CSI-Based Versus RSS-Based Secret-Key Generation Under Correlated Eavesdropping

François Rottenberg, *Member, IEEE*, Trung-Hien Nguyen, *Member, IEEE*, Jean-Michel Dricot, *Member, IEEE*, François Horlin, *Member, IEEE*, and Jérôme Louveaux, *Member, IEEE*

***Abstract*— Physical-layer security (PLS) has the potential to strongly enhance the overall system security as an alternative to or in combination with conventional cryptographic primitives usually implemented at higher network layers. Secret-key generation relying on wireless channel reciprocity is an interesting solution as it can be efficiently implemented at the physical layer of emerging wireless communication networks, while providing information-theoretic security guarantees. In this article, we investigate and compare the secret-key capacity based on the sampling of the entire complex channel state information (CSI) or only its envelope, the received signal strength (RSS). Moreover, as opposed to previous works, we take into account the fact that the eavesdropper's observations might be correlated and we consider the high signal-to-noise ratio (SNR) regime where we can find simple analytical expressions for the secret-key capacity. As already found in previous works, we find that RSS-based secret-key generation is heavily penalized as compared to CSI-based systems. At high SNR, we are able to precisely and simply quantify this penalty: a halved pre-log factor and a constant penalty of about 0.69 bit, which disappears as Eve's channel gets highly correlated.**

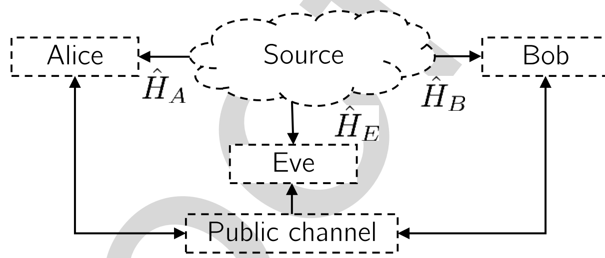
***Index Terms*— Secret-key generation, RSS, CSI, physical-layer security.**

I. Introduction

A. Problem Statement

WE CONSIDER in this article the problem of generating secret keys between two legitimate users (Alice and Bob), subject to an illegitimate user (Eve) trying to recover the key. Maurer [2] and Ahlswede and Csiszár [3] were the first to analyze the problem of generating a secret key from correlated observations. In the source model (see Fig. 1), Alice, Bob and Eve observe the realizations of a discrete memoryless source. From their sequence of observations, Alice and Bob have to distill an identical key that remains secret from Eve. Moreover, Alice and Bob have access to a public error-free authenticated channel with unlimited capacity. This helps them to perform *information reconciliation*, *i.e.*, exchanging a few parity bits so as to agree on a common sequence of symbols. However, since the channel is public, Eve can gain information about the secret key from these parity bits, on top of her own channel observations that can also be correlated with Alice and Bob observations. This is why *privacy amplification* is usually implemented after *information reconciliation*, which consists in reducing the size of the key, so that Eve information about the key is completely eliminated. Upper and lower bounds for the secret-key capacity, defined as the number of secret bits that can be generated per observation of the source, were derived in [2], [3]. In this work, we are interested in computing the secret-key capacity. Thus, we do not consider *information reconciliation* and *privacy amplification*. In practice they can be implemented through the use of, *e.g.*, low parity density check codes and universal hashing respectively. The interested reader is referred to [4] for more information on the subject.

A practical source of common randomness at Alice and Bob consists of the wireless channel reciprocity, which implies that the propagation channel from Alice to Bob and from Bob to Alice is identical if both are measured within the same channel coherence time and at the same frequency. At successive coherence times, Alice and Bob can repeatedly sample the channel by sending each other a pilot symbol so as to obtain a set of highly correlated observations and finally start a key-distillation procedure. In this article, we investigate the secret-key capacity relying on the entire complex channel state information (CSI) or only on the channel envelope, sometimes



AQ:5

Fig. 1. Source model for secret-key agreement.

AQ:1 Manuscript received June 19, 2020; revised September 24, 2020; accepted November 18, 2020. The research reported herein was partly funded by the
AQ:2 Fonds national de la recherche scientifique (F.R.S.-FNRS). This article has been presented in part at the IEEE PIMRC 2020 Conference. The associate editor coordinating the review of this article and approving it for publication was R. Thobaben. *(Corresponding author: François Rottenberg.)*

AQ:3 François Rottenberg is with the Université Catholique de Louvain, 1348 Louvain-la-Neuve, Belgium, and also with the Université Libre de Bruxelles, 1050 Brussels, Belgium (e-mail: francois.rottenberg@uclouvain.be).

AQ:4 Trung-Hien Nguyen, Jean-Michel Dricot, and François Horlin are with the Université Libre de Bruxelles, 1050 Brussels, Belgium.

Jérôme Louveaux is with the Université Catholique de Louvain, 1348 Louvain-la-Neuve, Belgium.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCOMM.2020.3040434.

Digital Object Identifier 10.1109/TCOMM.2020.3040434

also referred to as received signal strength (RSS).[1] We also consider the case where Eve's observations are correlated with the ones of Alice and Bob, which can occur in many practical situations. Related works are detailed in the next subsection while our contributions are presented in the subsequent subsection.

B. State of the Art

This study falls into the broad field of physical-layer security (PLS), which has attracted much interest in the recent decade as a competitive candidate to provide authentication, integrity and confidentiality in future communication networks [5]–[7]. We refer to [4] for an overview on the area. In the context of secret-key generation based on wireless reciprocity, there has been a large amount of related works, both from theoretical and experimental aspects [8]–[10]. In several recent approaches, more general models than the source model have been considered for secret-key generation, taking advantage of the channel to transmit part of the key [11], [12].

Many works have considered using RSS as a source of randomness for secret-key generation [13]–[19]. In [20], the authors show how to exploit the channel diversity coming from the multipath nature of the channel. The work of [21] leverages the use of multiple-antenna systems. In [22], the authors incorporate the orthogonal frequency division multiplexing (OFDM) modulation and carrier frequency offset as a way to increase bit generation in static environments with limited mobility. The choice of using RSS over full CSI is mainly due to its practical convenience. As opposed to CSI, RSS indicators are usually available at the higher layers of the communication layers, allowing for simple implementation of the key distillation procedure, relying on the legacy network infrastructure (no need to change the physical layer). Moreover, RSS is intrinsically more robust to phase offsets between Alice and Bob, relaxing constraints on the hardware, the synchronization and the reciprocity calibration. On the other hand, in the full CSI approaches, the reconciliation of phase information between legitimate users requires tightly synchronized nodes. A key selling point of PLS versus its cryptographic counterparts is its low implementation complexity, which is particularly suited in applications such as the Internet-of-Things or sensor networks where low power devices are used. In this context, the RSS approach can be more suited than the full CSI one.

The main disadvantage of RSS-based secret-key generation is that it does not use the full channel information and thus achieves a lower secret-key capacity than its CSI-based counterpart. In certain PLS applications, larger data rates and thus key sizes are targeted, using more powerful devices. For these use cases, using the full CSI approach can be more suited than the RSS one. CSI-based secret-key capacity is generally easier to characterize analytically, which has been done in a large number of works [23], [24], relying on multi-antenna systems [25]–[29], ultrawideband channels [30], and on the OFDM [31]–[34]. The authors in [20] analytically compare RSS and CSI approaches. The work of [35] also compares the two approaches relying on a thorough experimental study in various propagation environments, with different degrees of mobility.

The majority of works in the literature considers that Eve gets no side information about the key from her observations, which consist of the pilots transmitted by Alice and Bob [13], [24], [25], [27], [28]. Often, this assumption is justified by the fact that the channel environment is supposed to be rich enough in scattering implying that the fading process of the channels decorrelates quickly as a function of distance. Then, the observations of Eve have negligible correlation if she is assumed to be separated from Bob and Alice by more than one wavelength (otherwise she could be easily detected). The assumption of rapid decorrelation in space has been validated through measurements in rich scattering environments [13], [24], [35]–[37]. Moreover, this assumption simplifies the expression of the secret-key capacity, which simply becomes equal to the mutual information between Alice and Bob. However, it also occurs in practical scenarios, such as outdoor environments, that scatterers are clustered with small angular spread rather than being uniformly distributed, which leads to much longer spatial decorrelation length. The work of [1], relying on practical 3GPP channel models has shown that the assumption of full decorrelation of Eve's observations with respect to Alice and Bob is not always verified and critically depends on the propagation environment. At a cellular carrier frequency of 1 GHz, $\lambda = 30$ cm and Eve could be placed at $10\lambda = 3$ m while still having a significant correlation. The experimental work of [17] has also shown that there remains a strong correlation of the eavesdropper's channel even at distances much larger than half a wavelength. In [38], the authors studied the impact of channel sparsity, inducing correlated eavesdropping, on the secret-key capacity. In [39], the impact of the number of paths and the eavesdropper separation is analytically studied. In [40], spatial and time correlation of the channel is taken into account using a Jakes Doppler model. In [41], [42], experiments are conducted indoor to evaluate the correlation of the eavesdropper's observations and its impact on the secret-key capacity. A similar study is conducted for a MIMO indoor measurement campaign in [26]. The work of [19] also uses an indoor experimental approach and proposes results of cross-correlation, mutual information and secret-key rates, which depend on the eavesdropper's position.

C. Contributions

Our main contribution is to propose a novel analytical comparison of the secret-key capacity based on RSS and CSI for a narrowband channel. As opposed to similar previous works such as [20], we do not assume that Eve's observations are uncorrelated. This more general case adds to the complexity of the study while remaining of practical importance. Moreover, the authors in [20] could characterize the secret-key capacity for envelope sampling with a simple analytical expression. However, their simplification relied on the approximation of a sum of envelope components as Gaussian, which is not

[1]We focus the whole study in this article on the envelope of the channel, not its power. However, the final results in terms of capacity are equivalent given the one-to-one relationship between envelope and power.

applicable for our channel model. Furthermore, other works have already compared RSS and CSI-based approaches taking into account correlated eavesdropping, such as [35]. However, the studies were mostly conducted experimentally and not analytically.

More specifically, our contributions can be summarized as follows: 1) We evaluate lower and upper bounds on the secret-key capacity for both the complex (full CSI) and the envelope (RSS) cases. In the complex case, we obtain simple closed-form expressions, while, in the envelope case, the bounds must be evaluated numerically. Some of the expressions in the complex case were already obtained in previous works. We chose to present them again in this work to provide a systematic framework and useful comparison benchmarks for the envelope case. 2) We show that, in a number of particular cases, the lower and upper bounds become tight: low correlation of the eavesdropper, relatively smaller noise variance at Bob than Alice (and vice versa) and specific high signal-to-noise ratio (SNR) regimes. 3) We show that, as soon as Alice (or Bob since everything is symmetrical) samples the envelope of her channel estimate, the other parties do not lose information by taking the envelopes of their own channel estimates. 4) We show that, in the high SNR regime, the bounds can be evaluated in closed-form and result in simple expressions. The penalty of envelope-based versus complex-based secret-key generation is: i) a pre-log factor of $1/2$ instead of 1, implying a slower slope of the secret-key capacity as a function of SNR and ii) a constant penalty of 0.69 bit, which disappears as Eve's channel gets highly correlated.

The rest of this article is structured as follows. Section II describes the transmission model used in this work. Sections III and IV study the secret-key capacity based on complex and envelope sampling, respectively. Section V numerically analyzes the obtained results. Finally, Section VI concludes the paper.

Notations

Matrices are denoted by bold uppercase letters. Non bold upper case letter refers to a random variable. Superscript $*$ stands for conjugate operator. The symbol $\Re(.)$ denotes the real part. $\jmath$ is the imaginary unit. $|\mathbf{A}|$ is the determinant of matrix $\mathbf{A}$. The letters e and γ refer to the Euler number and the Euler-Mascheroni constant respectively. $h(.)$ and $I(.;.)$ refer to the differential entropy and the mutual information respectively. We use the notation $f(x) = O(g(x))$, as $x \to a$, if there exist positive numbers δ and λ such that $|f(x)| \leq \lambda g(x)$ when $0 < |x - a| < \delta$.

II. Transmission Model

Alice and Bob extract a common key from observations of their shared channel H, assumed to be reciprocal. The channel H is repeatedly sampled in time based on the transmission of *a priori* known pilots by Alice and Bob. We assume that the successive observations of H are distant enough in time so that they can be considered independent. Note that this is a conventional assumption in the literature [24], [27]. In practice, the sampling between successive samples can be related to the richness of scattering and the degree of mobility of the environment and the legitimate parties. During these successive observations, the environment remains stationary so that they can be considered as identically distributed. Considering a narrowband channel, the estimates of H at Alice's and Bob's sides, respectively denoted by $\hat{H}_A$ and $\hat{H}_B$, are given by

$$\hat{H}_A = H + W_A,\ \hat{H}_B = H + W_B,$$

where the additive noise samples W_A and W_B are modeled as independent zero mean circularly-symmetric complex Gaussian (ZMCSCG) random variables with variances σ_A^2 and σ_B^2 respectively.

The strategy of Eve consists in going as close as possible from Bob's antenna to try to maximize the correlation of its channel.[2] Then, Eve estimates her channel H_E between Alice's antenna and hers by intercepting the pilots sent from Alice to Bob. Since Eve is close to Bob, the channel from Alice to Eve will be spatially correlated with H while the channel between Bob and Eve will experience a negligible correlation with H. Therefore, we neglect the pilot sent by Bob and received by Eve in the following as she cannot get any useful information from it [39]. The channel estimate of Eve is given by

$$\hat{H}_E = H_E + W_E,$$

where W_E is modeled as ZMCSCG with variance σ_E^2. If Alice and Bob transmit a pilot of equal power and Alice, Bob and Eve use a similar receiver, one could expect a situation of equal noise variance $\sigma_A^2 = \sigma_B^2 = \sigma_E^2$. On the other hand, Eve could use a more powerful receiver than Alice and/or Bob by having, *e.g.*, a larger antenna size, a multi-antenna receiver or an amplifier with lower noise figure. This would result in a lower noise variance σ_E^2. Moreover, a different pilot power transmitted by Alice and Bob will induce variations in their noise variances σ_A^2 and σ_B^2. Indeed, in practice, the channel estimates $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$ are obtained by dividing the received signal, which includes the additive noise, by an *a priori* known pilot. For instance, if the pilot transmitted by Bob has a stronger power, the noise power at Alice σ_A^2 will be relatively weaker.

This scenario corresponds to the memoryless source model for secret-key agreement [3], [4] represented in Fig. 1: Alice, Bob and Eve observe a set of independent and identically distributed (i.i.d.) repetitions of the random variables $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$. Moreover, an error-free authenticated public channel of unlimited capacity is available for communication. All parties have access to the public channel.

In the following section, we will study the secret-key capacity of this model. To do this, we need to know the probability distributions of the random variables $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$, which directly depend on the probability distributions of W_A, W_B, W_E, H and H_E. The distributions of W_A, W_B and W_E were already detailed. Moreover, measurement campaigns have shown that the channels H and H_E can be accurately

[2]Note that all of the following derivations are symmetrical if Eve gets close to Alice instead of Bob.

modeled with a ZMCSCG distribution, especially in non-line-of-sight situations and rich scattering environments [43]. This model is commonly referred to as Rayleigh fading [44]. Therefore, we assume that (H, H_E) follows a ZMCSCG with covariance matrix given by

$$\mathbf{C}_{HH_E} = p \begin{pmatrix} 1 & \rho \\ \rho^* & 1 \end{pmatrix},$$

where p is the channel variance, such that $0 < p < \infty$. We assume that H and H_E have the same variance p, which makes sense in practice if Bob and Eve are close enough so as to belong to the same local area [43]. The coefficient $\rho = \mathbb{E}(HH_E^*)/p$ is the spatial correlation coefficient, such that $0 \leq |\rho| \leq 1$. We refer to [1], [43] for more information on the definition of this coefficient. In the following, we use the fact the differential entropy of a circularly symmetric Gaussian with covariance $\mathbf{C}$ is given by $\log_2(|\pi e \mathbf{C}|)$, where e is the Euler number.

In the sequel, at different places, we will consider the high SNR regime. When this regime is considered, we will always assume, implicitly or explicitly, that, as $\sigma_A^2 \to 0$, $\sigma_B^2 \to 0$ and $\sigma_E^2 \to 0$,

($\mathbf{As1}$): the ratio $\frac{\sigma_A^2}{\sigma_B^2}$ remains fixed and $0 < \frac{\sigma_A^2}{\sigma_B^2} < \infty$,

($\mathbf{As2}$): the ratio $\frac{\sigma_A^2}{\sigma_E^2}$ remains fixed and $0 < \frac{\sigma_A^2}{\sigma_E^2} < \infty$,

($\mathbf{As3}$): the ratio $\frac{\sigma_B^2}{\sigma_E^2}$ remains fixed and $0 < \frac{\sigma_B^2}{\sigma_E^2} < \infty$.

III. Secret-Key Capacity Based on Complex Channel Sampling

In this section, we analyze the secret-key capacity associated with complex channel sampling, that we denote by C_s^{Cplex}. Most of the results come from a direct evaluation of standard formulas for the differential entropy of Gaussian random variables. The result on the mutual information between Alice and Bob was already presented in [23]. We still present them as they provide accurate benchmarks as a comparison with the novel results that we derive for the envelope case in Section IV.

