In: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), 26-29 September 2022, London, UK
DOI:10.1109/VTC2022-Fall57202.2022.10012819

Secret Key Rate Upper-bound for Reconfigurable Intelligent Surface-combined System under Spoofing

Zhuangkun Wei
School of Aerospace,
Transport and Manufacturing,
Cranfield University,
Milton Keynes, UK, MK43 0AL
zhuangkun.wei@cranfield.ac.uk

Liang Wang
School of Aerospace,
Transport and Manufacturing,
Cranfield University,
Milton Keynes, UK, MK43 0AL
liang.wang.133@cranfield.ac.uk

Weisi Guo
School of Aerospace,
Transport and Manufacturing,
Cranfield University,
Milton Keynes, UK, MK43 0AL
weisi.guo@cranfield.ac.uk

***Abstract*—Reconfigurable intelligent surfaces (RIS) have been shown to improve the secret key rate (SKR) for physical layer secret key generation (PL-SKG), by using the programmable phase shifts to increase reciprocal channel entropy. Most current studies consider the role of RIS on passive eavesdroppers (Eves) and overlook active attackers, especially the pilot spoofing attacks (PSA). For PSA in PL-SKG setups, this is implemented by Eve sending an amplified pilot sequence simultaneously with legitimate user Alice. With the increase of the spoofing amplifying factor, the channel probing results at Bob and Eve become similar, thereby enabling Eve to generate shared secret key with Bob. In this work, we analyze how RIS can positively or negatively affect the PL-SKG under pilot spoofing. To do so, we theoretically express the legitimate and spoofing SKRs in terms of the RIS phase shifts. Leveraging this, the closed-form theoretical upper bounds of both legitimate and spoofing SKRs are deduced, which lead to two further findings. First, the legitimate SKR upper-bound does not vary with RIS phase shift vector, but reduces drastically with the increase of the spoofing amplifying factor. This suggests the limited effect of RIS against PL-SKG spoofing, since the legitimate SKR has a hard limit, which cannot be surpassed by adjusting RIS phase and reflecting power, but can even be 0 with properly assigned spoofing amplifying factor. Second, the spoofing SKR upper-bound shows a large gap from the non-optimized SKR, which indicates a potential for RIS phase optimization.**

***Index Terms*—Physical layer secret key, spoofing, reconfigurable intelligent surfaces, wireless communications.**

I. Introduction

Reconfigurable intelligent surface (RIS) has demonstrated great potential on programming the wireless channel state, which motivates and facilitates a plethora of research and industrial topics [1]. Among these is how a RIS can secure the physical layer of wireless channels. The research in this area can be categorized as key-less physical layer security (PLS) [2]–[4], and physical layer secret key generation (PL-SKG) [5]–[12].

A. RIS Research in PLS

Key-less PLS tries to create a superiority of the legitimate channels over the wiretap ones. They do so by maximizing the secrecy capacity in terms of the legitimate receiving signal to interference and noise ratio (SINR), via the optimization of the key variables, e.g., transmitter/receiver beamforming vectors [2], [3], and the trajectory of a mobile legitimate user [4]. With the help of RIS, its programmable phase shift vector can be exploited, which serves as a new domain-of-free (DoF) and is able to further enhance the superior secrecy rate among legitimate users, even with multiple eavesdroppers (Eves).

Another family is PL-SKG, which leverages the reciprocal channel randomness that is common at legitimate users to generate shared secret key [13]. To do so, two legitimate users (Alice and Bob) send pilot sequences in the time-division duplexing (TDD) mode to pursue channel probing, and use their common channel probing results for secret key generation. The challenge lies in the low secret key rate (SKR) due to the insufficient small-scale scattering, rendering the PL-SKG incompatible with the current Gbps order of data transmission. RIS's role here is to increase SKR, by (i) introducing extra randomness (entropy) via random phase shift strategy [6]–[9], or (ii) finding optimal fixed phase shift according to the statistical channel state information [10]–[12].

B. Lack of RIS Research in Spoofing Attacks

Most of the existing RIS-combined PLS studies only considered weak attackers (e.g., passive, and non-colluded Eve). Examples of more active attackers include multiple colluding Eves [14], and adversarial RIS is studied in [15]. However, there is still a lack on how RIS can defend or assist active attackers. In the context of active attacks, pilot spoofing attack (PSA) proposed by [16], has been proved to cause severe consequences (50% throughput reduction [17]). PSA can be easily implemented by an Eve sending an amplified pilot sequence in the same time-slot with legitimate user (e.g., Alice), so, the legitimate channel probing result (at Bob) will be the weighted combination of legitimate Alice-Bob link with the eavesdropping (Eve-Bob) link. As a consequence, Bob will design false beamforming vector for key-less PLS (referred to as key-less PLS spoofing), or generate shared secret key with Eve other than Alice in PL-SKG (referred to as PL-SKG spoofing). Combining PSA and RIS, the works in [18], [19] studied the RIS-assisted spoofing to further destroy the key-less PLS. Yet, there is a lack of analysis on how RIS can be used to defend the PL-SKG spoofing, or used by Eve to further destroy legitimate secret key, and this constitutes the motivation of this work.

In this work, we aim to study how RIS can affect the PL-SKG under pilot spoofing. We start by formulating the RIS combined PL-SKG scenario with a spoofing Eve (in Section II), where the channel probing results at Alice, Bob and Eve are provided. Then, in Section III, we compute the theoretical legitimate SKR and spoofing SKR, in terms of the RIS phase vector. Leveraging this, two closed-form upper-bound of legitimate and spoofing SKRs are then deduced, and two conclusions are provided. First, the legitimate SKR upper-bound does not vary with RIS phase shift vector, but reduces drastically with the increase of the spoofing amplifying factor. This suggests the limited effect of RIS against PL-SKG spoofing, since the legitimate SKR has a hard limit (the upper-bound), which cannot be surpassed by adjusting RIS phase and reflecting power, and can even be 0 with properly assigned spoofing amplifying factor. Second, the spoofing SKR upper-bound shows a large gap from the non-optimized SKR, which indicates a potential for adversarial RIS phase optimization. We therefore hope our work can provide a guideline for further studies of RIS combined pilot spoofing defense and attacks.

