be},\ell},\tag{10}$$

$$\bar{q}_{\mathrm{ae},\ell} = q_{\mathrm{ae},\ell} + \bar{n}_{\mathrm{ae},\ell},\tag{11}$$

where $g_{be,\ell} = h_{be} + \mathbf{h}_{br}^H \boldsymbol{\Phi}_{\ell} \mathbf{h}_{re}$, $g_{ae,\ell} = h_{ae} + \mathbf{h}_{ar}^H \boldsymbol{\Phi}_{\ell} \mathbf{h}_{re}$, and $\bar{n}_{be,\ell}$ and $\bar{n}_{ae,\ell}$ are independent $\mathcal{CN}(0,\bar{\sigma}^2)$ noises.

Next, Alice and Bob use the estimates $\bar{g}_{ba,\ell}$ and $\bar{g}_{ab,\ell}$ (which are dependent) to generate their shared key (as in [12, Ch. 22]). Note that since the channels are assumed to not vary

during a coherence block and to vary between blocks, the channel estimates will not be independently and identically distributed (i.i.d.) across multiple blocks. However, Alice and Bob can use the ℓ^{th} switching period in multiple coherence blocks to generate one key, making the estimates used to generate a given key i.i.d. as desired. This means that $\frac{T_k}{T_s}$ keys can be generated simultaneously. Alternatively, we can use interleaving to obtain a pseudo-i.i.d. estimates by taking the estimates from the first switching periods from a set of blocks, followed by the estimates from the second switching period, and so on. Next, we characterize the SKR.

B. Secret Key Rate

Let the estimates $\bar{g}_{\mathrm{ba},\ell}$, $\bar{g}_{\mathrm{ab},\ell}$, $\bar{g}_{\mathrm{be},\ell}$ and $\bar{g}_{\mathrm{ae},\ell}$ be represented by random variables \bar{G}_{ba} , \bar{G}_{ab} , \bar{G}_{be} and \bar{G}_{ae} , respectively. The SKR can be lower bounded by

$$R_{\rm k} \ge \frac{1}{T_{\rm s}/2} R_{\rm k}^{\rm lb},$$

where [2]

$$R_{k}^{lb} \triangleq I(\bar{G}_{ab}; \bar{G}_{ba})$$

$$- \min\{I(\bar{G}_{ab}; \bar{G}_{ae}, \bar{G}_{be}), I(\bar{G}_{ba}; \bar{G}_{ae}, \bar{G}_{be})\},$$

$$= -h(\bar{G}_{ab}|\bar{G}_{ba})$$

$$+ \max\{h(\bar{G}_{ab}|\bar{G}_{ae}, \bar{G}_{be}), h(\bar{G}_{ba}|\bar{G}_{ae}, \bar{G}_{be})\},$$

$$(12)$$

I(X;Y) is the mutual information, h(X|Y) is the conditional entropy, and the factor $\frac{1}{T_s/2}$ follows because there are $\frac{T_k}{T_s}$ channel estimates in key generation phase of duration T_k . To simplify this lower bound, we need to study the distributions of the channel estimates. We first note that $\bar{G}_{\rm ba}$, $\bar{G}_{\rm ab}$, $\bar{G}_{\rm be}$ and $\bar{G}_{\rm ae}$ have zero mean. Moreover, the covariances of the channels are given by

$$\rho_{ab} = \mathbb{E}[G_{ab}G_{ab}^*] = \mathbb{E}[G_{ab}G_{ba}^*] = \mathbb{E}[G_{ba}G_{ba}^*]$$

$$= \beta_{ab} + N\beta_{ar}\beta_{rb}, \qquad (13)$$

$$\rho_{ae} = \mathbb{E}[G_{ae}G_{ae}] = \rho_{ae} + N\rho_{ar}\rho_{re}, \qquad (14)$$

$$p_{\rm be} = \mathbb{E}[G_{\rm be}G_{\rm be}^*] = \beta_{\rm be}^2 + N\beta_{\rm br}\beta_{\rm re},\tag{15}$$

Then,

$$\operatorname{Cov}\left([\bar{G}_{\mathrm{ab}}\ \bar{G}_{\mathrm{ba}}]^{T}\right) = \begin{bmatrix} \rho_{\mathrm{ab}} + \bar{\sigma}^{2} & \rho_{\mathrm{ab}} \\ \rho_{\mathrm{ab}} & \rho_{\mathrm{ab}} + \bar{\sigma}^{2} \end{bmatrix}, \quad (16)$$

$$\operatorname{Cov}\left([\bar{G}_{ab}\ \bar{G}_{ae}\ \bar{G}_{be}]^{T}\right) = \operatorname{Cov}\left([\bar{G}_{ba}\ \bar{G}_{ae}\ \bar{G}_{be}]^{T}\right) \quad (17)$$
$$= \begin{bmatrix} \rho_{ab} + \bar{\sigma}^{2} & 0 & 0\\ 0 & \rho_{ae} + \bar{\sigma}^{2} & 0\\ 0 & 0 & \rho_{be} + \bar{\sigma}^{2} \end{bmatrix}.$$

Finally, we need the following statement to characterize the distribution of the estimates.