The secret-key capacity is defined as the maximal rate at which Alice and Bob can agree on a secret-key while keeping the rate at which Eve obtains information about the key arbitrarily small for a sufficiently large number of observations. Moreover, Alice and Bob should agree on a common key with high probability and the key should approach the uniform distribution. We refer to [2]–[4] for a formal definition. As explained in Section II, we consider that Eve gets useful information from her observation $\hat{H}_E$ over H. This implies that the secret-key capacity is not simply equal to $I(\hat{H}_A; \hat{H}_B)$, as was considered in many previous works [13], [23], [24], [27], [28]. Finding the general expression of the secret-key capacity for a given probability distribution of $\hat{H}_A, \hat{H}_B, \hat{H}_E$ is still an open problem. From [2], [3] [4, Prop. 5.4], the secret-key capacity, expressed in the number of generated secret bits per channel observation, can be lower and upper bounded as follows

$$C_s^{\text{Cplex}} \geq I(\hat{H}_A; \hat{H}_B) - \min\left[I(\hat{H}_A; \hat{H}_E), I(\hat{H}_B; \hat{H}_E)\right] \quad (1)$$

$$C_s^{\text{Cplex}} \leq \min\left[I(\hat{H}_A; \hat{H}_B), I(\hat{H}_A; \hat{H}_B|\hat{H}_E)\right]. \quad (2)$$

The lower bound (1) implies that, if Eve has less information about $\hat{H}_B$ than Alice or respectively about $\hat{H}_A$ than Bob, such a difference can be leveraged for secrecy [2]. Moreover, this rate can be achieved with one-way communication. On the other hand, the upper bound (2) implies that the secret-key rate cannot exceed the mutual information between Alice and Bob. Moreover, the secret-key rate cannot be higher than the mutual information between Alice and Bob if they happened to learn Eve's observation $\hat{H}_E$. In particular cases, the lower and upper bounds can become tight. In our context, three particular cases can be distinguished:

1) $\rho = 0$: Eve does not learn anything about H from $\hat{H}_E$, which becomes independent from $\hat{H}_A$ and $\hat{H}_B$. This leads to the trivial result $C_s^{\text{Cplex}} = I(\hat{H}_A; \hat{H}_B)$.
2) $\sigma_B^2 = 0$: this implies that $\hat{H}_A \to \hat{H}_B \to \hat{H}_E$ forms a Markov chain, which leads to [4, Corol. 4.1]
$$C_s^{\text{Cplex}} = I(\hat{H}_A; \hat{H}_B|\hat{H}_E) = I(\hat{H}_A; \hat{H}_B) - I(\hat{H}_A; \hat{H}_E).$$
3) $\sigma_A^2 = 0$: symmetrically as in 2), $C_s^{\text{Cplex}} = I(\hat{H}_A; \hat{H}_B|\hat{H}_E) = I(\hat{H}_A; \hat{H}_B) - I(\hat{H}_B; \hat{H}_E)$.

Cases 2) and 3) are only met when σ_B^2 or σ_A^2 are exactly zero, which never occurs in practice since all electronic devices suffer from, *e.g.*, thermal noise. However, cases 2) and 3) can be approached in particular situations in practice where $\sigma_A^2 \ll \sigma_B^2$ or $\sigma_B^2 \ll \sigma_A^2$. This could happen for instance if Alice sends a pilot with much stronger power than the one of Bob or if Alice uses an amplifier with much larger noise figure. Then, the SNR of the channel estimate of Bob will be significantly higher so that $\sigma_B^2 \ll \sigma_A^2$.

In the next subsections, we evaluate the different expressions of the mutual information required to compute the lower and upper bounds of (1) and (2): i) the mutual information between Alice and Bob $I(\hat{H}_A; \hat{H}_B)$; ii) the mutual information between Alice and Eve $I(\hat{H}_A; \hat{H}_E)$, and similarly for Bob $I(\hat{H}_B; \hat{H}_E)$; and iii) the conditional mutual information between Alice and Bob given Eve's observations $I(\hat{H}_A; \hat{H}_B|\hat{H}_E)$.

A. Mutual Information Between Alice and Bob

Using previously introduced transmission and channel models, we can find that the random variables $\hat{H}_A$ and $\hat{H}_B$ are jointly Gaussian distributed with covariance

$$\mathbf{C}_{\hat{H}_A\hat{H}_B} = \begin{pmatrix} p + \sigma_A^2 & p \\ p & p + \sigma_B^2 \end{pmatrix}.$$

From this distribution, we find back the result of [23]

$$\begin{aligned} I(\hat{H}_A; \hat{H}_B) &= h(\hat{H}_A) + h(\hat{H}_B) - h(\hat{H}_A, \hat{H}_B) \\ &= \log_2\left(\frac{(p + \sigma_A^2)(p + \sigma_B^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_B}|}\right) \\ &= \log_2\left(1 + \frac{p}{\sigma_A^2 + \sigma_B^2 + \frac{\sigma_A^2\sigma_B^2}{p}}\right). \quad (5) \end{aligned}$$

This rate corresponds to the secret-key capacity in case of uncorrelated observations at Eve ($\rho = 0$). At high SNR, as $\sigma_A^2 \to 0$ and $\sigma_B^2 \to 0$, the expressions becomes

$$I(\hat{H}_A;\hat{H}_B) = \log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) + O\left(\sigma_A^2\right), \tag{6}$$

which is characterized by a *pre-log factor* of one.

B. Mutual Information Between Alice/Bob and Eve

We can observe that $\hat{H}_A$ and $\hat{H}_E$ are jointly Gaussian distributed with covariance

$$\mathbf{C}_{\hat{H}_A\hat{H}_E} = \begin{pmatrix} p+\sigma_A^2 & \rho p \\ \rho^* p & p+\sigma_E^2 \end{pmatrix}.$$

This leads to the mutual information

$$\begin{aligned} I(\hat{H}_A;\hat{H}_E) &= \log_2\left(\frac{(p+\sigma_A^2)(p+\sigma_E^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) \\ &= \log_2\left(1+\frac{p|\rho|^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2+\frac{\sigma_A^2\sigma_E^2}{p}}\right). \end{aligned}$$

The mutual information $I(\hat{H}_B;\hat{H}_E)$ can be similarly obtained, simply replacing subscript A by B. Using the previously derived expressions of $I(\hat{H}_A;\hat{H}_B)$, $I(\hat{H}_A;\hat{H}_E)$ and $I(\hat{H}_B;\hat{H}_E)$, we find that the lower bound in (1) evaluates to (3), as shown at the bottom of the page. Note that the lower bound is not restricted to be positive (as will also be shown numerically in Section V), in which case it becomes useless since, by definition, $C_s^{\text{Cplex}} \geq 0$. Nonetheless, it does not necessarily imply that $C_s^{\text{Cplex}} = 0$. We can find the condition on the minimum noise variance at Eve σ_E^2 for having a larger-than-zero lower bound

$$\sigma_E^2 > p(|\rho|^2-1) + |\rho|^2\min(\sigma_A^2,\sigma_B^2). \tag{7}$$

In the worst-case, $|\rho| = 1$ and σ_E^2 has to be larger than the minimum of the noise variances of Alice and Bob. We can invert (7) to find the maximal correlation coefficient $|\rho|^2$ to have a larger-than-zero lower bound

$$|\rho|^2 < \frac{p+\sigma_E^2}{p+\min(\sigma_A^2,\sigma_B^2)}.$$

In the high SNR regime, as $\sigma_A^2 \to 0$, $\sigma_B^2 \to 0$ and $\sigma_E^2 \to 0$, equation (3) becomes

$$\begin{aligned} C_s^{\text{Cplex}} \geq{}& \log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) \\ &-\log_2\left(\frac{p}{p(1-|\rho|^2)+\max(\sigma_A^2,\sigma_B^2)+\sigma_E^2}\right) \\ &+O\left(\sigma_A^2\right). \end{aligned} \tag{8}$$

As soon as $|\rho| < 1$, C_s^{Cplex} is unbounded and goes to infinity as the SNR grows large. Indeed, $I(\hat{H}_A;\hat{H}_B)$ is unbounded, while $I(\hat{H}_A;\hat{H}_E)$ and $I(\hat{H}_B;\hat{H}_E)$ converge to $\log_2\left(\frac{1}{1-|\rho|^2}\right)$, which is bounded away from zero for $|\rho| < 1$.

C. Conditional Mutual Information Between Alice and Bob

We can note that $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$ are jointly Gaussian distributed with covariance matrix

$$\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E} = \begin{pmatrix} p+\sigma_A^2 & p & \rho p \\ p & p+\sigma_B^2 & \rho p \\ \rho^* p & \rho^* p & p+\sigma_E^2 \end{pmatrix},$$

which gives

$$\begin{aligned} I(\hat{H}_A;\hat{H}_B|\hat{H}_E) &= h(\hat{H}_A,\hat{H}_E) - h(\hat{H}_E) \\ &\quad + h(\hat{H}_B,\hat{H}_E) - h(\hat{H}_A,\hat{H}_B,\hat{H}_E) \\ &= \log_2\left(\frac{|\mathbf{C}_{\hat{H}_A\hat{H}_E}||\mathbf{C}_{\hat{H}_B\hat{H}_E}|}{(p+\sigma_E^2)|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}\right). \end{aligned} \tag{9}$$

The upper bound in (2) is then given by the minimum of $I(\hat{H}_A;\hat{H}_B|\hat{H}_E)$ and $I(\hat{H}_A;\hat{H}_B)$. In Appendix VII-A, we prove that the condition $I(\hat{H}_A;\hat{H}_B|\hat{H}_E) \leq I(\hat{H}_A;\hat{H}_B)$ is always verified under the jointly Gaussian channel model considered in this work. The upper bound is thus given by (4), as shown at the bottom of the page.

Based on the analytical expressions of the upper and lower bounds, we can find a novel condition for tightness of the bounds at high SNR.

Proposition 1: Under $(\mathbf{As1})-(\mathbf{As3})$*, as* $\sigma_A^2 \to 0$*,* $\sigma_B^2 \to 0$ *and* $\sigma_E^2 \to 0$*, if* $|\rho| < 1$*, the upper and lower bounds of (3) and (4) become tight and the secret-key capacity is given by*

$$C_s^{\text{Cplex}} = \log_2\left(\frac{p(1-|\rho|^2)}{\sigma_A^2+\sigma_B^2}\right) + O\left(\sigma_A^2\right). \tag{10}$$

Proof: The proof is easily obtained by taking the limits in (3) and (4) and seeing that they both converge towards (10), provided that $|\rho| < 1$. □

IV. Secret-Key Capacity Based on Channel Envelope Sampling

The goal of this section is to evaluate the impact on the secret-key capacity if Alice and Bob rely on the envelopes of their observations rather than the complex values to generate a secret key. We denote by C_s^{Evlpe} the secret-key capacity based on envelope sampling. We also introduce the notations

$$\hat{H}_A = \hat{R}_A e^{\jmath\hat{\Phi}_A},\ \hat{H}_B = \hat{R}_B e^{\jmath\hat{\Phi}_B},\ \hat{H}_E = \hat{R}_E e^{\jmath\hat{\Phi}_E},$$

where $\hat{R}_A$, $\hat{R}_B$ and $\hat{R}_E$ are the random modules of $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$ respectively. Similarly, $\hat{\Phi}_A$, $\hat{\Phi}_B$ and $\hat{\Phi}_E$ are their random phases. Note that $\hat{H}_A$ is equivalently represented by

$$C_s^{\text{Cplex}} \geq \log_2\left(1+\frac{p}{\sigma_A^2+\sigma_B^2+\frac{\sigma_A^2\sigma_B^2}{p}}\right) - \log_2\left(1+\frac{p|\rho|^2}{p(1-|\rho|^2)+\max(\sigma_A^2,\sigma_B^2)+\sigma_E^2+\frac{\max(\sigma_A^2,\sigma_B^2)\sigma_E^2}{p}}\right). \tag{3}$$

$$C_s^{\text{Cplex}} \leq \log_2\left(\frac{\left[(p+\sigma_A^2)(p+\sigma_E^2)-|\rho p|^2\right]\left[(p+\sigma_B^2)(p+\sigma_E^2)-|\rho p|^2\right]}{(p+\sigma_E^2)\left[(p(\sigma_A^2+\sigma_B^2)+\sigma_A^2\sigma_B^2)(p+\sigma_E^2)-|\rho p|^2(\sigma_A^2+\sigma_B^2)\right]}\right) \tag{4}$$

$\hat{R}_A$ and $\hat{\Phi}_A$ or $\Re(\hat{H}_A)$ and $\Im(\hat{H}_A)$. We start by stating an insightful result from [20, Th. 2], that we generalize for Eve's observations.

Proposition 2: The mutual information $I(\hat{H}_A;\hat{H}_E)$ satisfies

$$\begin{aligned} I(\hat{H}_A;\hat{H}_E) &= I(\Re(\hat{H}_A);\Re(\hat{H}_E)) + I(\Im(\hat{H}_A);\Im(\hat{H}_E)) \\ &\geq I(\hat{R}_A;\hat{R}_E) + I(\hat{\Phi}_A;\hat{\Phi}_E). \end{aligned}$$

Similarly, the mutual information $I(\hat{H}_A;\hat{H}_B)$ satisfies

$$\begin{aligned} I(\hat{H}_A;\hat{H}_B) &= I(\Re(\hat{H}_A);\Re(\hat{H}_B)) + I(\Im(\hat{H}_A);\Im(\hat{H}_B)) \\ &\geq I(\hat{R}_A;\hat{R}_B) + I(\hat{\Phi}_A;\hat{\Phi}_B). \end{aligned}$$

Proof: We conduct the proof for the more general case $I(\hat{H}_A;\hat{H}_E)$. Indeed, the mutual information $I(\hat{H}_A;\hat{H}_B)$ can be seen as a particular case for $\rho = 1$ and replacing subscripts E by B. On the one hand, we have

$$\begin{aligned} I(\hat{H}_A;\hat{H}_E) &= I(\hat{R}_A,\hat{\Phi}_A;\hat{R}_E,\hat{\Phi}_E) \\ &= h(\hat{R}_A,\hat{\Phi}_A) - h(\hat{R}_A,\hat{\Phi}_A|\hat{R}_E,\hat{\Phi}_E) \\ &\overset{(*)}{=} h(\hat{R}_A) - h(\hat{R}_A|\hat{R}_E,\hat{\Phi}_E) + h(\hat{\Phi}_A) \\ &\quad - h(\hat{\Phi}_A|\hat{R}_A,\hat{R}_E,\hat{\Phi}_E) \\ &\overset{(**)}{\geq} I(\hat{R}_A;\hat{R}_E) + I(\hat{\Phi}_A;\hat{\Phi}_E), \end{aligned}$$

where $(*)$ follows from the chain rule for entropy and the fact that $\hat{R}_A$ and $\hat{\Phi}_A$ are independent since the envelope and the phase of a ZMCSG are independent. $(**)$ follows from the fact that: i) $h(\hat{R}_A|\hat{R}_E,\hat{\Phi}_E) = h(\hat{R}_A|\hat{R}_E)$ since $(\hat{R}_A,\hat{R}_E)$ and $\hat{\Phi}_E$ are independent; ii) $h(\hat{\Phi}_A|\hat{R}_A,\hat{R}_E,\hat{\Phi}_E) \geq h(\hat{\Phi}_A|\hat{\Phi}_E)$ by the general properties of differential entropy and since $(\hat{\Phi}_A,\hat{\Phi}_E)$ is not independent from $(\hat{R}_A,\hat{R}_E)$. The proofs for the (in)dependence of random variables are given in Appendix VII-B.

On the other hand, a similar derivation can be made for $I(\Re(\hat{H}_A),\Im(\hat{H}_A);\Re(\hat{H}_E),\Im(\hat{H}_E))$, noticing that $\hat{H}_A$ and $\hat{H}_E$ are two ZMCSG, implying that their real and imaginary parts are independent, resulting in an equality with $I(\hat{H}_A;\hat{H}_E)$. □

Intuitively, this result can be explained by the fact that the random vectors $(\hat{\Phi}_A,\hat{\Phi}_E)$ and $(\hat{R}_A,\hat{R}_E)$ are not independent from one another while $(\Re(\hat{H}_A),\Re(\hat{H}_E))$ and $(\Im(\hat{H}_A),\Im(\hat{H}_E))$ are. There is thus a loss of information by treating phase and envelope separately as opposed to real and imaginary parts. This loss (or in other words the tightness of the inequality) is evaluated in [20, Fig. 2], where it is shown that the gap is significant and depends on the SNR. Interestingly, the mutual information between the phases $I(\hat{\Phi}_A;\hat{\Phi}_E)$ contains relatively more information than the mutual information between the envelopes $I(\hat{R}_A;\hat{R}_E)$.

One could wonder what is the best strategy of Bob and Eve if Alice uses $\hat{R}_A$ to generate a key. Imagine Bob and Eve have a more advanced receiver so that they can sample their observations in the complex domain, would it be beneficial for them? The answer is no, as shown in the following proposition.

Proposition 3: If Alice uses the envelope of her observations $\hat{R}_A$, then Eve does not lose information by taking the envelope of $\hat{H}_E$

$$I(\hat{R}_A;\hat{H}_E) = I(\hat{R}_A;\hat{R}_E).$$

Similarly, Bob does not lose information by taking the envelope of $\hat{H}_B$

$$I(\hat{R}_A;\hat{H}_B) = I(\hat{R}_A;\hat{R}_B).$$

The same result holds if Alice and Bob's roles are interchanged.