II. System Model & Problem Formulation

A. RIS-combined PL-SKG under Spoofing Eve

In this work, we consider a RIS-combined mm-wave communication system in Fig. 1, which comprises a pair of legitimate users (Alice and Bob with single-antenna), an illegal spoofing Eve (single-antenna), and a RIS (a uniform planar array with $M = M_x \times M_y$ reflecting elements). The direct channels from node $a \in \{A, B, S\}$ to RIS is modelled as Rayleigh fading channel [20], i.e., $\mathbf{g}_{aR} \sim \mathcal{CN}(0, 2\mathbf{\Sigma}_{aR})$ where $\mathbf{\Sigma}_{aR}$ of size $M \times M$ is the covariance matrix. And we assume that the direct wireless channels among Alice, Bob and spoofing Eve are blocked [12].

The RIS-combined PL-SKG process under spoofing is briefly described in the following. First, RIS phase vector, denoted as $\mathbf{w} \triangleq [\beta_1 e^{j\theta_1}, \cdots, \beta_M e^{j\theta_M}]^T$ with $\beta_m \in \mathbb{R}, \theta_m \in [0, 2\pi)$, is configured (by either legitimate users or spoofing Eve), according to the statistical channel correlation matrices (detailed in Section III). Then, Alice and Bob pursue channel probing by sending public pilot sequence in TDD mode, i.e., in two consecutive time slots. For spoofing purpose, the spoofing Eve sends an amplified Alice's pilot sequence simultaneously in the Alice's sending time slot. As such, the channel probing results (using least squared method) at Alice, Bob and spoofing Eve are:

$$\begin{aligned} \hat{h}_A &= \mathbf{g}_{AR}^T \cdot diag(\mathbf{w}) \cdot \mathbf{g}_{BR} + \epsilon_A, \\ \hat{h}_B &= \mathbf{g}_{BR}^T \cdot diag(\mathbf{w}) \cdot (\mathbf{g}_{AR} + \rho \cdot \mathbf{g}_{SR}) + \epsilon_B, \\ \hat{h}_S &= \mathbf{g}_{SR}^T \cdot diag(\mathbf{w}) \cdot \mathbf{g}_{BR} + \epsilon_S. \end{aligned} \tag{1}$$

where ρ is the amplifying factor by the spoofing Eve, and $\epsilon_A, \epsilon_B, \epsilon_S \sim \mathcal{CN}(0, 2\sigma_\epsilon^2)$ are the channel probing noises. From Eq. (1), the secret key between Alice and Bob (between the spoofing Eve and Bob) can be generated by feeding $\hat{h}_A$ and $\hat{h}_B$ ($\hat{h}_S$ and $\hat{h}_B$) into further key quantization, key reconciliation and privacy amplification modules.

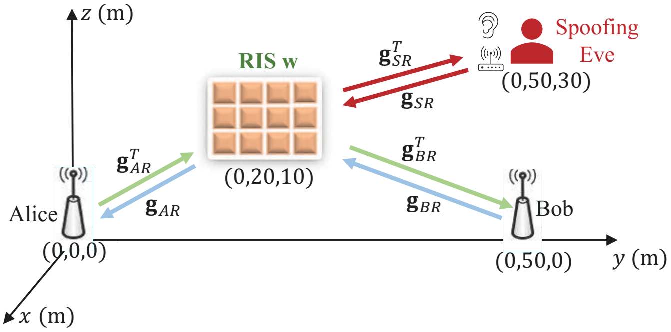

Fig. 1. Illustration of RIS-combined Alice, Bob and spoofing Eve model.

B. Problem Formulation

Observing from Eq. (1), it can be seen that the performances of the legitimate key and the spoofing key are determined by the spoofing amplifying factor ρ: A large ρ will lead to a reduced match rate of legitimate secret key but a large match rate between the spoofing Eve and Bob. Different from previous spoofing research, the introduction of RIS gives another DoF and may provide constructive/destructive effects in front of spoofing, which however has not been studied. Motivated by this, our work aims to analyze (i) how RIS can improve the legitimate PL-SKG under spoofing and (ii) how RIS can assist the spoofing attacks.

III. Effects of RIS on PL-SKG Spoofing

In this section, we analyze the constructive and destructive effects of RIS on PL-SKG under spoofing. We first provide the closed-form expressions of the legitimate and spoofing SKRs. Then, their upper-bound are deduced and analyzed.

A. Legitimate and Spoofing SKRs

The legitimate SKR is defined as

$$SKR_L \triangleq \max\left\{ I\left(\hat{h}_A; \hat{h}_B\right) - I\left(\hat{h}_S; \hat{h}_B\right), 0 \right\}, \tag{2}$$

where $I(\cdot;\cdot)$ denotes the mutual information. In Eq. (2), the legitimate SKR is interpreted as the mutual information between Alice and Bob minus that between Bob and spoofing Eve. This is because that as legitimate users, they consider not only how common between their channel probing results, but the difference of their channel probing from attackers to prevent eavesdropping.

Different from legitimate SKR, the spoofing SKR only requires the commonality of the channel probing results between the spoofing Eve and legitimate user (i.e., Bob in this work), so that the secret keys generated at Eve and Bob are similar. In this view, we define the spoofing SKR as:

$$SKR_S \triangleq I\left(\hat{h}_S; \hat{h}_B\right). \tag{3}$$

The deductions of SKR_L and SKR_S are pursued by (i) computing the joint and marginal probability distribution functions (PDFs) of $\hat{h}_A$, $\hat{h}_B$ and $\hat{h}_S$, and (ii) compute $I(\hat{h}_A;\hat{h}_B)$ and $I(\hat{h}_S;\hat{h}_B)$ using information theory. These are provided in the following Lemma and Theorem.