Lemma 1: Given circularly symmetric complex Gaussian channels, the aggregate channel $g_{ij,\ell} = h_{ij} + \mathbf{h}_{ir}^H \boldsymbol{\Phi}_{\ell} \mathbf{h}_{rj}, i \in \{a, b\}, j \in \{a, b, e\}, j \neq i$, can be modeled as a circularly symmetric complex Gaussian when N is large.

Proof: The statement is a consequence of the central limit theorem, and can be proved similar to [14, Lemma 2].

Based on this, the lower bound $R_{\rm k}^{\rm lb}$ can be simplified as follows.

Theorem 1: The SKR lower bound in (12) simplifies to

$$R_{\rm k}^{\rm lb} = \frac{1}{T_{\rm s}/2} \log_2 \left(1 + \frac{\rho_{\rm ab}^2}{\bar{\sigma}^2 (2\rho_{\rm ab} + \bar{\sigma}^2)} \right).$$
(18)

Proof: The statement is obtained by evaluating (12) with circularly symmetric complex Gaussian channel estimates (using Lemma 1) and the covariance matrices in (16) and (17).

Next, we present a protocol for secret key generation using this system.

IV. PROTOCOL FOR SECRET KEY GENERATION

In this section, we introduce a novel method for creating keys using several coherence blocks. Over several blocks $f = 1, \ldots, F$, we create $\frac{T_k}{T_s}$ keys. The number of estimates to be used for each key is F. In the ℓ^{th} switching period in multiple F blocks, Alice and Bob generate keys $\mathbf{k}_{a,\ell}$ and $\mathbf{k}_{b,\ell}$, respectively. If $\mathbf{k}_{a,\ell} = \mathbf{k}_{b,\ell} = \mathbf{k}_{\ell}$, i.e., the keys match, they are used for encryption. Otherwise, key ℓ is discarded. In general, some of the $\frac{T_k}{T_s}$ keys generated during F blocks will match and will be used for encryption. The process is repeated every F blocks.

A. Quantization of Channel Estimates

Following [20], Alice generates key bits from each block f by quantizing the phase of its channel estimate $\bar{g}_{ba,\ell}$ given by

$$\theta_{\mathrm{ba},\ell} = \tan^{-1}\left(\frac{\mathrm{imag}(\bar{g}_{\mathrm{ba},\ell})}{\mathrm{real}(\bar{g}_{\mathrm{ba},\ell})}\right), \ell = 1, \dots, \frac{T_{\mathrm{k}}}{T_{\mathrm{s}}}.$$
 (19)

Bob also does the same using the estimate $\bar{g}_{ab,\ell}$. This happens over the several blocks F until we obtain all the phases of all channel estimates. We define the quantization of the phase using a function $f_Q : \mathbb{R} \to \{1, \ldots, Q\}$, where Q is the number of quantization levels, such that

$$\theta_{ij,\ell}^Q = f_Q(\theta_{ij,\ell}) = q, \text{ if } \theta_{ij,\ell} \in \left(\frac{2\pi(q-1)}{Q}, \frac{2\pi(q)}{Q}\right), (20)$$

for q = 1, ..., Q, $i \in \{a, b\}$ with $i \neq j$. Thus, one channel estimate generates a random phase value that yields $\log_2(Q)$ key bits. The total number of key bits in key ℓ denoted by Lis thus

$$L = F \log_2(Q) \text{ bits.}$$
(21)

Note that a larger Q increases the number of key bits at the expense of higher mismatch probability as discussed next.

B. Key Mismatch Rate and Throughput Analysis

For each of the $\frac{T_{\rm k}}{T_{\rm s}}$ keys, we can define key mismatch rate (KMR) as

$$P(\mathbf{k}_{\mathrm{a},\ell} \neq \mathbf{k}_{\mathrm{b},\ell}) = 1 - p, \ \ell = 1, \dots, \frac{T_{\mathrm{k}}}{T_{\mathrm{s}}},$$
(22)

where p is the probability that two keys match and amounts to

$$p = [P(\theta_{\mathrm{ba},\ell}^Q = \theta_{\mathrm{ab},\ell}^Q)]^F$$
(23)

Parameter	Value
T_k	40 symbols
F	100 blocks
Noise level	30 dBm
P	1W
$\beta_{ab} = \beta_{ae} = \beta_{be}$	1
$\beta_{ar} = \beta_{rb} = \beta_{re}$	0.7