Proof: We conduct the proof for the more general case $I(\hat{R}_A;\hat{H}_E)$. Indeed, the mutual information $I(\hat{R}_A;\hat{H}_B)$ can be seen as a particular case for $\rho = 1$ and replacing subscripts E by B. By definition, we have

$$\begin{aligned} I(\hat{R}_A;\hat{R}_E,\hat{\Phi}_E) &= h(\hat{R}_E,\hat{\Phi}_E) - h(\hat{R}_E,\hat{\Phi}_E|\hat{R}_A) \\ &\overset{(*)}{=} h(\hat{R}_E) - h(\hat{R}_E|\hat{R}_A) + h(\hat{\Phi}_E) \\ &\quad - h(\hat{\Phi}_E|\hat{R}_A,\hat{R}_E) \\ &\overset{(**)}{=} I(\hat{R}_A;\hat{R}_E), \end{aligned}$$

where $(*)$ relies on the chain rule for entropy and the fact that $\hat{R}_E$ and $\hat{\Phi}_E$ are independent since the envelope and the phase of a ZMCSG are independent. $(**)$ relies on the fact that $h(\hat{\Phi}_E|\hat{R}_A,\hat{R}_E) = h(\hat{\Phi}_E)$ since $(\hat{R}_A,\hat{R}_E)$ and $\hat{\Phi}_E$ are independent. We refer to Appendix VII-B for the proofs on (in)dependence of random variables. □

Intuitively, the proposition can be explained by the fact that $\hat{\Phi}_B$ and $\hat{\Phi}_E$ are independent from $(\hat{R}_A,\hat{R}_B)$ and $(\hat{R}_A,\hat{R}_E)$ respectively. The propositions provide practical insight in the sense that, as soon as Alice (or Bob since everything is symmetrical) samples the envelope of her channel estimate, the other parties do not lose information by taking the envelopes of their own channel estimates. The other way around, Bob or Eve would not gain information to work on their complex channel estimate. In the light of this result, the definitions of the bounds of the secret-key capacity defined in (1) and (2) also hold here by replacing the complex values by their envelopes, *i.e.*, $\hat{R}_A$, $\hat{R}_B$ and $\hat{R}_E$ instead of $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$ respectively:

$$C_s^{\text{Evlpe}} \geq I(\hat{R}_A;\hat{R}_B) - \min\left[I(\hat{R}_A;\hat{R}_E), I(\hat{R}_B;\hat{R}_E)\right] \quad (11)$$

$$C_s^{\text{Evlpe}} \leq \min\left[I(\hat{R}_A;\hat{R}_B), I(\hat{R}_A;\hat{R}_B|\hat{R}_E)\right]. \quad (12)$$

Tight bounds can be found in the same cases and for the same reasons as in the complex case: 1) $\rho = 0$, 2) $\sigma_B^2 = 0$ and 3) $\sigma_A^2 = 0$.

Similarly as in Section III, we evaluate in the following subsections the quantities required to compute the lower and upper bounds (11) and (12): in Section IV-A, the mutual information between Alice and Bob $I(\hat{R}_A;\hat{R}_B)$; in Section IV-B, the mutual information between Alice and Eve $I(\hat{R}_A;\hat{R}_E)$, and similarly for Bob $I(\hat{R}_B;\hat{R}_E)$; and in Section IV-C, the conditional mutual information between Alice and Bob given Eve's observations $I(\hat{R}_A;\hat{R}_B|\hat{R}_E)$. Since $I(\hat{R}_A;\hat{R}_B)$ can be seen as a particularization of $I(\hat{R}_A;\hat{R}_E)$ for $\rho = 1$ and replacing subscript B by E, we will refer to Section IV-B for the proofs of the results in Section IV-A.

A. Mutual Information Between Alice and Bob

The mutual information between Alice and Bob is given by

$$I(\hat{R}_A;\hat{R}_B) = h(\hat{R}_A) + h(\hat{R}_B) - h(\hat{R}_A,\hat{R}_B). \quad (16)$$

The envelope of a ZMCSG random variable is well known to be Rayleigh distributed, *i.e.*, $\hat{R}_A \sim \text{Rayleigh}(\sqrt{\frac{p+\sigma_A^2}{2}})$ and $\hat{R}_B \sim \text{Rayleigh}(\sqrt{\frac{p+\sigma_B^2}{2}})$. The differential entropy of a Rayleigh distribution is also well known and is equal to [45]

$$h(\hat{R}_A) = \frac{1}{2}\log_2\left(\frac{p+\sigma_A^2}{4}\right) + \frac{1}{2}\log_2(e^{2+\gamma}) \tag{17}$$

$$h(\hat{R}_B) = \frac{1}{2}\log_2\left(\frac{p+\sigma_B^2}{4}\right) + \frac{1}{2}\log_2(e^{2+\gamma}), \tag{18}$$

where γ is the Euler-Mascheroni constant and e is the Euler number. On the other hand, the joint differential entropy of $(\hat{R}_A, \hat{R}_B)$ is more difficult to compute. The following lemma gives the joint probability density function (PDF) of $(\hat{R}_A, \hat{R}_B)$.

Lemma 1: The joint PDF of $(\hat{R}_A, \hat{R}_B)$ is given by (13), as shown at the bottom of the page, where $I_0(.)$ is the zero order modified Bessel function of the first kind.

Proof: The proof is obtained as a particular case of Lemma 3 for $\rho = 1$ and replacing subscripts E by B. □

Unfortunately, finding a closed-form expression for the joint differential entropy $h(\hat{R}_A, \hat{R}_B)$ is non-trivial given the presence of the Bessel function [45]. Still, $h(\hat{R}_A, \hat{R}_B)$ and thus $I(\hat{R}_A; \hat{R}_B)$, can be evaluated by numerical integration, relying on the PDF obtained in Lemma 1.

In the high SNR regime, the following lemma shows the limiting behavior of the PDF $f_{\hat{R}_A,\hat{R}_B}(\hat{r}_A, \hat{r}_B)$, which can be used to obtain a simple closed-form expression of $I(\hat{R}_A; \hat{R}_B)$, as shown in the subsequent theorem.

Lemma 2: Under $(\mathbf{As1})$, as $\sigma_A^2 \to 0$ and $\sigma_B^2 \to 0$, the PDF $f_{\hat{R}_A,\hat{R}_B}(\hat{r}_A, \hat{r}_B)$ asymptotically converges to

$$f_{\hat{R}_A,\hat{R}_B}(\hat{r}_A, \hat{r}_B) = \frac{2\hat{r}_A e^{-\frac{\hat{r}_A^2}{p}}}{p} \frac{e^{-\frac{(\hat{r}_B-\hat{r}_A)^2}{\sigma_A^2+\sigma_B^2}}}{\sqrt{\pi(\sigma_A^2+\sigma_B^2)}} + O(\sigma_A),$$

which corresponds to the product of a Rayleigh distribution of parameter $\frac{p}{2}$ and a conditional normal distribution centered in $\hat{R}_A$ and of variance $\frac{\sigma_A^2+\sigma_B^2}{2}$.

Proof: The proof is obtained as a particular case of Lemma 4 for $\rho = 1$ and replacing subscripts E by B. Since $\rho = 1$, the limit $|\rho| \to 1$ can be omitted. □

Theorem 1: Under $(\mathbf{As1})$, as $\sigma_A^2 \to 0$ and $\sigma_B^2 \to 0$, the mutual information $I(\hat{R}_A; \hat{R}_B)$ converges to

$$I(\hat{R}_A; \hat{R}_B) \to \frac{1}{2}\log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) - \chi,$$

where $\chi = \frac{1}{2}\log_2\left(\frac{4\pi}{e^{1+\gamma}}\right)$ is a constant penalty, given by 0.69 (up to the two first decimals).

Proof: The proof is obtained as a particular case of Theorem 2 for $\rho = 1$ and replacing subscripts E by B. Since $\rho = 1$, the limit $|\rho| \to 1$ can be omitted. □

The expression obtained in Theorem 1 gives a lot of insight on the high SNR secret-key capacity that can be obtained with envelope sampling, when there is no correlation ($\rho = 0$). As shown in the left column of Table I, two penalties can be observed as compared to complex sampling: i) a *pre-log factor* of $1/2$ instead of 1, implying a curve with smaller slope and ii) an additional penalty of a constant χ equivalent to about 0.69 bit. One should note that halved slope could be intuitively expected. Indeed, the full CSI approach samples two independent real-valued random variables while the RSS approach, only one.

B. Mutual Information Between Alice/Bob and Eve

We now analyze the mutual information between Alice and Eve and between Bob and Eve, which are given by

$$I(\hat{R}_A; \hat{R}_E) = h(\hat{R}_A) + h(\hat{R}_E) - h(\hat{R}_A, \hat{R}_E)$$
$$I(\hat{R}_B; \hat{R}_E) = h(\hat{R}_B) + h(\hat{R}_E) - h(\hat{R}_B, \hat{R}_E). \tag{19}$$

We already computed the values of $h(\hat{R}_A)$ and $h(\hat{R}_B)$. Similarly as for $\hat{R}_A$ and $\hat{R}_B$, we find that $\hat{R}_E \sim \text{Rayleigh}(\sqrt{\frac{p+\sigma_E^2}{2}})$ and [45]

$$h(\hat{R}_E) = \frac{1}{2}\log_2\left(\frac{p+\sigma_E^2}{4}\right) + \frac{1}{2}\log_2(e^{2+\gamma}). \tag{20}$$

The following lemma gives the joint PDFs of $(\hat{R}_A, \hat{R}_E)$ and $(\hat{R}_B, \hat{R}_E)$.

Lemma 3: The joint PDF of $(\hat{R}_A, \hat{R}_E)$ is given by (14), as shown at the bottom of the page. The joint PDF $f_{\hat{R}_B,\hat{R}_E}(\hat{r}_B, \hat{r}_E)$ is similarly obtained, replacing subscripts A by B.

Proof: The proof is given in Appendix VII-C. □

As for $h(\hat{R}_A, \hat{R}_B)$, it is difficult to find a closed-form expression of $h(\hat{R}_A, \hat{R}_E)$ and $h(\hat{R}_B, \hat{R}_E)$ due to the presence of the Bessel function. However, they can be evaluated numerically using the PDFs obtained in Lemma 3 so that $I(\hat{R}_A; \hat{R}_E)$ and $I(\hat{R}_B; \hat{R}_E)$ can be evaluated. Still, in specific regimes, closed-form solutions can be found.

$$f_{\hat{R}_A,\hat{R}_B}(\hat{r}_A, \hat{r}_B) = \frac{4\hat{r}_A\hat{r}_B}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} I_0\left(\frac{2p\hat{r}_A\hat{r}_B}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) \exp\left(-\frac{\hat{r}_A^2(p+\sigma_B^2) + \hat{r}_B^2(p+\sigma_A^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) \tag{13}$$

$$f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) = \frac{4\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} I_0\left(\frac{2p|\rho|\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) \exp\left(-\frac{\hat{r}_A^2(p+\sigma_E^2) + \hat{r}_E^2(p+\sigma_A^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) \tag{14}$$

$$\begin{aligned} f_{\hat{R}_A,\hat{R}_B,\hat{R}_E}(\hat{r}_A, \hat{r}_B, \hat{r}_E) = {} & \frac{8\hat{r}_A\hat{r}_B\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|} G\left(\frac{2p(p(1-|\rho|^2)+\sigma_E^2)\hat{r}_A\hat{r}_B}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}, \frac{2|\rho|p\sigma_B^2\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}, \frac{2|\rho|p\sigma_A^2\hat{r}_B\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}\right) \\ & \exp\left(-\frac{\hat{r}_A^2|\mathbf{C}_{\hat{H}_B\hat{H}_E}| + \hat{r}_B^2|\mathbf{C}_{\hat{H}_A\hat{H}_E}| + \hat{r}_E^2|\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}\right) \end{aligned} \tag{15}$$

TABLE I

HIGH SNR SECRET-KEY CAPACITY OF COMPLEX (CSI) VERSUS ENVELOPE (RSS) SAMPLING IN BOTH UNCORRELATED AND CORRELATED CASES, UNDER $(\mathbf{As1})$-$(\mathbf{As3})$. $\chi = 0.69\ldots$, $\sigma_*^2 = \max(\sigma_A^2, \sigma_B^2)$, $\epsilon_{\text{uncrl}} \to 0$, $\epsilon_{\text{crl}} \to 0$ ASYMPTOTICALLY

	High SNR ($\sigma_A^2, \sigma_B^2 \to 0$), uncorrelated ($\rho = 0$)	High SNR ($\sigma_A^2, \sigma_B^2, \sigma_E^2 \to 0$), correlated ($\|\rho\| > 0$)
Complex	$C_s^{\text{Cplex}} = \log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) + O(\sigma_A^2)$	$C_s^{\text{Cplex}} \geq \log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) - \log_2\left(\frac{p}{p(1-\|\rho\|^2)+\sigma_*^2+\sigma_E^2}\right) + O(\sigma_A^2)$
Envelope	$C_s^{\text{Evlpe}} = \frac{1}{2}\log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) - \chi + \epsilon_{\text{uncrl}}$	$C_s^{\text{Evlpe}} \underset{\|\rho\|\to 1}{\geq} \frac{1}{2}\left[\log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) - \log_2\left(\frac{p}{p(1-\|\rho\|^2)+\sigma_*^2+\sigma_E^2}\right)\right] + \epsilon_{\text{crl}}$

In the low correlation regime, when $|\rho| \to 0$, it is easy to see that $f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E)$ converges to the product of two independent Rayleigh PDFs $f_{\hat{R}_A}(\hat{r}_A)f_{\hat{R}_E}(\hat{r}_E)$ and thus $h(\hat{R}_A,\hat{R}_E) = h(\hat{R}_A)+h(\hat{R}_E)$. As could be expected, we find that $I(\hat{R}_A;\hat{R}_E) = I(\hat{R}_B;\hat{R}_E) = 0$ and the secret-key capacity is given by Theorem 1.

In the high SNR and correlation regime, the following lemma shows the limiting behavior of the PDFs of $(\hat{R}_A,\hat{R}_E)$ and $(\hat{R}_B,\hat{R}_E)$, which can be used to obtain a simple closed-form expression of $I(\hat{R}_A;\hat{R}_E)$ and $I(\hat{R}_B;\hat{R}_E)$.

Lemma 4: Under $(\mathbf{As2})$*, as* $|\rho| \to 1$, $\sigma_A^2 \to 0$ *and* $\sigma_E^2 \to 0$*, the PDF* $f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E)$ *asymptotically converges to*

$$f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E) = \frac{2\hat{r}_E e^{-\frac{\hat{r}_E^2}{p}}}{p}\frac{e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}}}{\sqrt{\pi(p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2)}} + O\left(\sqrt{1-|\rho|^2+\sigma_A^2}\right),$$

which corresponds to the product of a Rayleigh and a normal distribution. The same results holds for $f_{\hat{R}_B,\hat{R}_E}(\hat{r}_B,\hat{r}_E)$*, replacing subscripts* A *by* B*, under* $(\mathbf{As3})$.

Proof: The proof is given in Appendix VII-D. □

Theorem 2: Under $(\mathbf{As2})$*, as* $|\rho| \to 1$, $\sigma_A^2 \to 0$ *and* $\sigma_E^2 \to 0$*, the mutual information* $I(\hat{R}_A;\hat{R}_E)$ *converges to*

$$I(\hat{R}_A;\hat{R}_E) \to \frac{1}{2}\log_2\left(\frac{p}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}\right) - \chi,$$

where the constant penalty χ *is defined in Theorem 1. The mutual information* $I(\hat{R}_B;\hat{R}_E)$ *can be similarly approximated by replacing subscripts* A *by* B*, under* $(\mathbf{As3})$.

Proof: The proof is given in Appendix VII-E. □

Using the result of Theorem 2, we can evaluate the lower bound on the secret-key capacity (11) in the high SNR, high correlation regime, which is given in the right column of Table I. As compared with the complex case, the only difference is the *pre-log factor* of 1/2 for envelope sampling. Note that the constant penalty χ has canceled since it is also present in $I(\hat{R}_A;\hat{R}_B)$. As for the complex case, the lower bound is not restricted to be positive, in which case it is useless. The condition (7) for having a larger-than-zero lower bound, which was derived in the complex case, also applies here.

C. Conditional Mutual Information Between Alice and Bob

As shown in (9) in the complex case, to compute the conditional mutual information $I(\hat{R}_A;\hat{R}_B|\hat{R}_E)$, we need to evaluate the joint different entropy $h(\hat{R}_A,\hat{R}_B,\hat{R}_E)$. The following lemma gives the joint PDF of $(\hat{R}_A,\hat{R}_B,\hat{R}_E)$.

Lemma 5: The joint PDF of $(\hat{R}_A,\hat{R}_B,\hat{R}_E)$ *is given by (15), as shown at the bottom of the previous page, with the definition of the function* $G(\alpha_1,\alpha_2,\alpha_3)$

$$G(.) = \int_0^{2\pi}\int_0^{2\pi}\frac{e^{\alpha_1\cos(\phi_1)+\alpha_2\cos(\phi_2)+\alpha_3\cos(\phi_2-\phi_1)}}{(2\pi)^2}d\phi_1 d\phi_2.$$

Proof: The proof is given in Appendix VII-F. □

Here again, computing an analytical expression of the joint differential entropy of $(\hat{R}_A,\hat{R}_B,\hat{R}_E)$ is intricate. However, it can be evaluated numerically,[3] so that $I(\hat{R}_A;\hat{R}_B|\hat{R}_E)$ and thus (12) can be computed.

V. NUMERICAL ANALYSIS

This section aims at numerically analyzing the analytical results presented in previous sections. The following figures plot the lower bound (LB) and the upper bound (UB) on C_s^{Cplex} and C_s^{Evlpe}. For the envelope case, most of the information theoretic quantities could not be evaluated analytically. We evaluate them by numerical integration instead. We also compare some of them to the high SNR approximations that we derived and where simple analytical expressions were obtained. We will show many cases where the bounds become tight, as foreseen by the results of Sections III and IV. The mutual information quantities $I(\hat{H}_A;\hat{H}_B)$ and $I(\hat{R}_A;\hat{R}_B)$ are also plotted for comparison, as they correspond to the secret-key capacity in the case of uncorrelated observations at Eve, *i.e.*, $C_s^{\text{Cplex}} = I(\hat{H}_A;\hat{H}_B)$ and $C_s^{\text{Evlpe}} = I(\hat{R}_A;\hat{R}_B)$ for $\rho = 0$. They can also be seen as another UB, looser than $I(\hat{H}_A;\hat{H}_B|\hat{H}_E)$ and $I(\hat{R}_A;\hat{R}_B|\hat{R}_E)$.

A. Impact of SNR

In Fig. 2, the impact of the SNR on C_s^{Cplex} and C_s^{Evlpe} is studied. The SNR is defined as $\text{SNR} = p/\sigma_A^2 = p/\sigma_B^2 = p/\sigma_E^2$. A first observation is the large performance gain of complex sampling versus envelope sampling. This graph gives a quantitative criterion to better assess the trade-off full CSI versus RSS. The full CSI approach achieves higher secret-key rates at the price of stringent practical requirements. On the other hand, the RSS approach achieves lower key rates but is much more practical to implement.