Lemma 1: Following Eq. (1), the joint PDF of $\hat{h}_A$, $\hat{h}_B$ and $\hat{h}_S$ can be approximated as $[\hat{h}_A,\hat{h}_B,\hat{h}_S] \sim \mathcal{CN}(0,2\mathbf{\Psi})$, with the covariance matrix

$$\mathbf{\Psi}=\begin{bmatrix} \mathbf{w}^H\mathbf{R}_{AB}\mathbf{w}+\sigma_\epsilon^2 & \mathbf{w}^H\mathbf{R}_{AB}\mathbf{w} & 0 \\ \mathbf{w}^H\mathbf{R}_{AB}\mathbf{w} & \mathbf{w}^H\big(\mathbf{R}_{AB}+\rho^2\mathbf{R}_{SB}\big)\mathbf{w}+\sigma_\epsilon^2 & \rho\mathbf{w}^H\mathbf{R}_{SB}\mathbf{w} \\ 0 & \rho\mathbf{w}^H\mathbf{R}_{SB}\mathbf{w} & \mathbf{w}^H\mathbf{R}_{SB}\mathbf{w}+\sigma_\epsilon^2 \end{bmatrix}, \tag{4}$$

where $\mathbf{R}_{AB} \triangleq 2\mathbf{\Sigma}_{AR}\circ\mathbf{\Sigma}_{BR}$, and $\mathbf{R}_{SB} \triangleq 2\mathbf{\Sigma}_{SR}\circ\mathbf{\Sigma}_{BR}$ (with $\circ$ denotes the elemental-wise multiplication).

Proof: From Eq. (1), $\hat{h}_A$, $\hat{h}_B$ and $\hat{h}_S$ can be re-written as the summation of M (the number of RIS elements) random variables (RVs), i.e., $g_{aR,m}\cdot g_{bR,m}, a \neq b\{A,B,S\}$, with weak dependence, since $g_{aR,m}\cdot g_{bR,m}$ is independent with $g_{aR,n}\cdot g_{bR,n}$ when nth RIS element is half-wavelength away from mth RIS element [20]. As such, given the central limit theorem under weak dependence (Theorem 27.5 in [21]), $\hat{h}_A$, $\hat{h}_B$ and $\hat{h}_S$ can be approximated as joint complex Gaussian distribution.

Then, it is straightforward that the expectations of $\hat{h}_A$, $\hat{h}_B$ and $\hat{h}_S$ are 0 given the zero means of $\mathbf{g}_{aR}$ and ϵ_a ($a \in \{A,B,S\}$). The variances of and the covariance among $\hat{h}_A$, $\hat{h}_B$ and $\hat{h}_S$ are computed in the following:

$$\begin{aligned} &\mathbb{E}(\hat{h}_A^*\hat{h}_A) = \mathbb{E}\left(\mathbf{w}^H(\mathbf{g}_{AR}^*\circ\mathbf{g}_{BR}^*)\cdot(\mathbf{g}_{AR}^T\circ\mathbf{g}_{BR}^T)\mathbf{w}\right)+2\sigma_\epsilon^2 \\ &=\mathbf{w}^H\big[\mathbb{E}(\mathbf{g}_{AR}^*\mathbf{g}_{AR}^T)\circ\mathbb{E}(\mathbf{g}_{BR}^*\mathbf{g}_{BR}^T)\big]\mathbf{w}+2\sigma_\epsilon^2=2\mathbf{w}^H\mathbf{R}_{AB}\mathbf{w}+2\sigma_\epsilon^2, \\ &\mathbb{E}(\hat{h}_B^*\hat{h}_B) = \mathbf{w}^H\Big\{\left[\mathbb{E}(\mathbf{g}_{AR}^*\mathbf{g}_{AR}^T)+\rho^2\mathbb{E}(\mathbf{g}_{SR}^*\mathbf{g}_{SR}^T)\right] \\ &\circ\mathbb{E}(\mathbf{g}_{BR}^*\mathbf{g}_{BR}^T)\Big\}\mathbf{w}+2\sigma_\epsilon^2 = 2\mathbf{w}^H\left(\mathbf{R}_{AB}+\rho^2\mathbf{R}_{SB}\right)\mathbf{w}+2\sigma_\epsilon^2, \\ &\mathbb{E}(\hat{h}_S^*\hat{h}_S) = \mathbf{w}^H\left[\mathbb{E}(\mathbf{g}_{SR}^*\mathbf{g}_{SR}^T)\circ\mathbb{E}(\mathbf{g}_{BR}^*\mathbf{g}_{BR}^T)\right]\mathbf{w}+2\sigma_\epsilon^2 \\ &=2\mathbf{w}^H\mathbf{R}_{SB}\mathbf{w}+2\sigma_\epsilon^2, \end{aligned} \tag{5}$$

$$\begin{aligned} &\mathbb{E}(\hat{h}_B^*\hat{h}_A) = \mathbb{E}\left(\mathbf{w}^H\left[(\mathbf{g}_{AR}^*+\rho\mathbf{g}_{SR}^*)\circ\mathbf{g}_{BR}^*\right]\left(\mathbf{g}_{AR}^T\circ\mathbf{g}_{BR}^T\right)\mathbf{w}\right) \\ &=\mathbf{w}^H\left[\mathbb{E}\left(\mathbf{g}_{AR}^*\mathbf{g}_{AR}^T\right)\circ\mathbb{E}\left(\mathbf{g}_{BR}^*\mathbf{g}_{BR}^T\right)\right]\mathbf{w}=2\mathbf{w}^H\mathbf{R}_{AB}\mathbf{w}, \\ &\mathbb{E}(\hat{h}_S^*\hat{h}_A) = \mathbb{E}\left(\mathbf{w}^H\left(\mathbf{g}_{SR}^*\circ\mathbf{g}_{BR}^*\right)\left(\mathbf{g}_{AR}^T\circ\mathbf{g}_{BR}^T\right)\mathbf{w}\right) \\ &=\mathbf{w}^H\left\{\left[\mathbb{E}\left(\mathbf{g}_{SR}^*\right)\mathbb{E}\left(\mathbf{g}_{AR}^T\right)\right]\circ\mathbb{E}\left(\mathbf{g}_{BR}^*\mathbf{g}_{BR}^T\right)\right\}\mathbf{w}=0, \\ &\mathbb{E}(\hat{h}_S^*\hat{h}_B) = \mathbb{E}\left(\mathbf{w}^H\left(\mathbf{g}_{SR}^*\circ\mathbf{g}_{BR}^*\right)\left[\left(\mathbf{g}_{AR}^T+\rho\mathbf{g}_{SR}^T\right)\circ\mathbf{g}_{BR}^T\right]\mathbf{w}\right) \\ &=\mathbf{w}^H\left[\rho\mathbb{E}\left(\mathbf{g}_{SR}^*\mathbf{g}_{SR}^T\right)\circ\mathbb{E}\left(\mathbf{g}_{BR}^*\mathbf{g}_{BR}^T\right)\right]\mathbf{w}=2\rho\mathbf{w}^H\mathbf{R}_{SB}\mathbf{w}, \end{aligned} \tag{6}$$

which completes the proof of Lemma 1. ■

From Lemma 1, the marginal and joint distributions of $\hat{h}_A$, $\hat{h}_B$ and $\hat{h}_S$ are derived, which then will be used to compute the legitimate and spoofing SKRs.