TABLE I: Simulation Parameters.

in which $\theta_{ba,\ell}^Q$ and $\theta_{ab,\ell}^Q$ are as defined in (20).¹ After every key extraction round which extends over F blocks, Alice and Bob check whether they have matching keys. If not, the key is discarded, so that only matching keys are used for encryption. Thus, the number of trials n until a key match occurs for key ℓ can be modelled as geometrically distributed random variable X such that

$$P(X = n) = (1 - p)^{n-1}p, \ n = 1, 2, 3, \dots$$
 (24)

The average number of handshakes \bar{n} until success is given as

$$\bar{n} = \mathbb{E}[X] = \sum_{n=1}^{\infty} (1-p)^{n-1}n = \frac{1}{p}.$$
 (25)

Then, the average key throughput R_k can be found as the length of key ℓ which is $F \log_2(Q)$ multiplied by the number of keys in F frames which is $\frac{T_k}{T_s}$, divided by the total symbols allocated per node (Alice and Bob) $F \frac{T_k}{2}$ divided by the average number of handshakes $\frac{1}{n}$, yielding

$$\bar{R}_{\rm k} = \frac{p \log_2(Q)}{T_{\rm s}/2}$$
 bits per symbol. (26)

Next, we show simulations that show the effect of RIS on the key generation in terms of number of elements N and switching period T_s .

V. SIMULATIONS AND RESULTS

To evaluate the performance of the proposed protocol, we simulate it for a system with parameters provided in Table I.

We start by evaluating the KMR of the protocol. Fig. 3 shows the KMR of the protocol versus N for different scenarios: a system without an RIS in which the channels only consist of direct channels, i.e. $g_{ba,\ell} = h_{ba}$ and $g_{ab,\ell} = h_{ab}$, and a system with an RIS without switching where $T_s = T_k$, RIS with switching where $T_s = 10$ symbols, and with switching rate. The results show that using an RIS with no switching garners the smallest KMR because it leads to better channel estimate due to the longer channel probing time, and still performs better than a system without an RIS because the added RIS channels improves the overall channel gains. On the other hand, an RIS with $T_s = 2$ shows the worst performance in terms of KMR because the number of channel probing time is just one symbol for each of Alice and Bob, leading to poor

¹After generating a key (quantization), information reconciliation takes place [3] in order to detect and resolve key mismatch scenarios.



Number of elements N

Fig. 3: Key mismatch rate versus number of RIS elements N for different switching rates of the RIS as well as a no RIS scenario.

estimation accuracy and hence higher mismatch rate. However, with increasing N, the performances improves to rival the case with no RIS scenario due to the improved received signal corresponding to the increased number of reflectors.

In Fig. 4, we plot the KMR versus the signal-to-noise ratio (SNR) defined as SNR = $\frac{P}{\sigma^2}$, for different quantization levels Q = 2, 4, 8. All considered simulation scenarios show a downwards trend as SNR increases which is expected since the channel estimation quality improves. Moreover, we can observe the effect of quantization on the KMR in the figure. The effect of Q on the KMR can be seen implicitly in (23) where the match probability p decreases as Q increases because the quantization resolution increases and it becomes more likely that quantized phases extracted at Alice and Bob do not match. This explains why the highest KMR in the figure is for a system with an RIS with $T_s = 2$ and Q = 8. To summarize, KMR is affected primarily by Q and T_s , increasing T_s leads to lower KMR whilst increasing Q leads to higher KMR.

The average key throughput \bar{R}_k defined in (26) is depicted in Fig. 5 versus the number of RIS elements N. We see that a system with an RIS with $T_s = T_k$ has the lowest throughput and is comparable with the case of no RIS in the system. However, despite the higher KMR for the cases with $T_s = 2$ and 10, their average key throughput is higher. In the same figure, we plot the theoretical secret key rate lower bound $R_k^{\rm lb}$ given in (18) for the case with RIS $T_s = 2$ in order to compare it against the experimental throughput. In all cases, the average key throughput increases initially with increasing N due to the dependence of channel gains on N, and then stagnates after a certain N value. This is because the average key throughput depends on N through the match probability p. After a certain N value, p equals one and there is no gain in increasing N further.



Fig. 4: Key mismatch rate versus SNR for different quantization levels.



Fig. 5: Average key throughput versus N.

Finally, Fig. 6 shows the average throughput versus SNR, for different quantization levels. Note that Q has an implicit adverse effect on \overline{R}_k through p as well as an explicit positive effect manifested by the increase of $\log_2(Q)$ with Q. We see that the $\log_2(Q)$ term dominates in the expression as evident by the RIS with $T_s = 2$, Q = 8 having the best average key throughput. Note that at certain high SNR, the theoretical secret key rate lower bound $R_k^{\rm lb}$ exceeds the experimental throughputs. This is because the simulated protocol only uses the channel phases and neglects channel amplitudes, whereas both are used in the derivation of the theoretical lower bound on $R_k^{\rm lb}$.