Focusing first on the uncorrelated case ($I(\hat{H}_A;\hat{H}_B)$ and $I(\hat{R}_A;\hat{R}_B)$), two penalties of envelope sampling in the high SNR regime were identified in Table I: i) a *pre-log factor* of $1/2$ inducing a smaller slope as a function of SNR and ii) a

[3]For instance, by discretization and truncation of $f_{\hat{R}_A,\hat{R}_B,\hat{R}_E}(\hat{r}_A,\hat{r}_B,\hat{r}_E)$ and replacing the integral by a Riemann sum.

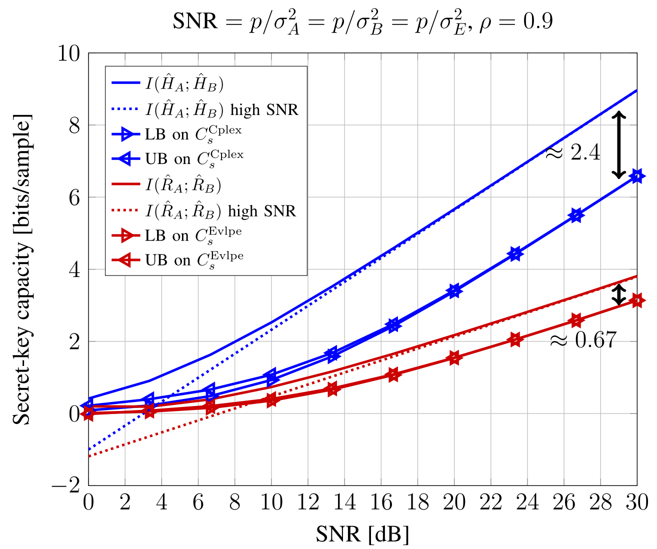


Fig. 2. Secret-key capacity for complex channel sampling versus envelope sampling as a function of SNR.

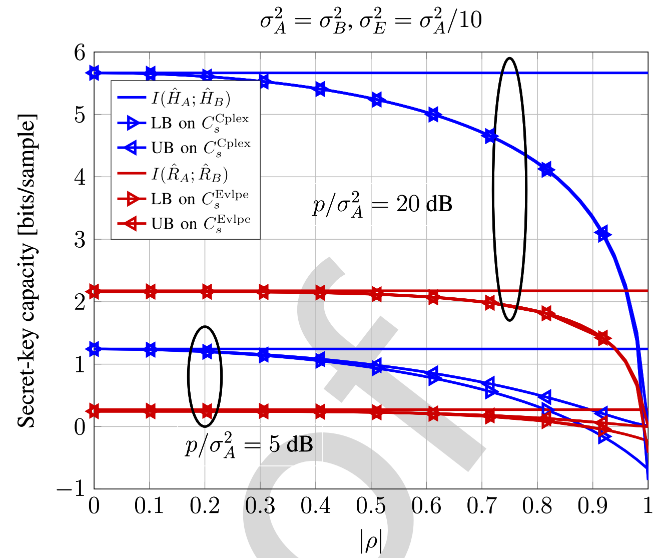


Fig. 3. Secret-key capacity for complex channel sampling versus envelope sampling as a function of correlation coefficient magnitude $|\rho|$.

constant penalty of χ bit, inducing a translation of the curve downwards of about 0.69 bit.

In the correlated case ($\rho = 0.9$), C_s^{Cplex} and C_s^{Evlpe} are reduced given the knowledge Eve has gained from her channel observations. As foreseen by Prop. 1, the bounds on C_s^{Cplex} become tight as the SNR grows large and a constant penalty of $\log_2(1 - |\rho|^2) \approx -2.4$ bits is observed as compared to the uncorrelated case. Interestingly, the bounds become tight for C_s^{Evlpe}, even for smaller values of SNR. The gap as compared to the uncorrelated case can be approximated from Table I as $\frac{1}{2}\log_2(1 - |\rho|^2) + \chi \approx -0.51$ bits. The inaccuracy with the simulated gap of -0.67 bit comes from the fact that the LB on C_s^{Evlpe} in Table I only asymptotically holds for $|\rho| \to 1$.

B. Impact of Correlation

In Fig. 3, the impact of the correlation coefficient magnitude $|\rho|$ is studied,[4] for two SNR regimes. We here consider an identical noise variance at Alice and Bob, while Eve uses a more powerful receiver so that $\sigma_A^2 = \sigma_B^2$ and $\sigma_E^2 = \sigma_A^2/10$.

One can see that, as $|\rho| \to 0$, the LB and UB become tight and converge to the mutual information between Alice's and Bob's observations. For larger values of $|\rho|$, bounds are less tight, especially in the complex case. As foreseen by Prop. 1, for a same value of $|\rho| < 1$, the LB and UB become tight for large SNR values. As already discussed in the context of equation (7), the LBs on the secret-key capacity are not restricted to be positive. This case is observed in Fig. 3 for large values of $|\rho|$. Note that this case arises here given the reduced noise power at Eve $\sigma_E^2 = \sigma_A^2/10$. In practice, the secret-key capacity cannot be lower than zero. We chose not to put negative values of the LB to zero, as it provides some physical insights on the problem.

[4]From previous analytical studies, it was shown that C_s^{Cplex} and C_s^{Evlpe} only depend on the magnitude of the correlation coefficient and not on its phase.

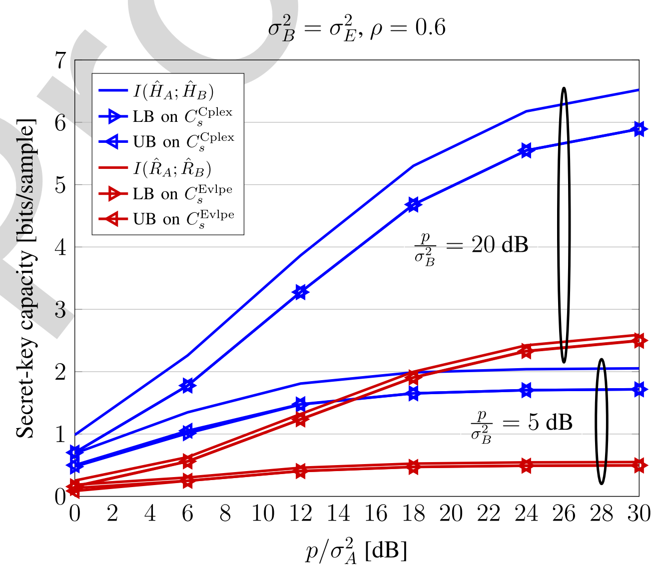


Fig. 4. Impact of a different noise variance at Alice and Bob.

C. Impact of Different Noise Variances at Alice and Bob

In Fig. 4, the impact of a different noise variance at Alice and Bob is studied. More specifically, the SNRs at Bob and Eve are kept identical, *i.e.*, $p/\sigma_B^2 = p/\sigma_E^2$, for two SNR regimes (5 dB and 20 dB). On the other hand, the SNR at Alice p/σ_A^2 is varied from 0 to 30 dB. The correlation coefficient is set to $\rho = 0.6$.

As foreseen in Sections III and IV, the LB and UB bounds become tight as $\sigma_A^2 \to 0$ for a fixed value of σ_B^2. Moreover, as p/σ_A^2 grows large, C_s^{Cplex} and C_s^{Evlpe} saturate at a plateau. This can be explained by the fact that they enter a regime limited by the fixed noise variance at Bob σ_B^2.

D. Impact of Different Noise Variance at Eve

In Fig. 5, the impact of a different noise variance at Eve is studied. More specifically, the SNRs at Alice and Bob are kept

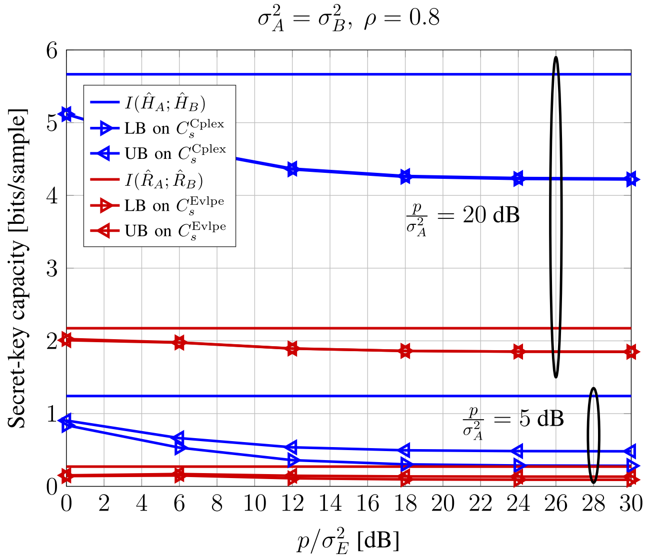


Fig. 5. Impact of a different noise variance at Eve.

identical, *i.e.*, $p/\sigma_A^2 = p/\sigma_B^2$, for two SNR regimes (5 dB and 20 dB). On the other hand, the SNR at Eve p/σ_E^2 is varied from 0 to 30 dB. The correlation coefficient is set to $\rho = 0.8$.

According to Prop. 1, the LB and UB are tight in the high SNR regime. Moreover, as p/σ_E^2 grows large, C_s^{Cplex} and C_s^{Evlpe} decrease up to a certain floor. This can be explained by the fact that Eve performance is not limited by σ_E^2 but by the fixed value of the correlation coefficient ρ.

VI. Conclusion

In this article, we have compared the secret-key capacity based on the sampling process of the entire CSI or only its envelope or RSS, taking into account correlation of Eve's observations. We have evaluated lower and upper bounds on the secret-key capacity. In the complex case, we obtain simple closed-form expressions. In the envelope case, the bounds must be evaluated numerically. In a number of particular cases, the lower and upper bounds become tight: low correlation of the eavesdropper, relatively smaller noise variance at Bob than Alice (or vice versa) and specific high SNR regimes. Finally, we have shown that, in the high SNR regime, the bounds can be evaluated in closed-form and result in simple expressions, which highlight the gain of CSI-based systems. The penalty of envelope-based versus complex-based secret-key generation is: i) a *pre-log* factor of $1/2$ instead of 1, implying a lower slope of the secret-key capacity as a function of SNR and ii) a constant penalty of about 0.69 bit, which disappears as Eve's channel gets highly correlated.

VII. Appendix

A. Upper Bound of Complex Sampling-Based Secret-Key Capacity

We need to show that $I(\hat{H}_A;\hat{H}_B|\hat{H}_E) \leq I(\hat{H}_A;\hat{H}_B)$, which is equivalent to showing that

$$0 \geq I(\hat{H}_A;\hat{H}_B|\hat{H}_E) - I(\hat{H}_A;\hat{H}_B),$$

or

$$1 \geq \frac{|\mathbf{C}_{\hat{H}_A\hat{H}_E}||\mathbf{C}_{\hat{H}_B\hat{H}_E}||\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{(p+\sigma_A^2)(p+\sigma_B^2)(p+\sigma_E^2)|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}$$

$$0 \geq \frac{|\mathbf{C}_{\hat{H}_A\hat{H}_E}||\mathbf{C}_{\hat{H}_B\hat{H}_E}||\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{(p+\sigma_A^2)(p+\sigma_B^2)(p+\sigma_E^2)} - |\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|.$$

After computing the expression of each determinant and several simplifications, we obtain

$$\begin{aligned}
&\frac{|\mathbf{C}_{\hat{H}_A\hat{H}_E}||\mathbf{C}_{\hat{H}_B\hat{H}_E}||\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{(p+\sigma_A^2)(p+\sigma_B^2)(p+\sigma_E^2)} - |\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}| \\
&\quad = -|\rho|^2 2p^3 + \frac{|\rho p|^4}{p+\sigma_E^2} + |\rho|^2 p^4 \left(\frac{1}{p+\sigma_A^2} + \frac{1}{p+\sigma_B^2}\right) \\
&\qquad - \frac{|\rho|^4\ p^6}{(p+\sigma_A^2)(p+\sigma_B^2)(p+\sigma_E^2)}.
\end{aligned}$$

We still need to prove that this quantity is smaller or equal to zero. We can first simplify the inequality by dividing by $|\rho|^2 p^3$. We then need to show that

$$\begin{aligned}
0 \geq -2 &+ \frac{1}{1+\sigma_A^2/p} + \frac{1}{1+\sigma_B^2/p} \\
&+ |\rho|^2 \frac{1}{1+\sigma_E^2/p}\left(1 - \frac{1}{(1+\sigma_A^2/p)(1+\sigma_B^2/p)}\right).
\end{aligned}$$

It is easy to see that the term on the right is maximized for $\sigma_E^2 = 0$ and $|\rho| = 1$ ($|\rho| \leq 1$ by definition). It is then sufficient to focus on that critical case and in particular to show that

$$\begin{aligned}
1 &\geq \frac{1}{1+\sigma_A^2/p} + \frac{1}{1+\sigma_B^2/p} - \frac{1}{(1+\sigma_A^2/p)(1+\sigma_B^2/p)} \\
&= \frac{1+\sigma_A^2/p+\sigma_B^2/p}{1+\sigma_A^2/p+\sigma_B^2/p+\sigma_A^2\sigma_B^2/p^2},
\end{aligned}$$

which is always smaller or equal to one given that σ_A^2, σ_B^2 and σ_E^2 and p are positive by definition.

B. Proof of (In)Dependence of Random Variables in Propositions 2 and 3

This section derives a set of results on the dependence of random variables, required in the proofs of Propositions 2 and 3. Note that, in the following sections, we conduct all the proofs considering Alice case. However, they can be straightforwardly extended to Bob's case by replacing subscript A by B in all of the following expressions.

A starting point is to write the PDF of the channel observations at Alice and Eve. We know that $\hat{H}_A$ and $\hat{H}_E$ follow a ZMCSG with covariance matrix $\mathbf{C}_{\hat{H}_A\hat{H}_E}$, which gives

$$f_{\hat{H}_A,\hat{H}_E}(\hat{h}_A,\hat{h}_E) = \frac{e^{-\frac{|\hat{h}_A|^2(p+\sigma_E^2)+|\hat{h}_E|^2(p+\sigma_A^2)-2p\Re(\rho^*\hat{h}_A\hat{h}_E^*)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}}{\pi^2|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}.$$

We can express this PDF in polar coordinates using the change of variables $\hat{H}_A = \hat{R}_A\exp(\jmath\hat{\Phi}_A)$, $\hat{H}_E = \hat{R}_E\exp(\jmath\hat{\Phi}_E)$. Doing this, we obtain the joint PDF

$$\begin{aligned}
&f_{\hat{R}_A,\hat{\Phi}_A,\hat{R}_E,\hat{\Phi}_E}(\hat{r}_A,\hat{\phi}_A,\hat{r}_E,\hat{\phi}_E) \\
&\quad = \frac{\hat{r}_A\hat{r}_E e^{-\frac{\hat{r}_A^2(p+\sigma_E^2)+\hat{r}_E^2(p+\sigma_A^2)-2p\hat{r}_A\hat{r}_E|\rho|\cos(\hat{\phi}_A-\hat{\phi}_E-\angle\rho)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}}{\pi^2|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}. \quad (21)
\end{aligned}$$

We now prove each of the results, relying on (21). Firstly, the random vector $(\hat{\Phi}_A, \hat{\Phi}_E)$ is not independent from $(\hat{R}_A, \hat{R}_E)$, if $|\rho| > 0$. Indeed, by simple inspection of (21), we can see that $f_{\hat{R}_A,\hat{\Phi}_A,\hat{R}_E,\hat{\Phi}_E}(\hat{r}_A, \hat{\phi}_A, \hat{r}_E, \hat{\phi}_E) \neq f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) f_{\hat{\Phi}_A,\hat{\Phi}_E}(\hat{\phi}_A, \hat{\phi}_E)$. The same result holds for $(\hat{\Phi}_A, \hat{\Phi}_B)$ and $(\hat{R}_A, \hat{R}_B)$, as a particularization to the case $\rho = 1$ and replacing subscripts E by B.

Secondly, $\hat{\Phi}_E$ and $(\hat{R}_A, \hat{R}_E)$ are independent. This can be shown by integrating (21) over $\hat{\phi}_A$ giving

$$
\begin{aligned}
&f_{\hat{R}_A,\hat{R}_E,\hat{\Phi}_E}(\hat{r}_A, \hat{r}_E, \hat{\phi}_E) \\
&\quad = \int_0^{2\pi} f_{\hat{R}_A,\hat{\Phi}_A,\hat{R}_E,\hat{\Phi}_E}(\ldots) d\hat{\phi}_A \\
&\quad = \frac{2\hat{r}_A\hat{r}_E}{\pi|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} I_0\left(\frac{2p|\rho|\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) e^{-\frac{\hat{r}_A^2(p+\sigma_E^2)+\hat{r}_E^2(p+\sigma_A^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}, \quad (22)
\end{aligned}
$$

where $I_0(.)$ is the zero order modified Bessel function of the first kind. Since the phase $\hat{\phi}_E$ does not appear, it implies that it is uniformly distributed and thus $f_{\hat{R}_A,\hat{R}_E,\hat{\Phi}_E}(\hat{r}_A, \hat{r}_E, \hat{\phi}_E) = f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) f_{\hat{\Phi}_E}(\hat{\phi}_E)$. The same result holds for $\hat{\Phi}_B$ and $(\hat{R}_A, \hat{R}_B)$, as a particularization to the case $\rho = 1$ and replacing subscripts E by B.

Thirdly, the envelope and the phase of a ZMCSG are independent. Take for instance the PDF of $\hat{H}_E$, which can be written in polar coordinates, using a change of variable $\hat{H}_E = \hat{R}_E \exp(\jmath\hat{\Phi}_E)$, as

$$
f_{\hat{R}_E,\hat{\Phi}_E}(\hat{r}_E, \hat{\phi}_E) = \frac{\hat{r}_E}{\pi(p+\sigma_E^2)} e^{-\frac{\hat{r}_E^2}{p+\sigma_E^2}},
$$

which shows that $f_{\hat{R}_E,\hat{\Phi}_E}(\hat{r}_E, \hat{\phi}_E) = f_{\hat{R}_E}(\hat{r}_E) f_{\hat{\Phi}_E}(\hat{\phi}_E)$, with $\hat{\Phi}_E$ uniformly distributed, implying independence. The same result holds for $\hat{H}_A$ and $\hat{H}_B$.