Theorem 1: Following Lemma 1, the legitimate and spoofing SKRs are computed as:

$$SKR_L = \max\left\{0.5\log_2\frac{\Psi_{1,1}\cdot det(\mathbf{\Psi}_{2:3,2:3})}{\Psi_{3,3}\cdot det(\mathbf{\Psi}_{1:2,1:2})},0\right\}, \tag{7}$$

$$SKR_S = 0.5\log_2\frac{\Psi_{2,2}\cdot\Psi_{3,3}}{det(\mathbf{\Psi}_{2:3,2:3})}, \tag{8}$$

where $\Psi_{i,i}$ is the (i,i)th element of matrix $\mathbf{\Psi}$, and $\mathbf{\Psi}_{i:n,i:n}$ is the sub-matrix determined by rows and columns from i to n. $det(\cdot)$ is the matrix determinant.

Proof: Eqs. (7)-(8) can be easily computed by the following two information theory formulas, i.e., the mutual information of two RVs X and Y is $I(X;Y)=h(X)+h(Y)-h(X,Y)$, and the differential entropy of $D\in\mathbb{N}^+$-dimensional joint Gaussian RV $[X_1,\cdots,X_D]$ is $h([X_1,\cdots,X_D]) = 0.5\log_2((2\pi e)^D det(\mathbf{\Psi}_X))$ with $\mathbf{\Psi}_X$ the covariance matrix. ■

From Theorem 1, the legitimate and spoofing SKRs are explicitly expressed via the RIS phase vector $\mathbf{w}$ (contained in the covariance matrix $\mathbf{\Psi}$). This therefore enables the analysis/optimisations on how the RIS can enhance either the legitimate SKR (when controlled by legitimate users), or the spoofing SKR (if controlled by the spoofing Eve). In the rest of this work, we will provide the upper-bound of legitimate and spoofing SKRs respectively, which can be treated as a theoretical limit for further qualitative security analysis and quantitative SKR optimisation.

B. Legitimate SKR Upper-bound

The upper-bound of legitimate SKR is provided by the following Theorem.

Theorem 2: When $\sigma_\epsilon^2 \to 0$ (i.e., with high receiving signal-to-noise ratio, SNR), the legitimate SKR has an upper-bound as:

$$SKR_L < \max\left\{0.5\log_2\frac{1}{\rho^2}\lambda_{max}\left((\mathbf{U}_{SB}^{-1})^H\mathbf{R}_{AB}\mathbf{U}_{SB}^{-1}\right),0\right\}, \tag{9}$$

where $\lambda_{max}(\cdot)$ represents the maximal eigenvalue of a matrix. $\mathbf{U}_{SB} \triangleq \mathbf{\Lambda}_{SB}^{0.5}\mathbf{\Gamma}_{SB}^H$, with the eigen-decomposition of $\mathbf{R}_{SB}$, i.e., $\mathbf{R}_{SB}=\mathbf{\Gamma}_{SB}\mathbf{\Lambda}_{SB}\mathbf{\Gamma}_{SB}^H$.

Proof: First, we show that the definition of $\mathbf{U}_{SB} = \mathbf{\Lambda}_{SB}^{0.5}\mathbf{\Gamma}_{SB}^H$ makes sense. This holds if $\mathbf{R}_{SB}$ is Hermitian and positive-definite, since Hermitian property leads to $\mathbf{\Gamma}_{SB}^H = \mathbf{\Gamma}_{SB}^{-1}$, and positive-definite leads to that all eigenvalues of $\mathbf{R}_{SB}$, i.e., the diagonal elements in $\mathbf{\Lambda}_{SB}$ are positive and therefore can be squared. We show why $\mathbf{R}_{SB}$ is Hermitian and positive-definite by the following Lemma.

Lemma 2: For any two Hermitian and positive-definite matrices, $\mathbf{\Sigma}_1,\mathbf{\Sigma}_2$ with same size, $\mathbf{R}=\mathbf{\Sigma}_1\circ\mathbf{\Sigma}_2$ is Hermitian and positive-definite.

A brief proof of Lemma 2 is provided here. $\mathbf{R}^H=\mathbf{\Sigma}_1^H\circ\mathbf{\Sigma}_2^H=\mathbf{\Sigma}_1\circ\mathbf{\Sigma}_2=\mathbf{R}$ and thereby $\mathbf{R}$ is Hermitian. The positive-definite property of the Hermitian $\mathbf{R}$ is equivalent to its least eigenvalue is positive, i.e., $\lambda_{min}(\mathbf{R})=\lambda_{min}(\mathbf{\Sigma}_1\circ\mathbf{\Sigma}_2) > \lambda_{min}(\mathbf{\Sigma}_1)\cdot\lambda_{min}(\mathbf{\Sigma}_2) > 0$ (Theorem 3 in [22]).

From Lemma 2, $\mathbf{R}_{SB}$ is Hermitian and positive-definite, which makes $\mathbf{U}_{SB}=\mathbf{\Lambda}_{SB}^{0.5}\mathbf{\Gamma}_{SB}^H$ exist.