VI. CONCLUSION

In this paper, we study the RIS effect in enhancing key generation, where the RIS provides a two-fold enhancement by adding additional channels and by perturbing the static



Fig. 6: Average key throughput versus SNR.

channel in order to obtain a higher key rate. We formulate an expression for the theoretical achievable SKR lower bound using our proposed system model under block fading channels. Moreover, we derive the average key throughput for a proposed protocol and further study the effect of changing RIS parameters such as the number of elements N and the switching rate of the RIS T_s , as well as system parameters such as the quantization Q on the key throughput. Using theoretical findings and simulations, we discover that increasing N and Qwhile decreasing T_s yields the highest average key throughput. Future directions and extensions include finding the optimal parameters for the key throughput and investigating other channel models such as Ricean fading.

REFERENCES

- W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory (2nd Edition)*. USA: Prentice-Hall, Inc., 2005.
- [2] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.
- [3] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.
- [4] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.
- [5] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, 2013.
- [6] M. Di Renzo, m. Debbah, D.-T. Phan-Huy, A. Zappone, M.-S. Alouini, C. Yuen, V. Sciancalepore, G. Alexandropoulos, J. Hoydis, H. Gacanin, J. Rosny, A. Bounceur, G. Lerosey, and M. Fink, "Smart radio environments empowered by reconfigurable ai meta-surfaces: an idea whose time has come," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, 05 2019.
- [7] P. Staat, H. Elders-Boll, M. Heinrichs, R. Kronberger, C. T. Zenger, and C. Paar, "Intelligent reflecting surface-assisted wireless key generation for low-entropy environments," *CoRR*, vol. abs/2010.06613, 2020. [Online]. Available: https://arxiv.org/abs/2010.06613
- [8] Y. Gao, D. Guo, J. Xiong, and D. Ma, "Intelligent reflecting surface assisted multi-user robust secret key generation for low-entropy environments," *Entropy*, vol. 23, no. 10, 2021. [Online]. Available: https://www.mdpi.com/1099-4300/23/10/1342

- [9] Y. Chen, G. Li, C. Pan, L. Hu, and A. Hu, "Intelligent reflecting surfaceassisted secret key generation in multi-antenna network," 2021.
- [10] Z. Ji, P. L. Yeoh, D. Zhang, G. Chen, Y. Zhang, Z. He, H. Yin, and Y. Ii, "Secret key generation for intelligent reflecting surface assisted wireless communication networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 1030–1034, 2021.
- [11] E. Björnson and L. Sanguinetti, "Rayleigh fading modeling and channel hardening for reconfigurable intelligent surfaces," *IEEE Wireless Communications Letters*, vol. 10, no. 4, pp. 830–834, 2021.
- [12] A. El Gamal and Y.-H. Kim, Network Information Theory. Cambridge University Press, 2011.
- [13] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020.
- [14] Z. Ding, R. Schober, and H. V. Poor, "On the impact of phase shifting designs on irs-noma," *IEEE Wireless Communications Letters*, vol. PP, pp. 1–1, 04 2020.
- [15] Q.-U.-A. Nadeem *et al.*, "Intelligent reflecting surface assisted multi-user miso communication: Channel estimation and beamforming design," *IEEE Open J. Commun. Soc.*, vol. PP, pp. 1–1, May 2020.
- [16] Q.-U.-A. Nadeem, A. Chaaban, and M. Debbah, "Opportunistic beamforming using an intelligent reflecting surface without instantaneous csi," *IEEE Wireless Communications Letters*, vol. 10, pp. 146–150, 2021.
- [17] P. Viswanath, D. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1277–1294, 2002.
- [18] S. A. Tegos, D. Tyrovolas, P. D. Diamantoulakis, C. K. Liaskos, and G. K. Karagiannidis, "On the distribution of the sum of doublenakagami-*m* random vectors and application in randomly reconfigurable surfaces," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7297–7307, 2022.
- [19] Q.-U.-A. Nadeem, A. Zappone, and A. Chaaban, "Intelligent reflecting surface enabled random rotations scheme for the miso broadcast channel," *IEEE Transactions on Wireless Communications*, vol. 20, no. 8, pp. 5226–5242, 2021.
- [20] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in 2008 IEEE International Conference on Acoustics, Speech and Signal Processing, 2008, pp. 3013–3016.
- [21] Z. Ji, P. L. Yeoh, G. Chen, C. Pan, Y. Zhang, Z. He, H. Yin, and Y. Li, "Random shifting intelligent reflecting surface for otp encrypted data transmission," *IEEE Wireless Communications Letters*, vol. 10, no. 6, pp. 1192–1196, 2021.