C. Proof of Lemma 3

The joint PDF $f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E)$ can be obtained by integrating (22) over $\hat{\phi}_E$, which gives

$$
\begin{aligned}
&f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) \\
&\quad = \int_0^{2\pi} f_{\hat{R}_A,\hat{R}_E,\hat{\Phi}_E}(\hat{r}_A, \hat{r}_E, \hat{\phi}_E) d\hat{\phi}_E \\
&\quad = \frac{4\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} I_0\left(\frac{2p|\rho|\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) e^{-\frac{\hat{r}_A^2(p+\sigma_E^2)+\hat{r}_E^2(p+\sigma_A^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}, \quad (23)
\end{aligned}
$$

and leads to the result of Lemma 3.

D. Proof of Lemma 4

From Bessel function theory [46, Eq. 10.40.1], we know that, as $r \to +\infty$,

$$
I_0(r) = \frac{e^r}{\sqrt{2\pi r}} + \epsilon_0, \ |\epsilon_0| = O\left(\frac{e^r}{r^{3/2}}\right). \quad (24)
$$

In our case, we have

$$
r = \frac{2p|\rho|\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} = \frac{2p|\rho|\hat{r}_A\hat{r}_E}{(1-|\rho|^2)p^2 + p(\sigma_E^2+\sigma_A^2) + \sigma_E^2\sigma_A^2}. \quad (25)
$$

The Bessel asymptotic expansion is thus accurate when r becomes large. This is precisely the case as $\sigma_A^2 \to 0$, $\sigma_E^2 \to 0$ and $|\rho| \to 1$, for $\hat{r}_A > 0$ and $\hat{r}_E > 0$. Using the Bessel asymptotic expansion of $I_0(.)$ in (23), we get

$$
\begin{aligned}
f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) = &\frac{2}{p}\sqrt{\frac{\hat{r}_A\hat{r}_E}{|\rho|}} e^{-\frac{\hat{r}_A^2\sigma_E^2+\hat{r}_E^2(\sigma_A^2+p(1-|\rho|^2))}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}} \\
&\frac{1}{\sqrt{\pi|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}} e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}} + \epsilon_1, \quad (26)
\end{aligned}
$$

where ϵ_1 is the approximation error

$$
\epsilon_1 = \frac{4\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\exp\left(-\frac{\hat{r}_A^2(p+\sigma_E^2)+\hat{r}_E^2(p+\sigma_A^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right)\epsilon_0.
$$

Note that, in the particular cases $\hat{r}_A = 0$ or $\hat{r}_E = 0$, $\epsilon_1 = 0$ since (26) = (23) = 0. Using (24) and the definition of r in (25), we can bound the error ϵ_1 as follows

$$
\begin{aligned}
|\epsilon_1| &= O\left(\frac{\left(|\mathbf{C}_{\hat{H}_A\hat{H}_E}|\right)^{1/2} e^{-\frac{\hat{r}_A^2\left(p+\sigma_E^2\right)+\hat{r}_E^2\left(p+\sigma_A^2\right)-2p|\rho|\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}}{\left(p|\rho|\right)^{3/2}\left(\hat{r}_A\hat{r}_E\right)^{1/2}}\right) \\
&= O\left(\sqrt{1-|\rho|^2+\sigma_A^2+\sigma_E^2}\right),
\end{aligned}
$$

where we used the fact that the exponential can be bounded in the asymptotic regime by an independent constant. The second exponential term of (26) suggests the following approximation $\hat{r}_A \approx |\rho|\hat{r}_E$. We thus obtain

$$
\begin{aligned}
f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) = &\frac{2\hat{r}_E e^{-\hat{r}_E^2\frac{p(1-|\rho|^2)+|\rho|^2\sigma_E^2+\sigma_A^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}} e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}}}{p\sqrt{\pi|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}} \\
&+\epsilon_1 + \epsilon_2, \quad (27)
\end{aligned}
$$

where ϵ_2 is the approximation error related to this second approximation

$$
\begin{aligned}
\epsilon_2 = \frac{2}{p}\frac{e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}}}{\sqrt{\pi|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}}\Bigg(&\sqrt{\frac{\hat{r}_A\hat{r}_E}{|\rho|}} e^{-\frac{\hat{r}_A^2\sigma_E^2+\hat{r}_E^2(\sigma_A^2+p(1-|\rho|^2))}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}} \\
&-\hat{r}_E e^{-\hat{r}_E^2\frac{p(1-|\rho|^2)+|\rho|^2\sigma_E^2+\sigma_A^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}\Bigg).
\end{aligned}
$$

When $\hat{r}_A = |\rho|\hat{r}_E$, the term in parenthesis is exactly zero and so $\epsilon_2 = 0$. In other cases, it can be bounded by an independent constant as $\sigma_A^2 \to 0$, $\sigma_E^2 \to 0$ and $|\rho| \to 1$, giving

$$
|\epsilon_2| = O\left(\frac{e^{-\frac{\beta}{(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}}}{\sqrt{1-|\rho|^2+\sigma_A^2+\sigma_E^2}}\right),
$$

where β is some real strictly positive constant. Moreover, we can still simplify (27) by performing the two following approximations $|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p \approx p(1-|\rho|^2) + \sigma_A^2 + \sigma_E^2$ and

$\frac{p(1-|\rho|^2)+|\rho|^2\sigma_E^2+\sigma_A^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} \approx 1/p$ so that we get

$$
\begin{aligned}
f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E) = &\frac{2\hat{r}_E e^{-\frac{\hat{r}_E^2}{p}}}{p} \frac{e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}}}{\sqrt{\pi(p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2)}} \\
&+\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4,
\end{aligned}
$$

which gives the asymptotic distribution of Lemma 4 and where ϵ_3 and ϵ_4 are the approximation errors related to the approximations

$$
\begin{aligned}
\epsilon_3 = &\frac{2\hat{r}_E}{p\sqrt{\pi|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}} \left(e^{-\hat{r}_E^2 \frac{p(1-|\rho|^2)+|\rho|^2\sigma_E^2+\sigma_A^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} - \frac{p(\hat{r}_A-|\rho|\hat{r}_E)^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}} \right. \\
&\left. - e^{-\frac{\hat{r}_E^2}{p}} e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}} \right) \\
\epsilon_4 = &\frac{2\hat{r}_E e^{-\frac{\hat{r}_E^2}{p}} e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}}}{p\sqrt{\pi}} \left(\frac{1}{\sqrt{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}} \right. \\
&\left. - \frac{1}{\sqrt{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}} \right).
\end{aligned}
$$

To bound ϵ_3 and ϵ_4, we can use a first order Taylor expansion of the exponential and the inverse of a square root respectively. We find

$$
\begin{aligned}
|\epsilon_3| &= O\left(\frac{(1-|\rho|^2)\sigma_E^2+\sigma_A^2\sigma_E^2}{(1-|\rho|^2+\sigma_A^2+\sigma_E^2)^{3/2}} \right) \\
|\epsilon_4| &= O\left(\frac{\sigma_A^2+\sigma_E^2}{\sqrt{1-|\rho|^2+\sigma_A^2+\sigma_E^2}} \right).
\end{aligned}
$$

Finally, combining the bounds on the approximation errors $\epsilon_1, \epsilon_2, \epsilon_3$ and ϵ_4, we find that the total approximation error can be bounded as

$$
|\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4| = O\left(\sqrt{1-|\rho|^2+\sigma_A^2} \right),
$$

where we used (**As2**). This completes the proof.

E. Proof of Theorem 2

Let us define the asymptotic PDF of $f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E)$ as

$$
f^{\text{High}}_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E) = \frac{2\hat{r}_E e^{-\frac{\hat{r}_E^2}{p}}}{p} \frac{e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}}}{\sqrt{\pi(p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2)}}.
$$

We can see that the PDF factorizes as $f^{\text{High}}_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E) = f_1(\hat{r}_E)f_2(\hat{r}_A|\hat{r}_E)$. We can identify $f_1(\hat{r}_E)$ to be a Rayleigh distribution with parameter $\frac{p}{2}$, while the conditional PDF $f_2(\hat{r}_A|\hat{r}_E)$ is a normal centered in $|\rho|\hat{r}_E$ and of variance $(p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2)/2$.

Results such as [47, Th. 1] can be used to prove that, for a sequence of PDFs such that $f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E) \to f^{\text{High}}_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E)$ pointwise, their differential entropy also converges provided that: i) their second order moments are bounded from above and ii) their PDF is bounded from above. These two conditions are satisfied in our case as long as p, σ_A^2 and σ_E^2 are bounded from above, which makes practical sense. In the pathological case $\sigma_A^2 = 0$, $\sigma_E^2 = 0$ or $|\rho| = 1$, $|\mathbf{C}_{\hat{H}_A\hat{H}_E}| = 0$ and the PDFs are unbounded, which makes practical sense since $h(\hat{R}_A,\hat{R}_E) \to -\infty$. Unfortunately, finding the analytical rate of convergence of the differential entropy is intricate.

All of the following expressions should be understood in the asymptotic sense as $\sigma_A^2 \to 0$ and $\sigma_E^2 \to 0$ and $|\rho| \to 1$. Using the chain rule for the differential entropy $h(X,Y) = h(X) + h(Y|X)$, the general expression of the differential entropies of Rayleigh and normal distributions, the joint differential entropy of the distribution $f^{\text{High}}_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E)$ can be easily computed and we find

$$
\begin{aligned}
h(\hat{R}_A,\hat{R}_E) \to &\frac{1}{2}\log_2\left(p^2(1-|\rho|^2)+p(\sigma_A^2+\sigma_E^2)\right) \\
&+\frac{1}{2}\log_2\left(\frac{\pi e^{3+\gamma}}{4}\right).
\end{aligned}
$$

Inserting this expression in (19), together with the expressions of $h(\hat{R}_A)$ and $h(\hat{R}_E)$ given in (17) and (20) respectively, we finally obtain

$$
\begin{aligned}
I(\hat{R}_A;\hat{R}_E) &\to \frac{1}{2}\log_2\left(\frac{(p+\sigma_A^2)(p+\sigma_E^2)}{p^2(1-|\rho|^2)+p(\sigma_A^2+\sigma_E^2)} \right) + \chi \\
&\to \frac{1}{2}\log_2\left(\frac{p}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2} \right) + \chi,
\end{aligned}
$$

with the definition of χ introduced in Theorem 1, which concludes the proof.

F. Proof of Lemma 5

We know that $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$ follow a ZMCSG with covariance matrix $\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}$, which gives

$$
\begin{aligned}
&f_{\hat{H}_A,\hat{H}_B,\hat{H}_E}(\hat{h}_A,\hat{h}_B,\hat{h}_E) \\
&\quad = \frac{e^{\frac{2p(p(1-|\rho|^2)+\sigma_E^2)\hat{h}_A\hat{h}_B^* + 2\ p\sigma_B^2\Re(\hat{h}_A\rho^*\hat{h}_E^*) + 2\ p\sigma_A^2\Re(\hat{h}_B\rho^*\hat{h}_E^*)}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}}}{\pi^3|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|} \\
&\qquad e^{-\frac{|\hat{h}_A|^2|\mathbf{C}_{\hat{H}_B\hat{H}_E}| + |\hat{h}_B|^2|\mathbf{C}_{\hat{H}_A\hat{H}_E}| + |\hat{h}_E|^2|\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}}.
\end{aligned}
$$

This PDF can be expressed in polar coordinates as

$$
\begin{aligned}
&f_{\hat{R}_A,\hat{R}_B,\hat{R}_E,\hat{\Phi}_A,\hat{\Phi}_B,\hat{\Phi}_E}(\hat{r}_A,\hat{r}_B,\hat{r}_E,\hat{\phi}_A,\hat{\phi}_B,\hat{\phi}_E) \\
&\quad = \frac{\hat{r}_A\hat{r}_B\hat{r}_E}{\pi^3|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|} e^{-\frac{\hat{r}_A^2|\mathbf{C}_{\hat{H}_B\hat{H}_E}| + \hat{r}_B^2|\mathbf{C}_{\hat{H}_A\hat{H}_E}| + \hat{r}_E^2|\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}} \\
&\qquad e^{\frac{2p(p(1-|\rho|^2)+\sigma_E^2)\hat{r}_A\hat{r}_B\cos(\hat{\phi}_A-\hat{\phi}_B)}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}} e^{\frac{2p\sigma_B^2\hat{r}_A\hat{r}_E|\rho|\cos(\hat{\phi}_A-\hat{\phi}_E-\angle\rho)}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}} \\
&\qquad e^{\frac{2p\sigma_A^2\hat{r}_B\hat{r}_E|\rho|\cos(\hat{\phi}_B-\hat{\phi}_E-\angle\rho)}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}}. \qquad (28)
\end{aligned}
$$

The joint PDF $f_{\hat{R}_A,\hat{R}_B,\hat{R}_E}(\hat{r}_A,\hat{r}_B,\hat{r}_E)$ can be obtained by integrating (28) over the phases $\hat{\phi}_A$, $\hat{\phi}_B$ and $\hat{\phi}_E$, which leads to the result of Lemma 5. Indeed the first two terms do not depend on the phases, so that they can be put out of the integrals. The third term however does. One can easily see that the phase of ρ does not impact the result, so that it can be removed. One can further notice that the cosines do not depend on the absolute phases $\hat{\phi}_A, \hat{\phi}_B, \hat{\phi}_E$ but on their differences.

Making a change of variable $\phi_1 = \hat{\phi}_A - \hat{\phi}_B$, $\phi_2 = \hat{\phi}_A - \hat{\phi}_E$, we see that the last difference is $\hat{\phi}_B - \hat{\phi}_E = \phi_2 - \phi_1$. Hence, one integral simplifies.

References

[1] F. Rottenberg, P. De Doncker, F. Horlin, and J. Louveaux, "Impact of realistic propagation conditions on reciprocity-based secret-key capacity," in *Proc. IEEE 31st Annu. Int. Symp. Pers., Indoor Mobile Radio Commun.*, Aug. 2020, pp. 1–6.

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[5] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[7] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[8] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[9] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proc. IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct. 2015.

[10] 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.

[11] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key generation using correlated sources and channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 652–670, Feb. 2012.

[12] G. Bassi, P. Piantanida, and S. Shamai (Shitz), "The secret key capacity of a class of noisy channels with correlated sources," *Entropy*, vol. 21, no. 8, p. 732, Jul. 2019.

[13] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 401–410, doi: 10.1145/1315245.1315295.

[14] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw.*, 2009, p. 321, doi: 10.1145/1614320.1614356.

[15] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[16] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[17] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proc. 4th Eur. Workshop Syst. Secur.*, 2011, doi: 10.1145/1972551.1972559.

[18] R. Guillaume, F. Winzer, A. Czylwik, C. T. Zenger, and C. Paar, "Bringing PHY-based key generation into the field: An evaluation for practical scenarios," in *Proc. IEEE 82nd Veh. Technol. Conf.*, Sep. 2015, pp. 1–5.

[19] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, "The passive eavesdropper affects my channel: Secret-key rates under real-world conditions," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–6.

[20] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.

[21] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[22] M. Jacovic, M. Kraus, G. Mainland, and K. R. Dandekar, "Evaluation of physical layer secret key generation for IoT devices," in *Proc. IEEE 20th Wireless Microw. Technol. Conf. (WAMICON)*, Apr. 2019, pp. 1–6.

[23] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 2593–2597.

[24] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[25] T. F. Wong, M. Bloch, and J. M. Shea, "Secret sharing over fast-fading MIMO wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, Dec. 2009, Art. no. 506973.

[26] J. W. Wal and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[27] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.

[28] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret key generation from reciprocal spatially correlated MIMO channels," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2013, pp. 1245–1250.

[29] B. T. Quist and M. A. Jensen, "Optimal channel estimation in beamformed systems for common-randomness-based secret key establishment," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1211–1220, Jul. 2013.

[30] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[31] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 3048–3056.

[32] X. Wu, Y. Peng, C. Hu, H. Zhao, and L. Shu, "A secret key generation method based on CSI in OFDM-FDD system," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2013, pp. 1297–1302.

[33] J. Zhang, M. Ding, D. Lopez-Perez, A. Marshall, and L. Hanzo, "Design of an efficient OFDMA-based multi-user key generation protocol," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8842–8852, Sep. 2019.

[34] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "An efficient OFDM-based encryption scheme using a dynamic key approach," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 361–378, Feb. 2019.

[35] J. Zhang *et al.*, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[36] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, Sep. 2008, pp. 128–139, doi: 10.1145/1409944.1409960.

[37] M. Ghoreishi Madiseh, S. He, M. L. Mcguire, S. W. Neville, and X. Dong, "Verification of secret key generation from UWB channel observations," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–5.

[38] T.-H. Chou, S. C. Draper, and A. M. Sayeed, "Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2518–2522.

[39] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. 3rd Eur. Conf. Antennas Propag.*, Mar. 2009, pp. 1499–1503.

[40] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, Apr. 2017.

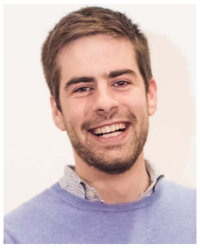
[41] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "Experimental aspects of secret key generation in indoor wireless environments," in *Proc. IEEE 14th Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2013, pp. 669–673.

[42] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "The effect of Eavesdropper's statistics in experimental wireless secret-key generation," 2013, *arXiv:1312.3304*. [Online]. Available: http://arxiv.org/abs/1312.3304

[43] G. D. Durgin, *Space-Time Wireless Channels*. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[44] B. Sklar, "Rayleigh fading channels in mobile digital communication systems.I. Characterization," *IEEE Commun. Mag.*, vol. 35, pp. 90–100, Jul. 1997.