Next, we prove Eq. (9). When $\sigma_\epsilon^2=0$, the first-term in the right-hand side of Eq. (7) can be written as:

$$
\begin{aligned}
&\log_2 \frac{\Psi_{1,1}\cdot det(\mathbf{\Psi}_{2:3,2:3})}{\Psi_{3,3}\cdot det(\mathbf{\Psi}_{1:2,1:2})} \overset{(a)}{=} \log_2 \frac{\mathbf{w}^H\mathbf{R}_{AB}\mathbf{w}}{\rho^2\cdot\mathbf{w}^H\mathbf{R}_{SB}\mathbf{w}} \\
&\overset{(b)}{=} \log_2 \frac{\mathbf{w}^H\mathbf{R}_{AB}\mathbf{w}}{\rho^2\mathbf{w}^H\mathbf{U}_{SB}^H\mathbf{U}_{SB}\mathbf{w}} \overset{(c)}{=} \log_2 \frac{\mathbf{v}^H(\mathbf{U}_{SB}^{-1})^H\mathbf{R}_{AB}\mathbf{U}_{SB}^{-1}\mathbf{v}}{\rho^2\mathbf{v}^H\mathbf{v}} \\
&\overset{(d)}{<} \log_2 \frac{1}{\rho^2}\lambda_{max}\left((\mathbf{U}_{SB}^{-1})^H\mathbf{R}_{AB}\mathbf{U}_{SB}^{-1}\right)\cdot\frac{\mathbf{v}^H\mathbf{v}}{\mathbf{v}^H\mathbf{v}}.
\end{aligned}
\tag{10}
$$

In Eq. (10), (a) is by taking $\sigma_\epsilon^2 = 0$. (b) is due to $\mathbf{R}_{SB} = \mathbf{U}_{SB}^H\mathbf{U}_{SB}$. (c) is by setting $\mathbf{v} = \mathbf{U}_{SB}\mathbf{w}$, and it is noteworthy that $\mathbf{U}_{SB}^{-1} = \mathbf{\Gamma}_{SB}\mathbf{\Lambda}_{SB}^{-0.5}$ exists since all eigenvalues of $\mathbf{R}_{SB}$, i.e., the diagonal elements in $\mathbf{\Lambda}_{SB}$ are positive and can be squared. For the inequality in (d), it is noticed that $(\mathbf{U}_{SB}^{-1})^H\mathbf{R}_{AB}\mathbf{U}_{SB}^{-1}$ is Hermitian and positive-definite, i.e., $\forall\mathbf{x}\in\mathbb{C}^M, \mathbf{x}^H(\mathbf{U}_{SB}^{-1})^H\mathbf{R}_{AB}\mathbf{U}_{SB}^{-1}\mathbf{x} = (\mathbf{U}_{SB}^{-1}\mathbf{x})^H\mathbf{R}_{AB}(\mathbf{U}_{SB}^{-1}\mathbf{x}) > 0$, given that $\mathbf{R}_{AB}$ is positive-definite (from Lemma2). So, the normalized quadratic form on this Hermitian and positive-definite matrix is less than its maximal eigenvalue. Combined Eq. (10) with Eq. (7), the proof of Theorem 2 completes. ■

From Theorem 2, we derive the upper-bound of the legitimate SKR when the receiving SNR (before channel probing) is large. Further Propositions will provide two critical analysis of this upper-bound.

Proposition 1: Following Theorem 2, this deduced legitimate SKR upper-bound does not vary with the change of RIS phase vector $\mathbf{w}$, specially, with the increase of RIS reflecting power, i.e., $\|\mathbf{w}\|_2^2$.

Proof: This is straightforward as the legitimate SKR upper-bound in Eq. (9) does not involve RIS phase $\mathbf{w}$. ■

The significance of Proposition 1 is to provide an insight: In RIS-combined system under pilot spoofing, the legitimate SKR has a hard upper-bound (limit), which cannot be surpassed by adjusting RIS phase vector or reflecting power. This can be further demonstrated via the next Proposition.

Proposition 2: Following Theorem 2, the legitimate SKR upper-bound reduces to 0, when the spoofing amplifying factor

$$\rho > \sqrt{\lambda_{max}\left((\mathbf{U}_{SB}^{-1})^H\mathbf{R}_{AB}\mathbf{U}_{SB}^{-1}\right)}. \tag{11}$$

Proof: This can be easily proved by making the term in $\log_2(\cdot)$ of Eq. (9) less than 1. ■

From Proposition 2, it is seen that when the spoofing amplifying factor is larger than a threshold, legitimate users cannot have any SKR even if assisted by the RIS phase vector. Combining Propositions 1-2, we find that the RIS effect is limited when defending the spoofing PL-SKG, since there is a hard limit, which can even be 0 with properly assigned spoofing amplifying factor.

C. Spoofing SKR Upper-bound

The upper-bound of spoofing SKR is provided by the following Theorem.

Theorem 3: The spoofing SKR is bounded by:

$$SKR_S < 0.5\log_2\left(1+\rho^2\lambda_{max}\left((\mathbf{U}_{AB}^{-1})^H\mathbf{R}_{SB}\mathbf{U}_{AB}^{-1}\right)\right), \tag{12}$$

where $\mathbf{U}_{AB} \triangleq \mathbf{\Lambda}_{AB}^{0.5}\mathbf{\Gamma}_{AB}^H$, with the eigen-decomposition of $\mathbf{R}_{AB}$, i.e., $\mathbf{R}_{AB} = \mathbf{\Gamma}_{AB}\mathbf{\Lambda}_{AB}\mathbf{\Gamma}_{AB}^H$.

Proof: First, from Lemma 2, $\mathbf{R}_{AB}$ is Hermitian and positive-definite, which suggest all eigenvalues of $\mathbf{R}_{AB}$, i.e., the diagonal elements in $\mathbf{\Lambda}_{AB}$ are positive and can be squared, and thereby $\mathbf{U}_{AB} = \mathbf{\Lambda}_{AB}^{0.5}\mathbf{\Gamma}_{AB}^H$ makes sense.