[45] J. V. Michalowicz, J. M. Nichols, and F. Bucholtz, *Handbook of Differential Entropy*. Boca Raton, FL, USA: CRC Press, 2013.
[46] *NIST Digital Library of Mathematical Functions*. W. J. Olver *et al.*, Eds. 2020. http://dlmf.nist.gov/
[47] M. Godavarti and A. Hero, "Convergence of differential entropies," *IEEE Trans. Inf. Theory*, vol. 50, no. 1, pp. 171–176, Jan. 2004.



François Rottenberg (Member, IEEE) received the M.Sc. degree in electrical engineering from the Université Catholique de Louvain (UCLouvain), Louvain-la-Neuve, in 2014, and the Ph.D. degree jointly from UCLouvain and the Université Libre de Bruxelles (ULB), Brussels, in 2018. From September 2018 to August 2019, he was a Post-Doctoral Researcher with the University of Southern California (USC), Los Angeles, USA, leading the 5G massive MIMO research efforts. He is currently a Post-Doctoral Researcher affiliated with UCLouvain and ULB, funded by the Belgian National Science Foundation (FRS-FNRS). He participated to various national, European, and international projects. Since 2015, he has been a Regular Visitor and a Collaborator with the Centre Tecnològic Telecomunicacions Catalunya (CTTC), Castelldefels, Spain, and the National Institute of Information and Communications Technology (NICT), Tokyo, Japan. His main research interests include signal processing for next generations of communication systems, including novel modulation formats, multi-antenna systems, and physical-layer security.

Trung-Hien Nguyen (Member, IEEE) received the B.Sc. degree in electronics and telecommunications from the Hanoi Posts and Telecommunications Institute of Technology (PTIT), Vietnam, in 2010, and the Ph.D. degree in physics from the University of Rennes 1, France, in 2015. Since December 2015, he has been a Post-Doctoral Researcher with the OPERA Department, Université Libre de Bruxelles (ULB), Belgium. His research interests include optical fiber communication systems and localization based on 5G signals.

Jean-Michel Dricot (Member, IEEE) received the Ph.D. degree in network engineering with a focus on wireless sensor networks protocols and architectures. He leads research on network security with a specific focus on the Internet of Things (IoT) and wireless networks. He teaches communication networks, mobile networks, the Internet of Things, and network security. After his Ph.D. degree, he joined France Telecom Research and Development (Orange Labs), Grenoble, France, as a Research Engineer. He started there a project aiming at securing lightweight communication protocols, with a specific focus on wireless smart meters and body area networks. Next, he moved back to the Machine Learning Group, ULB, where he worked on the IoT-based localization techniques. In 2010, he was appointed as a Professor with the Université Libre de Bruxelles, with a tenure in mobile and wireless networks. He is the author or a coauthor of more than 100 papers published in peer-reviewed international journals and conferences. He served as a reviewer for European projects.

François Horlin (Member, IEEE) received the Ph.D. degree from the Université Catholique de Louvain (UCL) in 2002. He specialized in the field of signal processing for digital communications. After his Ph.D. degree, he joined the Inter-University Micro-Electronics Center (IMEC). He led the project aiming at developing a 4G cellular communication system in collaboration with Samsung Korea. In 2007, he became a Professor with the Université Libre de Bruxelles (ULB). He is currently supervising a Research Team working on next-generation communication systems. His current research interests include localization based on 5G signals, filterbank-based modulations, massive MIMO, and passive radars. He has been an Academic Representative to the executive board of ULB from 2010 to 2015. Since 2017, he has been the Vice Dean for research at the Ecole Polytechnique de Bruxelles (EPB).

Jérôme Louveaux (Member, IEEE) received the Electrical Engineering degree and the Ph.D. degree from the Université Catholique de Louvain (UCL), Louvain-la-Neuve, Belgium, in 1996 and 2000, respectively. From 2000 to 2001, he was a Visiting Scholar with the Electrical Engineering Department, Stanford University, CA, USA. From 2004 to 2005, he was a Post-Doctoral Researcher with the Delft University of Technology, The Netherlands. Since 2006, he has been a Professor with the ICTEAM Institute, UCL. His research interests include signal processing for digital communications, and in particular: multicarrier modulations, xDSL systems, resource allocation, synchronization, and estimation. He was a co-recipient of the Prix biennal Siemens 2000 for a contribution on filter-bank based multi-carrier transmission and the Prix Scientifique Alcatel 2005 for a contribution in the field of powerline communications.

AUTHOR QUERIES

AUTHOR PLEASE ANSWER ALL QUERIES

PLEASE NOTE: We cannot accept new source files as corrections for your article. If possible, please annotate the PDF proof we have sent you with your corrections and upload it via the Author Gateway. Alternatively, you may send us your corrections in list format. You may also upload revised graphics via the Author Gateway.

Carefully check the page proofs (and coordinate with all authors); additional changes or updates WILL NOT be accepted after the article is published online/print in its final form. Please check author names and affiliations, funding, as well as the overall article for any errors prior to sending in your author proof corrections. Your article has been peer reviewed, accepted as final, and sent in to IEEE. No text changes have been made to the main part of the article as dictated by the editorial level of service for your publication.

AQ:1 = Please confirm or add details for any funding or financial support for the research of this article.

AQ:2 = Please confirm whether the edits made in the presentation line are correct.

AQ:3 = Please provide the department name for Université Catholique de Louvain and Université Libre de Bruxelles.

AQ:4 = Please confirm the city name for Université Libre de Bruxelles.

AQ:5 = Note that if you require corrections/changes to tables or figures, you must supply the revised files, as these items are not edited for you.

AQ:6 = Please provide the author name, publisher name, and publisher location for Ref. [46].

CSI-Based Versus RSS-Based Secret-Key Generation Under Correlated Eavesdropping

François Rottenberg, *Member, IEEE*, Trung-Hien Nguyen, *Member, IEEE*, Jean-Michel Dricot, *Member, IEEE*, François Horlin, *Member, IEEE*, and Jérôme Louveaux, *Member, IEEE*

***Abstract*— Physical-layer security (PLS) has the potential to strongly enhance the overall system security as an alternative to or in combination with conventional cryptographic primitives usually implemented at higher network layers. Secret-key generation relying on wireless channel reciprocity is an interesting solution as it can be efficiently implemented at the physical layer of emerging wireless communication networks, while providing information-theoretic security guarantees. In this article, we investigate and compare the secret-key capacity based on the sampling of the entire complex channel state information (CSI) or only its envelope, the received signal strength (RSS). Moreover, as opposed to previous works, we take into account the fact that the eavesdropper's observations might be correlated and we consider the high signal-to-noise ratio (SNR) regime where we can find simple analytical expressions for the secret-key capacity. As already found in previous works, we find that RSS-based secret-key generation is heavily penalized as compared to CSI-based systems. At high SNR, we are able to precisely and simply quantify this penalty: a halved pre-log factor and a constant penalty of about 0.69 bit, which disappears as Eve's channel gets highly correlated.**

***Index Terms*— Secret-key generation, RSS, CSI, physical-layer security.**

I. Introduction

A. Problem Statement

WE CONSIDER in this article the problem of generating secret keys between two legitimate users (Alice and Bob), subject to an illegitimate user (Eve) trying to recover the key. Maurer [2] and Ahlswede and Csiszár [3] were the first to analyze the problem of generating a secret key from correlated observations. In the source model (see Fig. 1), Alice, Bob and Eve observe the realizations of a discrete memoryless source. From their sequence of observations, Alice and Bob have to distill an identical key that remains secret from Eve. Moreover, Alice and Bob have access to a public error-free authenticated channel with unlimited capacity. This helps them to perform *information reconciliation*, *i.e.*, exchanging a few parity bits so as to agree on a common sequence of symbols. However, since the channel is public, Eve can gain information about the secret key from these parity bits, on top of her own channel observations that can also be correlated with Alice and Bob observations. This is why *privacy amplification* is usually implemented after *information reconciliation*, which consists in reducing the size of the key, so that Eve information about the key is completely eliminated. Upper and lower bounds for the secret-key capacity, defined as the number of secret bits that can be generated per observation of the source, were derived in [2], [3]. In this work, we are interested in computing the secret-key capacity. Thus, we do not consider *information reconciliation* and *privacy amplification*. In practice they can be implemented through the use of, *e.g.*, low parity density check codes and universal hashing respectively. The interested reader is referred to [4] for more information on the subject.

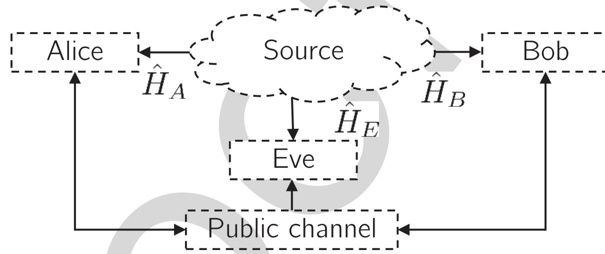


Fig. 1. Source model for secret-key agreement.

A practical source of common randomness at Alice and Bob consists of the wireless channel reciprocity, which implies that the propagation channel from Alice to Bob and from Bob to Alice is identical if both are measured within the same channel coherence time and at the same frequency. At successive coherence times, Alice and Bob can repeatedly sample the channel by sending each other a pilot symbol so as to obtain a set of highly correlated observations and finally start a key-distillation procedure. In this article, we investigate the secret-key capacity relying on the entire complex channel state information (CSI) or only on the channel envelope, sometimes

Manuscript received June 19, 2020; revised September 24, 2020; accepted November 18, 2020. The research reported herein was partly funded by the Fonds national de la recherche scientifique (F.R.S.-FNRS). This article has been presented in part at the IEEE PIMRC 2020 Conference. The associate editor coordinating the review of this article and approving it for publication was R. Thobaben. *(Corresponding author: François Rottenberg.)*

François Rottenberg is with the Université Catholique de Louvain, 1348 Louvain-la-Neuve, Belgium, and also with the Université Libre de Bruxelles, 1050 Brussels, Belgium (e-mail: francois.rottenberg@uclouvain.be).

Trung-Hien Nguyen, Jean-Michel Dricot, and François Horlin are with the Université Libre de Bruxelles, 1050 Brussels, Belgium.

Jérôme Louveaux is with the Université Catholique de Louvain, 1348 Louvain-la-Neuve, Belgium.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCOMM.2020.3040434.

Digital Object Identifier 10.1109/TCOMM.2020.3040434

also referred to as received signal strength (RSS).[1] We also consider the case where Eve's observations are correlated with the ones of Alice and Bob, which can occur in many practical situations. Related works are detailed in the next subsection while our contributions are presented in the subsequent subsection.

B. State of the Art

This study falls into the broad field of physical-layer security (PLS), which has attracted much interest in the recent decade as a competitive candidate to provide authentication, integrity and confidentiality in future communication networks [5]–[7]. We refer to [4] for an overview on the area. In the context of secret-key generation based on wireless reciprocity, there has been a large amount of related works, both from theoretical and experimental aspects [8]–[10]. In several recent approaches, more general models than the source model have been considered for secret-key generation, taking advantage of the channel to transmit part of the key [11], [12].

Many works have considered using RSS as a source of randomness for secret-key generation [13]–[19]. In [20], the authors show how to exploit the channel diversity coming from the multipath nature of the channel. The work of [21] leverages the use of multiple-antenna systems. In [22], the authors incorporate the orthogonal frequency division multiplexing (OFDM) modulation and carrier frequency offset as a way to increase bit generation in static environments with limited mobility. The choice of using RSS over full CSI is mainly due to its practical convenience. As opposed to CSI, RSS indicators are usually available at the higher layers of the communication layers, allowing for simple implementation of the key distillation procedure, relying on the legacy network infrastructure (no need to change the physical layer). Moreover, RSS is intrinsically more robust to phase offsets between Alice and Bob, relaxing constraints on the hardware, the synchronization and the reciprocity calibration. On the other hand, in the full CSI approaches, the reconciliation of phase information between legitimate users requires tightly synchronized nodes. A key selling point of PLS versus its cryptographic counterparts is its low implementation complexity, which is particularly suited in applications such as the Internet-of-Things or sensor networks where low power devices are used. In this context, the RSS approach can be more suited than the full CSI one.

The main disadvantage of RSS-based secret-key generation is that it does not use the full channel information and thus achieves a lower secret-key capacity than its CSI-based counterpart. In certain PLS applications, larger data rates and thus key sizes are targeted, using more powerful devices. For these use cases, using the full CSI approach can be more suited than the RSS one. CSI-based secret-key capacity is generally easier to characterize analytically, which has been done in a large number of works [23], [24], relying on multi-antenna systems [25]–[29], ultrawideband channels [30], and on the OFDM [31]–[34]. The authors in [20] analytically compare RSS and CSI approaches. The work of [35] also compares the two approaches relying on a thorough experimental study in various propagation environments, with different degrees of mobility.

The majority of works in the literature considers that Eve gets no side information about the key from her observations, which consist of the pilots transmitted by Alice and Bob [13], [24], [25], [27], [28]. Often, this assumption is justified by the fact that the channel environment is supposed to be rich enough in scattering implying that the fading process of the channels decorrelates quickly as a function of distance. Then, the observations of Eve have negligible correlation if she is assumed to be separated from Bob and Alice by more than one wavelength (otherwise she could be easily detected). The assumption of rapid decorrelation in space has been validated through measurements in rich scattering environments [13], [24], [35]–[37]. Moreover, this assumption simplifies the expression of the secret-key capacity, which simply becomes equal to the mutual information between Alice and Bob. However, it also occurs in practical scenarios, such as outdoor environments, that scatterers are clustered with small angular spread rather than being uniformly distributed, which leads to much longer spatial decorrelation length. The work of [1], relying on practical 3GPP channel models has shown that the assumption of full decorrelation of Eve's observations with respect to Alice and Bob is not always verified and critically depends on the propagation environment. At a cellular carrier frequency of 1 GHz, $\lambda = 30$ cm and Eve could be placed at $10\lambda = 3$ m while still having a significant correlation. The experimental work of [17] has also shown that there remains a strong correlation of the eavesdropper's channel even at distances much larger than half a wavelength. In [38], the authors studied the impact of channel sparsity, inducing correlated eavesdropping, on the secret-key capacity. In [39], the impact of the number of paths and the eavesdropper separation is analytically studied. In [40], spatial and time correlation of the channel is taken into account using a Jakes Doppler model. In [41], [42], experiments are conducted indoor to evaluate the correlation of the eavesdropper's observations and its impact on the secret-key capacity. A similar study is conducted for a MIMO indoor measurement campaign in [26]. The work of [19] also uses an indoor experimental approach and proposes results of cross-correlation, mutual information and secret-key rates, which depend on the eavesdropper's position.

C. Contributions

Our main contribution is to propose a novel analytical comparison of the secret-key capacity based on RSS and CSI for a narrowband channel. As opposed to similar previous works such as [20], we do not assume that Eve's observations are uncorrelated. This more general case adds to the complexity of the study while remaining of practical importance. Moreover, the authors in [20] could characterize the secret-key capacity for envelope sampling with a simple analytical expression. However, their simplification relied on the approximation of a sum of envelope components as Gaussian, which is not

[1] We focus the whole study in this article on the envelope of the channel, not its power. However, the final results in terms of capacity are equivalent given the one-to-one relationship between envelope and power.

applicable for our channel model. Furthermore, other works have already compared RSS and CSI-based approaches taking into account correlated eavesdropping, such as [35]. However, the studies were mostly conducted experimentally and not analytically.

More specifically, our contributions can be summarized as follows: 1) We evaluate lower and upper bounds on the secret-key capacity for both the complex (full CSI) and the envelope (RSS) cases. In the complex case, we obtain simple closed-form expressions, while, in the envelope case, the bounds must be evaluated numerically. Some of the expressions in the complex case were already obtained in previous works. We chose to present them again in this work to provide a systematic framework and useful comparison benchmarks for the envelope case. 2) We show that, in a number of particular cases, the lower and upper bounds become tight: low correlation of the eavesdropper, relatively smaller noise variance at Bob than Alice (and vice versa) and specific high signal-to-noise ratio (SNR) regimes. 3) We show that, as soon as Alice (or Bob since everything is symmetrical) samples the envelope of her channel estimate, the other parties do not lose information by taking the envelopes of their own channel estimates. 4) We show that, in the high SNR regime, the bounds can be evaluated in closed-form and result in simple expressions. The penalty of envelope-based versus complex-based secret-key generation is: i) a pre-log factor of $1/2$ instead of 1, implying a slower slope of the secret-key capacity as a function of SNR and ii) a constant penalty of 0.69 bit, which disappears as Eve's channel gets highly correlated.

The rest of this article is structured as follows. Section II describes the transmission model used in this work. Sections III and IV study the secret-key capacity based on complex and envelope sampling, respectively. Section V numerically analyzes the obtained results. Finally, Section VI concludes the paper.

Notations

Matrices are denoted by bold uppercase letters. Non bold upper case letter refers to a random variable. Superscript * stands for conjugate operator. The symbol $\Re(.)$ denotes the real part. $\jmath$ is the imaginary unit. $|\mathbf{A}|$ is the determinant of matrix $\mathbf{A}$. The letters e and γ refer to the Euler number and the Euler-Mascheroni constant respectively. $h(.)$ and $I(.;.)$ refer to the differential entropy and the mutual information respectively. We use the notation $f(x) = O(g(x))$, as $x \to a$, if there exist positive numbers δ and λ such that $|f(x)| \leq \lambda g(x)$ when $0 < |x - a| < \delta$.

II. TRANSMISSION MODEL

Alice and Bob extract a common key from observations of their shared channel H, assumed to be reciprocal. The channel H is repeatedly sampled in time based on the transmission of *a priori* known pilots by Alice and Bob. We assume that the successive observations of H are distant enough in time so that they can be considered independent. Note that this is a conventional assumption in the literature [24], [27]. In practice, the sampling between successive samples can be related to the richness of scattering and the degree of mobility of the environment and the legitimate parties. During these successive observations, the environment remains stationary so that they can be considered as identically distributed. Considering a narrowband channel, the estimates of H at Alice's and Bob's sides, respectively denoted by $\hat{H}_A$ and $\hat{H}_B$, are given by

$$\hat{H}_A = H + W_A, \ \hat{H}_B = H + W_B,$$

where the additive noise samples W_A and W_B are modeled as independent zero mean circularly-symmetric complex Gaussian (ZMCSCG) random variables with variances σ_A^2 and σ_B^2 respectively.