Then, we extend SKR_S of Theorem 1 as:

$$
\begin{aligned}
&\log_2 \frac{\Psi_{2,2}\cdot\Psi_{3,3}}{det(\mathbf{\Psi}_{2:3,2:3})} \\
&= \log_2\left(1 - \frac{\rho^2(\mathbf{w}^H\mathbf{R}_{SB}\mathbf{w})^2}{(\mathbf{w}^H(\mathbf{R}_{AB}+\rho^2\mathbf{R}_{SB})\mathbf{w}+\sigma_\epsilon^2)\,(\mathbf{w}^H\mathbf{R}_{SB}\mathbf{w}+\sigma_\epsilon^2)}\right) \\
&\overset{(e)}{<} -\log_2\left(1-\frac{\rho^2\mathbf{w}^H\mathbf{R}_{SB}\mathbf{w}}{\mathbf{w}^H(\mathbf{R}_{AB}+\rho^2\mathbf{R}_{SB})\mathbf{w}}\right) = \log_2\left(1+\frac{\rho^2\mathbf{w}^H\mathbf{R}_{SB}\mathbf{w}}{\mathbf{w}^H\mathbf{R}_{AB}\mathbf{w}}\right) \\
&\overset{(f)}{=} \log_2\left(1+\frac{\rho^2\boldsymbol{\xi}^H(\mathbf{U}_{AB}^{-1})^H\mathbf{R}_{SB}\mathbf{U}_{AB}^{-1}\boldsymbol{\xi}}{\boldsymbol{\xi}^H\boldsymbol{\xi}}\right) \\
&\overset{(g)}{<} \log_2\left(1+\rho^2\lambda_{max}\left((\mathbf{U}_{AB}^{-1})^H\mathbf{R}_{SB}\mathbf{U}_{AB}^{-1}\right)\cdot\frac{\boldsymbol{\xi}^H\boldsymbol{\xi}}{\boldsymbol{\xi}^H\boldsymbol{\xi}}\right).
\end{aligned}
\tag{13}
$$

In Eq. (13), (e) is because the function is monotonous decreasing with the increase of σ_ϵ^2, and therefore the inequality holds when $\sigma_\epsilon^2 = 0$. (f) is by setting $\boldsymbol{\xi} = \mathbf{U}_{AB}\mathbf{w}$, and it is noteworthy that $\mathbf{U}_{AB}^{-1} = \mathbf{\Gamma}_{AB}\mathbf{\Lambda}_{AB}^{-0.5}$ exists since all eigenvalues of $\mathbf{R}_{AB}$, i.e., the diagonal elements in $\mathbf{\Lambda}_{AB}$ are positive and can be squared. For the inequality in (g), it is noticed that $(\mathbf{U}_{AB}^{-1})^H\mathbf{R}_{SB}\mathbf{U}_{AB}^{-1}$ is Hermitian and positive-definite, i.e., $\forall\mathbf{x}\in\mathbb{C}^M, \mathbf{x}^H(\mathbf{U}_{AB}^{-1})^H\mathbf{R}_{SB}\mathbf{U}_{AB}^{-1}\mathbf{x} = (\mathbf{U}_{AB}^{-1}\mathbf{x})^H\mathbf{R}_{SB}(\mathbf{U}_{AB}^{-1}\mathbf{x}) > 0$, given that $\mathbf{R}_{SB}$ is positive-definite (from Lemma2). So, the normalized quadratic form on this Hermitian and positive-definite matrix is less than its maximal eigenvalue. Combined Eq. (13) with Eq. (8), the proof of Theorem 3 is complete. ■

From Theorem 3, the upper-bound of the spoofing SKR is derived. Inspired by the deduction process in Eq. (13), we here give an unconstrained sub-optimal RIS phase, denoted as $\mathbf{w}_{\text{s-opt}}$, to maximize the spoofing SKR, i.e., by solving

$$(\mathbf{R}_{SB} - \lambda_{max}(\mathbf{R}_{SB})\cdot\mathbf{I}_M)\cdot\mathbf{w}_{\text{s-opt}} = \mathbf{0} \tag{14}$$

where $\mathbf{I}_M$ is the identity matrix of size $M\times M$. Future work will be on designing algorithms to solve the non-convex problem $\max_{\mathbf{w}} SKR_S$ using semi-definite relaxation (SDR) and successive convex approximation (SCA) methods.

IV. Numerical Simulations

In this section, we evaluate our deduced legitimate and spoofing SKRs and their upper-bound. The simulation setting is provided in the following. In a 3D space, Alice, Bob, RIS and the spoofing Eve are located at $(0,0,0)$, $(0,50,0)$, $(0,20,10)$, and $(0,50,30)$, with unit m (see Fig. 1). The number of RIS elements is assigned as $M = M_x\times M_y = 10\times 10 = 100$. The direct channels from node a to RIS,

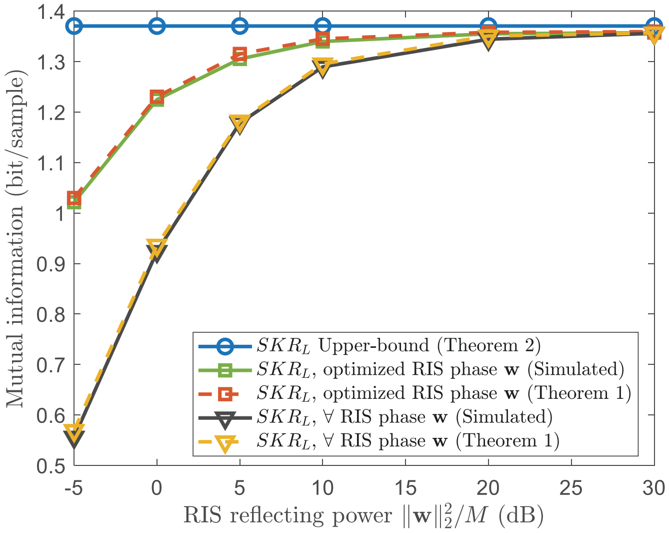

Fig. 2. RIS effect on legitimate SKR when defending spoofing Eve: Legitimate SKRs v.s. RIS reflecting power.

i.e., $\mathbf{g}_{aR}$ ($a \in \{A, B, S\}$) is formulated via the narrow-band geometric channel model, i.e., [20]

$$\mathbf{g}_{aR} = \sum_{l=1}^{L} \frac{c_{a,l}}{\sqrt{L}} \left[e^{j\boldsymbol{\zeta}(\varphi_{a,l},\phi_{a,l})\mathbf{p}_1}, \cdots, e^{j\boldsymbol{\zeta}(\varphi_{a,l},\phi_{a,l})\mathbf{p}_M} \right]^T$$
$$\boldsymbol{\zeta}(\varphi,\phi) = \frac{2\pi}{\lambda}[\cos(\phi)\cos(\varphi), \cos(\phi)\sin(\varphi), \sin(\varphi)]$$
$$\mathbf{p}_m = [0, mod(m-1, M_x)d, \lfloor (m-1)/M_y \rfloor d]^T . \tag{15}$$