The strategy of Eve consists in going as close as possible from Bob's antenna to try to maximize the correlation of its channel.[2] Then, Eve estimates her channel H_E between Alice's antenna and hers by intercepting the pilots sent from Alice to Bob. Since Eve is close to Bob, the channel from Alice to Eve will be spatially correlated with H while the channel between Bob and Eve will experience a negligible correlation with H. Therefore, we neglect the pilot sent by Bob and received by Eve in the following as she cannot get any useful information from it [39]. The channel estimate of Eve is given by

$$\hat{H}_E = H_E + W_E,$$

where W_E is modeled as ZMCSCG with variance σ_E^2. If Alice and Bob transmit a pilot of equal power and Alice, Bob and Eve use a similar receiver, one could expect a situation of equal noise variance $\sigma_A^2 = \sigma_B^2 = \sigma_E^2$. On the other hand, Eve could use a more powerful receiver than Alice and/or Bob by having, *e.g.*, a larger antenna size, a multi-antenna receiver or an amplifier with lower noise figure. This would result in a lower noise variance σ_E^2. Moreover, a different pilot power transmitted by Alice and Bob will induce variations in their noise variances σ_A^2 and σ_B^2. Indeed, in practice, the channel estimates $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$ are obtained by dividing the received signal, which includes the additive noise, by an *a priori* known pilot. For instance, if the pilot transmitted by Bob has a stronger power, the noise power at Alice σ_A^2 will be relatively weaker.

This scenario corresponds to the memoryless source model for secret-key agreement [3], [4] represented in Fig. 1: Alice, Bob and Eve observe a set of independent and identically distributed (i.i.d.) repetitions of the random variables $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$. Moreover, an error-free authenticated public channel of unlimited capacity is available for communication. All parties have access to the public channel.

In the following section, we will study the secret-key capacity of this model. To do this, we need to know the probability distributions of the random variables $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$, which directly depend on the probability distributions of W_A, W_B, W_E, H and H_E. The distributions of W_A, W_B and W_E were already detailed. Moreover, measurement campaigns have shown that the channels H and H_E can be accurately

[2]Note that all of the following derivations are symmetrical if Eve gets close to Alice instead of Bob.

modeled with a ZMCSCG distribution, especially in non-line-of-sight situations and rich scattering environments [43]. This model is commonly referred to as Rayleigh fading [44]. Therefore, we assume that (H, H_E) follows a ZMCSCG with covariance matrix given by

$$\mathbf{C}_{HH_E} = p \begin{pmatrix} 1 & \rho \\ \rho^* & 1 \end{pmatrix},$$

where p is the channel variance, such that $0 < p < \infty$. We assume that H and H_E have the same variance p, which makes sense in practice if Bob and Eve are close enough so as to belong to the same local area [43]. The coefficient $\rho = \mathbb{E}(HH_E^*)/p$ is the spatial correlation coefficient, such that $0 \le |\rho| \le 1$. We refer to [1], [43] for more information on the definition of this coefficient. In the following, we use the fact the differential entropy of a circularly symmetric Gaussian with covariance $\mathbf{C}$ is given by $\log_2(|\pi e \mathbf{C}|)$, where e is the Euler number.

In the sequel, at different places, we will consider the high SNR regime. When this regime is considered, we will always assume, implicitly or explicitly, that, as $\sigma_A^2 \to 0$, $\sigma_B^2 \to 0$ and $\sigma_E^2 \to 0$,

(**As1**): the ratio $\frac{\sigma_A^2}{\sigma_B^2}$ remains fixed and $0 < \frac{\sigma_A^2}{\sigma_B^2} < \infty$,

(**As2**): the ratio $\frac{\sigma_A^2}{\sigma_E^2}$ remains fixed and $0 < \frac{\sigma_A^2}{\sigma_E^2} < \infty$,

(**As3**): the ratio $\frac{\sigma_B^2}{\sigma_E^2}$ remains fixed and $0 < \frac{\sigma_B^2}{\sigma_E^2} < \infty$.

III. Secret-Key Capacity Based on Complex Channel Sampling

In this section, we analyze the secret-key capacity associated with complex channel sampling, that we denote by C_s^{Cplex}. Most of the results come from a direct evaluation of standard formulas for the differential entropy of Gaussian random variables. The result on the mutual information between Alice and Bob was already presented in [23]. We still present them as they provide accurate benchmarks as a comparison with the novel results that we derive for the envelope case in Section IV.

The secret-key capacity is defined as the maximal rate at which Alice and Bob can agree on a secret-key while keeping the rate at which Eve obtains information about the key arbitrarily small for a sufficiently large number of observations. Moreover, Alice and Bob should agree on a common key with high probability and the key should approach the uniform distribution. We refer to [2]–[4] for a formal definition. As explained in Section II, we consider that Eve gets useful information from her observation $\hat{H}_E$ over H. This implies that the secret-key capacity is not simply equal to $I(\hat{H}_A; \hat{H}_B)$, as was considered in many previous works [13], [23], [24], [27], [28]. Finding the general expression of the secret-key capacity for a given probability distribution of $\hat{H}_A, \hat{H}_B, \hat{H}_E$ is still an open problem. From [2], [3] [4, Prop. 5.4], the secret-key capacity, expressed in the number of generated secret bits per channel observation, can be lower and upper bounded as follows

$$C_s^{\text{Cplex}} \ge I(\hat{H}_A; \hat{H}_B) - \min\left[I(\hat{H}_A; \hat{H}_E), I(\hat{H}_B; \hat{H}_E)\right] \quad (1)$$

$$C_s^{\text{Cplex}} \le \min\left[I(\hat{H}_A; \hat{H}_B), I(\hat{H}_A; \hat{H}_B | \hat{H}_E)\right]. \quad (2)$$

The lower bound (1) implies that, if Eve has less information about $\hat{H}_B$ than Alice or respectively about $\hat{H}_A$ than Bob, such a difference can be leveraged for secrecy [2]. Moreover, this rate can be achieved with one-way communication. On the other hand, the upper bound (2) implies that the secret-key rate cannot exceed the mutual information between Alice and Bob. Moreover, the secret-key rate cannot be higher than the mutual information between Alice and Bob if they happened to learn Eve's observation $\hat{H}_E$. In particular cases, the lower and upper bounds can become tight. In our context, three particular cases can be distinguished:

1) $\rho = 0$: Eve does not learn anything about H from $\hat{H}_E$, which becomes independent from $\hat{H}_A$ and $\hat{H}_B$. This leads to the trivial result $C_s^{\text{Cplex}} = I(\hat{H}_A; \hat{H}_B)$.
2) $\sigma_B^2 = 0$: this implies that $\hat{H}_A \to \hat{H}_B \to \hat{H}_E$ forms a Markov chain, which leads to [4, Corol. 4.1]
$$C_s^{\text{Cplex}} = I(\hat{H}_A; \hat{H}_B | \hat{H}_E) = I(\hat{H}_A; \hat{H}_B) - I(\hat{H}_A; \hat{H}_E).$$
3) $\sigma_A^2 = 0$: symmetrically as in 2), $C_s^{\text{Cplex}} = I(\hat{H}_A; \hat{H}_B | \hat{H}_E) = I(\hat{H}_A; \hat{H}_B) - I(\hat{H}_B; \hat{H}_E)$.

Cases 2) and 3) are only met when σ_B^2 or σ_A^2 are exactly zero, which never occurs in practice since all electronic devices suffer from, *e.g.*, thermal noise. However, cases 2) and 3) can be approached in particular situations in practice where $\sigma_A^2 \ll \sigma_B^2$ or $\sigma_B^2 \ll \sigma_A^2$. This could happen for instance if Alice sends a pilot with much stronger power than the one of Bob or if Alice uses an amplifier with much larger noise figure. Then, the SNR of the channel estimate of Bob will be significantly higher so that $\sigma_B^2 \ll \sigma_A^2$.

In the next subsections, we evaluate the different expressions of the mutual information required to compute the lower and upper bounds of (1) and (2): i) the mutual information between Alice and Bob $I(\hat{H}_A; \hat{H}_B)$; ii) the mutual information between Alice and Eve $I(\hat{H}_A; \hat{H}_E)$, and similarly for Bob $I(\hat{H}_B; \hat{H}_E)$; and iii) the conditional mutual information between Alice and Bob given Eve's observations $I(\hat{H}_A; \hat{H}_B | \hat{H}_E)$.

A. Mutual Information Between Alice and Bob

Using previously introduced transmission and channel models, we can find that the random variables $\hat{H}_A$ and $\hat{H}_B$ are jointly Gaussian distributed with covariance

$$\mathbf{C}_{\hat{H}_A \hat{H}_B} = \begin{pmatrix} p + \sigma_A^2 & p \\ p & p + \sigma_B^2 \end{pmatrix}.$$

From this distribution, we find back the result of [23]

$$\begin{aligned} I(\hat{H}_A; \hat{H}_B) &= h(\hat{H}_A) + h(\hat{H}_B) - h(\hat{H}_A, \hat{H}_B) \\ &= \log_2\left(\frac{(p+\sigma_A^2)(p+\sigma_B^2)}{|\mathbf{C}_{\hat{H}_A \hat{H}_B}|}\right) \\ &= \log_2\left(1 + \frac{p}{\sigma_A^2 + \sigma_B^2 + \frac{\sigma_A^2 \sigma_B^2}{p}}\right). \quad (5) \end{aligned}$$

This rate corresponds to the secret-key capacity in case of uncorrelated observations at Eve ($\rho = 0$). At high SNR, as $\sigma_A^2 \to 0$ and $\sigma_B^2 \to 0$, the expressions becomes

$$I(\hat{H}_A;\hat{H}_B) = \log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) + O\left(\sigma_A^2\right), \tag{6}$$

which is characterized by a *pre-log factor* of one.

B. Mutual Information Between Alice/Bob and Eve

We can observe that $\hat{H}_A$ and $\hat{H}_E$ are jointly Gaussian distributed with covariance

$$\mathbf{C}_{\hat{H}_A\hat{H}_E} = \begin{pmatrix} p+\sigma_A^2 & \rho p \\ \rho^* p & p+\sigma_E^2 \end{pmatrix}.$$

This leads to the mutual information

$$\begin{aligned} I(\hat{H}_A;\hat{H}_E) &= \log_2\left(\frac{(p+\sigma_A^2)(p+\sigma_E^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) \\ &= \log_2\left(1+\frac{p|\rho|^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2+\frac{\sigma_A^2\sigma_E^2}{p}}\right). \end{aligned}$$

The mutual information $I(\hat{H}_B;\hat{H}_E)$ can be similarly obtained, simply replacing subscript A by B. Using the previously derived expressions of $I(\hat{H}_A;\hat{H}_B)$, $I(\hat{H}_A;\hat{H}_E)$ and $I(\hat{H}_B;\hat{H}_E)$, we find that the lower bound in (1) evaluates to (3), as shown at the bottom of the page. Note that the lower bound is not restricted to be positive (as will also be shown numerically in Section V), in which case it becomes useless since, by definition, $C_s^{\mathrm{Cplex}} \geq 0$. Nonetheless, it does not necessarily imply that $C_s^{\mathrm{Cplex}} = 0$. We can find the condition on the minimum noise variance at Eve σ_E^2 for having a larger-than-zero lower bound

$$\sigma_E^2 > p(|\rho|^2-1) + |\rho|^2\min(\sigma_A^2,\sigma_B^2). \tag{7}$$

In the worst-case, $|\rho| = 1$ and σ_E^2 has to be larger than the minimum of the noise variances of Alice and Bob. We can invert (7) to find the maximal correlation coefficient $|\rho|^2$ to have a larger-than-zero lower bound

$$|\rho|^2 < \frac{p+\sigma_E^2}{p+\min(\sigma_A^2,\sigma_B^2)}.$$

In the high SNR regime, as $\sigma_A^2 \to 0$, $\sigma_B^2 \to 0$ and $\sigma_E^2 \to 0$, equation (3) becomes

$$\begin{aligned} C_s^{\mathrm{Cplex}} &\geq \log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) \\ &\quad -\log_2\left(\frac{p}{p(1-|\rho|^2)+\max(\sigma_A^2,\sigma_B^2)+\sigma_E^2}\right) \\ &\quad +O\left(\sigma_A^2\right). \end{aligned} \tag{8}$$

As soon as $|\rho| < 1$, C_s^{Cplex} is unbounded and goes to infinity as the SNR grows large. Indeed, $I(\hat{H}_A;\hat{H}_B)$ is unbounded, while $I(\hat{H}_A;\hat{H}_E)$ and $I(\hat{H}_B;\hat{H}_E)$ converge to $\log_2\left(\frac{1}{1-|\rho|^2}\right)$, which is bounded away from zero for $|\rho| < 1$.

C. Conditional Mutual Information Between Alice and Bob

We can note that $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$ are jointly Gaussian distributed with covariance matrix

$$\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E} = \begin{pmatrix} p+\sigma_A^2 & p & \rho p \\ p & p+\sigma_B^2 & \rho p \\ \rho^* p & \rho^* p & p+\sigma_E^2 \end{pmatrix},$$

which gives

$$\begin{aligned} I(\hat{H}_A;\hat{H}_B|\hat{H}_E) &= h(\hat{H}_A,\hat{H}_E) - h(\hat{H}_E) \\ &\quad + h(\hat{H}_B,\hat{H}_E) - h(\hat{H}_A,\hat{H}_B,\hat{H}_E) \\ &= \log_2\left(\frac{|\mathbf{C}_{\hat{H}_A\hat{H}_E}||\mathbf{C}_{\hat{H}_B\hat{H}_E}|}{(p+\sigma_E^2)|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}\right). \end{aligned} \tag{9}$$

The upper bound in (2) is then given by the minimum of $I(\hat{H}_A;\hat{H}_B|\hat{H}_E)$ and $I(\hat{H}_A;\hat{H}_B)$. In Appendix VII-A, we prove that the condition $I(\hat{H}_A;\hat{H}_B|\hat{H}_E) \leq I(\hat{H}_A;\hat{H}_B)$ is always verified under the jointly Gaussian channel model considered in this work. The upper bound is thus given by (4), as shown at the bottom of the page.

Based on the analytical expressions of the upper and lower bounds, we can find a novel condition for tightness of the bounds at high SNR.

Proposition 1: Under $(\mathbf{As1})-(\mathbf{As3})$*, as* $\sigma_A^2 \to 0$*,* $\sigma_B^2 \to 0$ *and* $\sigma_E^2 \to 0$*, if* $|\rho| < 1$*, the upper and lower bounds of (3) and (4) become tight and the secret-key capacity is given by*

$$C_s^{\mathrm{Cplex}} = \log_2\left(\frac{p(1-|\rho|^2)}{\sigma_A^2+\sigma_B^2}\right) + O\left(\sigma_A^2\right). \tag{10}$$

Proof: The proof is easily obtained by taking the limits in (3) and (4) and seeing that they both converge towards (10), provided that $|\rho| < 1$. □

IV. Secret-Key Capacity Based on Channel Envelope Sampling

The goal of this section is to evaluate the impact on the secret-key capacity if Alice and Bob rely on the envelopes of their observations rather than the complex values to generate a secret key. We denote by C_s^{Evlpe} the secret-key capacity based on envelope sampling. We also introduce the notations

$$\hat{H}_A = \hat{R}_A e^{\jmath\hat{\Phi}_A},\ \hat{H}_B = \hat{R}_B e^{\jmath\hat{\Phi}_B},\ \hat{H}_E = \hat{R}_E e^{\jmath\hat{\Phi}_E},$$

where $\hat{R}_A$, $\hat{R}_B$ and $\hat{R}_E$ are the random modules of $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$ respectively. Similarly, $\hat{\Phi}_A$, $\hat{\Phi}_B$ and $\hat{\Phi}_E$ are their random phases. Note that $\hat{H}_A$ is equivalently represented by

$$C_s^{\mathrm{Cplex}} \geq \log_2\left(1+\frac{p}{\sigma_A^2+\sigma_B^2+\frac{\sigma_A^2\sigma_B^2}{p}}\right) - \log_2\left(1+\frac{p|\rho|^2}{p(1-|\rho|^2)+\max(\sigma_A^2,\sigma_B^2)+\sigma_E^2+\frac{\max(\sigma_A^2,\sigma_B^2)\sigma_E^2}{p}}\right). \tag{3}$$

$$C_s^{\mathrm{Cplex}} \leq \log_2\left(\frac{\left[(p+\sigma_A^2)(p+\sigma_E^2)-|\rho p|^2\right]\left[(p+\sigma_B^2)(p+\sigma_E^2)-|\rho p|^2\right]}{(p+\sigma_E^2)\left[(p(\sigma_A^2+\sigma_B^2)+\sigma_A^2\sigma_B^2)(p+\sigma_E^2)-|\rho p|^2(\sigma_A^2+\sigma_B^2)\right]}\right) \tag{4}$$

$\hat{R}_A$ and $\hat{\Phi}_A$ or $\Re(\hat{H}_A)$ and $\Im(\hat{H}_A)$. We start by stating an insightful result from [20, Th. 2], that we generalize for Eve's observations.