In Eq. (15), $L = 10$ is the number of Rician paths, and $c_{a,l} \sim \mathcal{CN}(0, C_0 r_{aR}^{-\alpha})$ is the complex signal attenuation of lth path, with $C_0 = -30dBw$ the path-loss at reference distance (i.e., 1m), r_{aR} the distance between node a and RIS, and $\alpha = 3$ the path-loss exponent. $\boldsymbol{\zeta}(\varphi, \phi)$ is the wave vector, where λ is the wavelength, and $\varphi, \phi \sim [-\pi/2, \pi/2]$ [20] are the half-space random azimuth and elevation angles. $\mathbf{p}_m$ is the coordinate of the mth RIS element, where $mod(\cdot,\cdot)$ denotes the modulus operator and $\lfloor\cdot\rfloor$ truncates the argument, and $d = \lambda/8$ [20], [23], [24] is the space between two adjacent RIS elements.

A. RIS Effect on Legitimate SKR

We here evaluate the effect of RIS when defending the spoofing Eve. In Fig. 2, x-coordinate is the RIS reflecting power $\|\mathbf{w}\|_2^2/M$, and y-coordinate represents the legitimate SKRs (i.e., SKR_L).

It is firstly demonstrate that our deduced SKR_L upper-bound in Theorem 2 is a valid bound, which the SKR_L of both optimized and of not-optimized RIS phase $\mathbf{w}$ are below. Then, it is shown that the deduced SKR_L upper-bound is a hard limit that does not vary with the RIS reflecting power (Proposition 1). This suggests that the effect of RIS on defending PL-SKG spoofing is limited by a hard limit, which however, cannot be surpassed by purely RIS phase programming.

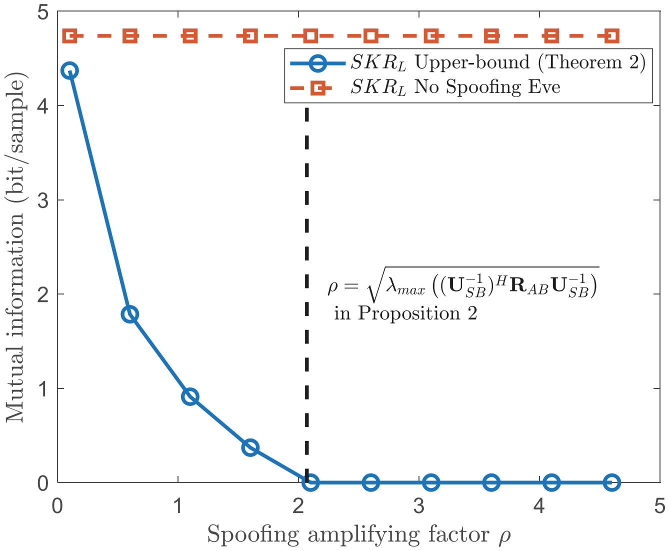

Fig. 3. RIS effect on legitimate SKR when defending spoofing Eve: Legitimate SKRs v.s. spoofing amplifying factor.

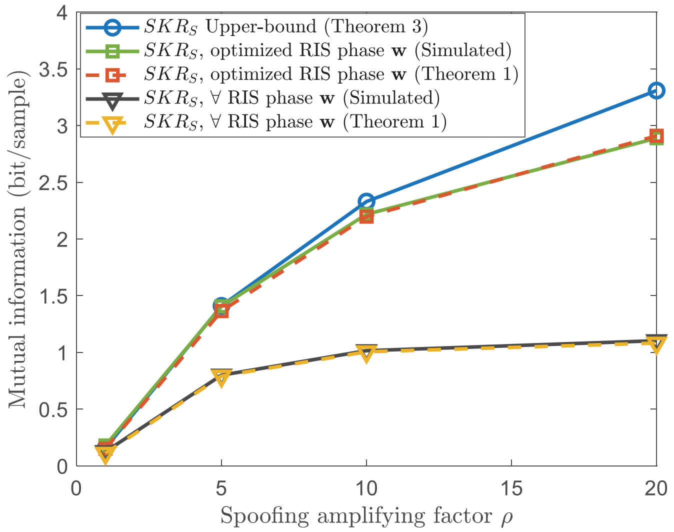

Fig. 4. RIS Effect on Spoofing SKR: Spoofing SKR versus spoofing amplifying factor.

Such RIS optimization limit can be further demonstrated via Fig. 3, where the legitimate SKRs, i.e., SKR_L, versus spoofing amplifying factor, i.e., ρ, are shown. It is observed that with the increase of ρ, the SKR_L upper-bound decreases drastically and even to 0 when ρ passes a threshold (Proposition 2). In other words, under a relatively powerful spoofing Eve, even if one can optimize the RIS phase for legitimate SKR maximization, the theoretical upper-bound of legitimate SKR is very low (nearly 0), therefore weakening the effect of RIS.

B. RIS Effect on Spoofing SKR

We next test the performance of RIS on improving spoofing SKR (when RIS is controlled by the spoofing Eve). Fig. 4

provides the curves of the spoofing SKR, i.e., SKR_S (y-coordinate) versus the spoofing amplifying factor, i.e., ρ (x-coordinate). It is seen that with the growth of ρ, all SKR_S (upper-bound, optimized, and not-optimized) increase, as a larger spoofing amplifying factor gives a larger correlation of channel probing results from of the legitimate user and spoofing Eve. Then, it is observed that our deduced SKR_S upper-bound indeed serves as a tight bound for both optimized and not-optimized SKR_S, which validates Theorem 3. Furthermore, it is noticed that the theoretical upper-bound is greatly larger than the not-optimized SKR_S, and there is still a gap between the upper-bound and the sub-optimal SKR_S, i.e., Eq. (14). This thereby indicates the potential that an adversarial RIS can be further combined with the spoofing Eve for bettering the spoofing performance.

V. Conclusion

In this work, we provided analysis on the effect of RIS to defend or assist the pilot spoofing on PL-SKG. Specially, the closed-form upper bounds of the legitimate and spoofing SKRs were deduced, from which two findings were obtained. First, we found that the legitimate SKR upper-bound is irrelevant with RIS phase, and reduces drastically with the increase of the spoofing amplifying factor. This therefore suggests the limited effect of RIS when defending PL-SKG spoofing. Second, we found that the spoofing SKR upper-bound provides a large gap from the not-optimized spoofing SKR, which indicates a potential for the adversarial RIS phase optimization. We hope this work can provide a guideline on further studies of RIS combined pilot spoofing defense/attacks.

Acknowledgment

This work was supported by the UKRI Trustworthy Autonomous System Node in Security [EPSRC grant EP/V026763/1], and by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity [EPSRC grant EP/S035362/1].

References

[1] Q. Wu and R. Zhang, "Intelligent Reflecting Surface Enhanced Wireless Network: Joint Active and Passive Beamforming Design," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.

[2] W. Wang, X. Liu, J. Tang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, "Beamforming and Jamming Optimization for IRS-Aided Secure NOMA Networks," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2021.

[3] W. Jiang, B. Chen, J. Zhao, Z. Xiong, and Z. Ding, "Joint Active and Passive Beamforming Design for the IRS-Assisted MIMOME-OFDM Secure Communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 10, pp. 10 369–10 381, 2021.

[4] X. Pang, N. Zhao, J. Tang, C. Wu, D. Niyato, and K.-K. Wong, "IRS-Assisted Secure UAV Transmission via Joint Trajectory and Beamforming Design," *IEEE Transactions on Communications*, pp. 1–1, 2021.

[5] G. Li, L. Hu, P. Staat, H. Elders-Boll, C. Zenger, C. Paar, and A. Hu, "Reconfigurable Intelligent Surface for Physical Layer Key Generation: Constructive or Destructive?" *IEEE Wireless Communications*, pp. 1–12, 2022.

[6] T. Lu, L. Chen, J. Zhang, K. Cao, and A. Hu, "Reconfigurable Intelligent Surface Assisted Secret Key Generation in Quasi-Static Environments," *IEEE Communications Letters*, vol. 26, no. 2, pp. 244–248, 2022.

[7] X. Hu, L. Jin, K. Huang, X. Sun, Y. Zhou, and J. Qu, "Intelligent Reflecting Surface-Assisted Secret Key Generation With Discrete Phase Shifts in Static Environment," *IEEE Wireless Communications Letters*, vol. 10, no. 9, pp. 1867–1870, 2021.

[8] 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.

[9] P. Staat, H. Elders-Boll, M. Heinrichs, R. Kronberger, C. Zenger, and C. Paar, "Intelligent Reflecting Surface-Assisted Wireless Key Generation for Low-Entropy Environments," in *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2021, pp. 745–751.

[10] X. Lu, J. Lei, Y. Shi, and W. Li, "Intelligent Reflecting Surface Assisted Secret Key Generation," *IEEE Signal Processing Letters*, vol. 28, pp. 1036–1040, 2021.

[11] Z. Ji, P. L. Yeoh, D. Zhang, G. Chen, Y. Zhang, Z. He, H. Yin, and Y. li, "Secret Key Generation for Intelligent Reflecting Surface Assisted Wireless Communication Networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 1030–1034, 2021.

[12] G. Li, C. Sun, W. Xu, M. D. Renzo, and A. Hu, "On Maximizing the Sum Secret Key Rate for Reconfigurable Intelligent Surface-Assisted Multiuser Systems," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 211–225, 2022.

[13] 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.

[14] Z. Wei, W. Guo, and B. Li, "A Multi-Eavesdropper Scheme Against RIS Secured LoS-Dominated Channel," *IEEE Communications Letters*, vol. 26, no. 6, pp. 1221–1225, 2022.

[15] Z. Wei, B. Li, and W. Guo, "Adversarial Reconfigurable Intelligent Surface Against Physical Layer Key Generation," *arXiv preprint arXiv:2206.10955*, 2022.

[16] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot Contamination for Active Eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 903–907, 2012.

[17] B. Akgun, M. Krunz, and O. Ozan Koyluoglu, "Vulnerabilities of Massive MIMO Systems to Pilot Contamination Attacks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1251–1263, 2019.

[18] K.-W. Huang and H.-M. Wang, "Intelligent Reflecting Surface Aided Pilot Contamination Attack and Its Countermeasure," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 345–359, 2021.

[19] J. Yang, X. Ji, F. Wang, K. Huang, and L. Guo, "A Novel Pilot Spoofing Scheme via Intelligent Reflecting Surface Based on Statistical CSI," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 12 847–12 857, 2021.

[20] 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.

[21] P. Billingsley, "Probability and Measure. 3rd Wiley," *New York*, 1995.

[22] R. Bapat and V. Sunder, "On majorization and Schur products," *Linear Algebra and its Applications*, vol. 72, pp. 107–117, 1985.

[23] O. Tsilipakos, A. C. Tasolamprou, A. Pitilakis, F. Liu, X. Wang, M. S. Mirmoosa, D. C. Tzarouchis, S. Abadal, H. Taghvaee, C. Liaskos *et al.*, "Toward Intelligent Metasurfaces: The Progress from Globally Tunable Metasurfaces to Software-Defined Metasurfaces with an Embedded Network of Controllers," *Advanced optical materials*, vol. 8, no. 17, p. 2000783, 2020.

[24] O. Özdogan, E. Björnson, and E. G. Larsson, "Intelligent Reflecting Surfaces: Physics, Propagation, and Pathloss Modeling," *IEEE Wireless Communications Letters*, vol. 9, no. 5, pp. 581–585, 2020.

2023-01-18

Secret key rate upper-bound for reconfigurable intelligent surface-combined system under spoofing

Wei, Zhuangkun

IEEE

Wei Z, Wang L, Guo W. (2023) Secret key rate upper-bound for reconfigurable intelligent surface-combined system under spoofing. In: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), 26-29 September 2022, London

https://doi.org/10.1109/VTC2022-Fall57202.2022.10012819