Proposition 2: The mutual information $I(\hat{H}_A; \hat{H}_E)$ satisfies

$$\begin{aligned} I(\hat{H}_A; \hat{H}_E) &= I(\Re(\hat{H}_A); \Re(\hat{H}_E)) + I(\Im(\hat{H}_A); \Im(\hat{H}_E)) \\ &\geq I(\hat{R}_A; \hat{R}_E) + I(\hat{\Phi}_A; \hat{\Phi}_E). \end{aligned}$$

Similarly, the mutual information $I(\hat{H}_A; \hat{H}_B)$ satisfies

$$\begin{aligned} I(\hat{H}_A; \hat{H}_B) &= I(\Re(\hat{H}_A); \Re(\hat{H}_B)) + I(\Im(\hat{H}_A); \Im(\hat{H}_B)) \\ &\geq I(\hat{R}_A; \hat{R}_B) + I(\hat{\Phi}_A; \hat{\Phi}_B). \end{aligned}$$

Proof: We conduct the proof for the more general case $I(\hat{H}_A; \hat{H}_E)$. Indeed, the mutual information $I(\hat{H}_A; \hat{H}_B)$ can be seen as a particular case for $\rho = 1$ and replacing subscripts E by B. On the one hand, we have

$$\begin{aligned} I(\hat{H}_A; \hat{H}_E) &= I(\hat{R}_A, \hat{\Phi}_A; \hat{R}_E, \hat{\Phi}_E) \\ &= h(\hat{R}_A, \hat{\Phi}_A) - h(\hat{R}_A, \hat{\Phi}_A | \hat{R}_E, \hat{\Phi}_E) \\ &\overset{(*)}{=} h(\hat{R}_A) - h(\hat{R}_A | \hat{R}_E, \hat{\Phi}_E) + h(\hat{\Phi}_A) \\ &\quad - h(\hat{\Phi}_A | \hat{R}_A, \hat{R}_E, \hat{\Phi}_E) \\ &\overset{(**)}{\geq} I(\hat{R}_A; \hat{R}_E) + I(\hat{\Phi}_A; \hat{\Phi}_E), \end{aligned}$$

where $(*)$ follows from the chain rule for entropy and the fact that $\hat{R}_A$ and $\hat{\Phi}_A$ are independent since the envelope and the phase of a ZMCSG are independent. $(**)$ follows from the fact that: i) $h(\hat{R}_A | \hat{R}_E, \hat{\Phi}_E) = h(\hat{R}_A | \hat{R}_E)$ since $(\hat{R}_A, \hat{R}_E)$ and $\hat{\Phi}_E$ are independent; ii) $h(\hat{\Phi}_A | \hat{R}_A, \hat{R}_E, \hat{\Phi}_E) \geq h(\hat{\Phi}_A | \hat{\Phi}_E)$ by the general properties of differential entropy and since $(\hat{\Phi}_A, \hat{\Phi}_E)$ is not independent from $(\hat{R}_A, \hat{R}_E)$. The proofs for the (in)dependence of random variables are given in Appendix VII-B.

On the other hand, a similar derivation can be made for $I(\Re(\hat{H}_A), \Im(\hat{H}_A); \Re(\hat{H}_E), \Im(\hat{H}_E))$, noticing that $\hat{H}_A$ and $\hat{H}_E$ are two ZMCSG, implying that their real and imaginary parts are independent, resulting in an equality with $I(\hat{H}_A; \hat{H}_E)$. □

Intuitively, this result can be explained by the fact that the random vectors $(\hat{\Phi}_A, \hat{\Phi}_E)$ and $(\hat{R}_A, \hat{R}_E)$ are not independent from one another while $(\Re(\hat{H}_A), \Re(\hat{H}_E))$ and $(\Im(\hat{H}_A), \Im(\hat{H}_E))$ are. There is thus a loss of information by treating phase and envelope separately as opposed to real and imaginary parts. This loss (or in other words the tightness of the inequality) is evaluated in [20, Fig. 2], where it is shown that the gap is significant and depends on the SNR. Interestingly, the mutual information between the phases $I(\hat{\Phi}_A; \hat{\Phi}_E)$ contains relatively more information than the mutual information between the envelopes $I(\hat{R}_A; \hat{R}_E)$.

One could wonder what is the best strategy of Bob and Eve if Alice uses $\hat{R}_A$ to generate a key. Imagine Bob and Eve have a more advanced receiver so that they can sample their observations in the complex domain, would it be beneficial for them? The answer is no, as shown in the following proposition.

Proposition 3: If Alice uses the envelope of her observations $\hat{R}_A$, then Eve does not lose information by taking the envelope of $\hat{H}_E$

$$I(\hat{R}_A; \hat{H}_E) = I(\hat{R}_A; \hat{R}_E).$$

Similarly, Bob does not lose information by taking the envelope of $\hat{H}_B$

$$I(\hat{R}_A; \hat{H}_B) = I(\hat{R}_A; \hat{R}_B).$$

The same result holds if Alice and Bob's roles are interchanged.

Proof: We conduct the proof for the more general case $I(\hat{R}_A; \hat{H}_E)$. Indeed, the mutual information $I(\hat{R}_A; \hat{H}_B)$ can be seen as a particular case for $\rho = 1$ and replacing subscripts E by B. By definition, we have

$$\begin{aligned} I(\hat{R}_A; \hat{R}_E, \hat{\Phi}_E) &= h(\hat{R}_E, \hat{\Phi}_E) - h(\hat{R}_E, \hat{\Phi}_E | \hat{R}_A) \\ &\overset{(*)}{=} h(\hat{R}_E) - h(\hat{R}_E | \hat{R}_A) + h(\hat{\Phi}_E) \\ &\quad - h(\hat{\Phi}_E | \hat{R}_A, \hat{R}_E) \\ &\overset{(**)}{=} I(\hat{R}_A; \hat{R}_E), \end{aligned}$$

where $(*)$ relies on the chain rule for entropy and the fact that $\hat{R}_E$ and $\hat{\Phi}_E$ are independent since the envelope and the phase of a ZMCSG are independent. $(**)$ relies on the fact that $h(\hat{\Phi}_E | \hat{R}_A, \hat{R}_E) = h(\hat{\Phi}_E)$ since $(\hat{R}_A, \hat{R}_E)$ and $\hat{\Phi}_E$ are independent. We refer to Appendix VII-B for the proofs on (in)dependence of random variables. □

Intuitively, the proposition can be explained by the fact that $\hat{\Phi}_B$ and $\hat{\Phi}_E$ are independent from $(\hat{R}_A, \hat{R}_B)$ and $(\hat{R}_A, \hat{R}_E)$ respectively. The propositions provide practical insight in the sense that, as soon as Alice (or Bob since everything is symmetrical) samples the envelope of her channel estimate, the other parties do not lose information by taking the envelopes of their own channel estimates. The other way around, Bob or Eve would not gain information to work on their complex channel estimate. In the light of this result, the definitions of the bounds of the secret-key capacity defined in (1) and (2) also hold here by replacing the complex values by their envelopes, *i.e.*, $\hat{R}_A$, $\hat{R}_B$ and $\hat{R}_E$ instead of $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$ respectively:

$$C_s^{\text{Evlpe}} \geq I(\hat{R}_A; \hat{R}_B) - \min\left[I(\hat{R}_A; \hat{R}_E), I(\hat{R}_B; \hat{R}_E)\right] \quad (11)$$

$$C_s^{\text{Evlpe}} \leq \min\left[I(\hat{R}_A; \hat{R}_B), I(\hat{R}_A; \hat{R}_B | \hat{R}_E)\right]. \quad (12)$$

Tight bounds can be found in the same cases and for the same reasons as in the complex case: 1) $\rho = 0$, 2) $\sigma_B^2 = 0$ and 3) $\sigma_A^2 = 0$.

Similarly as in Section III, we evaluate in the following subsections the quantities required to compute the lower and upper bounds (11) and (12): in Section IV-A, the mutual information between Alice and Bob $I(\hat{R}_A; \hat{R}_B)$; in Section IV-B, the mutual information between Alice and Eve $I(\hat{R}_A; \hat{R}_E)$, and similarly for Bob $I(\hat{R}_B; \hat{R}_E)$; and in Section IV-C, the conditional mutual information between Alice and Bob given Eve's observations $I(\hat{R}_A; \hat{R}_B | \hat{R}_E)$. Since $I(\hat{R}_A; \hat{R}_B)$ can be seen as a particularization of $I(\hat{R}_A; \hat{R}_E)$ for $\rho = 1$ and replacing subscript B by E, we will refer to Section IV-B for the proofs of the results in Section IV-A.

A. Mutual Information Between Alice and Bob

The mutual information between Alice and Bob is given by

$$I(\hat{R}_A; \hat{R}_B) = h(\hat{R}_A) + h(\hat{R}_B) - h(\hat{R}_A, \hat{R}_B). \quad (16)$$

The envelope of a ZMCSG random variable is well known to be Rayleigh distributed, *i.e.*, $\hat{R}_A \sim \text{Rayleigh}(\sqrt{\frac{p+\sigma_A^2}{2}})$ and $\hat{R}_B \sim \text{Rayleigh}(\sqrt{\frac{p+\sigma_B^2}{2}})$. The differential entropy of a Rayleigh distribution is also well known and is equal to [45]

$$h(\hat{R}_A) = \frac{1}{2}\log_2\left(\frac{p+\sigma_A^2}{4}\right) + \frac{1}{2}\log_2(e^{2+\gamma}) \tag{17}$$

$$h(\hat{R}_B) = \frac{1}{2}\log_2\left(\frac{p+\sigma_B^2}{4}\right) + \frac{1}{2}\log_2(e^{2+\gamma}), \tag{18}$$

where γ is the Euler-Mascheroni constant and e is the Euler number. On the other hand, the joint differential entropy of $(\hat{R}_A, \hat{R}_B)$ is more difficult to compute. The following lemma gives the joint probability density function (PDF) of $(\hat{R}_A, \hat{R}_B)$.

Lemma 1: The joint PDF of $(\hat{R}_A, \hat{R}_B)$ is given by (13), as shown at the bottom of the page, where $I_0(.)$ is the zero order modified Bessel function of the first kind.

Proof: The proof is obtained as a particular case of Lemma 3 for $\rho = 1$ and replacing subscripts E by B. □

Unfortunately, finding a closed-form expression for the joint differential entropy $h(\hat{R}_A, \hat{R}_B)$ is non-trivial given the presence of the Bessel function [45]. Still, $h(\hat{R}_A, \hat{R}_B)$ and thus $I(\hat{R}_A; \hat{R}_B)$, can be evaluated by numerical integration, relying on the PDF obtained in Lemma 1.

In the high SNR regime, the following lemma shows the limiting behavior of the PDF $f_{\hat{R}_A,\hat{R}_B}(\hat{r}_A, \hat{r}_B)$, which can be used to obtain a simple closed-form expression of $I(\hat{R}_A; \hat{R}_B)$, as shown in the subsequent theorem.

Lemma 2: Under $(\mathbf{As1})$, as $\sigma_A^2 \to 0$ and $\sigma_B^2 \to 0$, the PDF $f_{\hat{R}_A,\hat{R}_B}(\hat{r}_A, \hat{r}_B)$ asymptotically converges to

$$f_{\hat{R}_A,\hat{R}_B}(\hat{r}_A, \hat{r}_B) = \frac{2\hat{r}_A e^{-\frac{\hat{r}_A^2}{p}}}{p} \frac{e^{-\frac{(\hat{r}_B-\hat{r}_A)^2}{\sigma_A^2+\sigma_B^2}}}{\sqrt{\pi(\sigma_A^2+\sigma_B^2)}} + O(\sigma_A),$$

which corresponds to the product of a Rayleigh distribution of parameter $\frac{p}{2}$ and a conditional normal distribution centered in $\hat{R}_A$ and of variance $\frac{\sigma_A^2+\sigma_B^2}{2}$.

Proof: The proof is obtained as a particular case of Lemma 4 for $\rho = 1$ and replacing subscripts E by B. Since $\rho = 1$, the limit $|\rho| \to 1$ can be omitted. □

Theorem 1: Under $(\mathbf{As1})$, as $\sigma_A^2 \to 0$ and $\sigma_B^2 \to 0$, the mutual information $I(\hat{R}_A; \hat{R}_B)$ converges to

$$I(\hat{R}_A; \hat{R}_B) \to \tfrac{1}{2}\log_2\left(\tfrac{p}{\sigma_A^2+\sigma_B^2}\right) - \chi,$$

where $\chi = \frac{1}{2}\log_2\left(\frac{4\pi}{e^{1+\gamma}}\right)$ is a constant penalty, given by 0.69 (up to the two first decimals).

Proof: The proof is obtained as a particular case of Theorem 2 for $\rho = 1$ and replacing subscripts E by B. Since $\rho = 1$, the limit $|\rho| \to 1$ can be omitted. □

The expression obtained in Theorem 1 gives a lot of insight on the high SNR secret-key capacity that can be obtained with envelope sampling, when there is no correlation ($\rho = 0$). As shown in the left column of Table I, two penalties can be observed as compared to complex sampling: i) a *pre-log factor* of $1/2$ instead of 1, implying a curve with smaller slope and ii) an additional penalty of a constant χ equivalent to about 0.69 bit. One should note that halved slope could be intuitively expected. Indeed, the full CSI approach samples two independent real-valued random variables while the RSS approach, only one.

B. Mutual Information Between Alice/Bob and Eve

We now analyze the mutual information between Alice and Eve and between Bob and Eve, which are given by

$$\begin{aligned} I(\hat{R}_A; \hat{R}_E) &= h(\hat{R}_A) + h(\hat{R}_E) - h(\hat{R}_A, \hat{R}_E) \\ I(\hat{R}_B; \hat{R}_E) &= h(\hat{R}_B) + h(\hat{R}_E) - h(\hat{R}_B, \hat{R}_E). \end{aligned} \tag{19}$$

We already computed the values of $h(\hat{R}_A)$ and $h(\hat{R}_B)$. Similarly as for $\hat{R}_A$ and $\hat{R}_B$, we find that $\hat{R}_E \sim \text{Rayleigh}(\sqrt{\frac{p+\sigma_E^2}{2}})$ and [45]

$$h(\hat{R}_E) = \frac{1}{2}\log_2\left(\frac{p+\sigma_E^2}{4}\right) + \frac{1}{2}\log_2(e^{2+\gamma}). \tag{20}$$

The following lemma gives the joint PDFs of $(\hat{R}_A, \hat{R}_E)$ and $(\hat{R}_B, \hat{R}_E)$.

Lemma 3: The joint PDF of $(\hat{R}_A, \hat{R}_E)$ is given by (14), as shown at the bottom of the page. The joint PDF $f_{\hat{R}_B,\hat{R}_E}(\hat{r}_B, \hat{r}_E)$ is similarly obtained, replacing subscripts A by B.

Proof: The proof is given in Appendix VII-C. □

As for $h(\hat{R}_A, \hat{R}_B)$, it is difficult to find a closed-form expression of $h(\hat{R}_A, \hat{R}_E)$ and $h(\hat{R}_B, \hat{R}_E)$ due to the presence of the Bessel function. However, they can be evaluated numerically using the PDFs obtained in Lemma 3 so that $I(\hat{R}_A; \hat{R}_E)$ and $I(\hat{R}_B; \hat{R}_E)$ can be evaluated. Still, in specific regimes, closed-form solutions can be found.

$$f_{\hat{R}_A,\hat{R}_B}(\hat{r}_A, \hat{r}_B) = \frac{4\hat{r}_A\hat{r}_B}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} I_0\left(\frac{2p\hat{r}_A\hat{r}_B}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) \exp\left(-\frac{\hat{r}_A^2(p+\sigma_B^2) + \hat{r}_B^2(p+\sigma_A^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) \tag{13}$$

$$f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) = \frac{4\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} I_0\left(\frac{2p|\rho|\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) \exp\left(-\frac{\hat{r}_A^2(p+\sigma_E^2) + \hat{r}_E^2(p+\sigma_A^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) \tag{14}$$

$$\begin{aligned} f_{\hat{R}_A,\hat{R}_B,\hat{R}_E}(\hat{r}_A, \hat{r}_B, \hat{r}_E) &= \frac{8\hat{r}_A\hat{r}_B\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|} G\left(\frac{2p(p(1-|\rho|^2)+\sigma_E^2)\hat{r}_A\hat{r}_B}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}, \frac{2|\rho|p\sigma_B^2\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}, \frac{2|\rho|p\sigma_A^2\hat{r}_B\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}\right) \\ &\quad \exp\left(-\frac{\hat{r}_A^2|\mathbf{C}_{\hat{H}_B\hat{H}_E}| + \hat{r}_B^2|\mathbf{C}_{\hat{H}_A\hat{H}_E}| + \hat{r}_E^2|\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}\right) \end{aligned} \tag{15}$$

TABLE I

HIGH SNR SECRET-KEY CAPACITY OF COMPLEX (CSI) VERSUS ENVELOPE (RSS) SAMPLING IN BOTH UNCORRELATED AND CORRELATED CASES, UNDER $(\mathbf{As1})$-$(\mathbf{As3})$. $\chi = 0.69\ldots$, $\sigma_*^2 = \max(\sigma_A^2, \sigma_B^2)$, $\epsilon_{\text{uncrl}} \to 0$, $\epsilon_{\text{crl}} \to 0$ ASYMPTOTICALLY

	High SNR ($\sigma_A^2, \sigma_B^2 \to 0$), uncorrelated ($\rho = 0$)	High SNR ($\sigma_A^2, \sigma_B^2, \sigma_E^2 \to 0$), correlated ($\|\rho\| > 0$)
Complex	$C_s^{\text{Cplex}} = \log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) + O(\sigma_A^2)$	$C_s^{\text{Cplex}} \geq \log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) - \log_2\left(\frac{p}{p(1-\|\rho\|^2)+\sigma_*^2+\sigma_E^2}\right) + O(\sigma_A^2)$
Envelope	$C_s^{\text{Evlpe}} = \frac{1}{2}\log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) - \chi + \epsilon_{\text{uncrl}}$	$C_s^{\text{Evlpe}} \underset{\|\rho\|\to 1}{\geq} \frac{1}{2}\left[\log_2\left(\frac{p}{\sigma_A^2+\sigma_B^2}\right) - \log_2\left(\frac{p}{p(1-\|\rho\|^2)+\sigma_*^2+\sigma_E^2}\right)\right] + \epsilon_{\text{crl}}$

In the low correlation regime, when $|\rho| \to 0$, it is easy to see that $f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E)$ converges to the product of two independent Rayleigh PDFs $f_{\hat{R}_A}(\hat{r}_A) f_{\hat{R}_E}(\hat{r}_E)$ and thus $h(\hat{R}_A,\hat{R}_E) = h(\hat{R}_A) + h(\hat{R}_E)$. As could be expected, we find that $I(\hat{R}_A;\hat{R}_E) = I(\hat{R}_B;\hat{R}_E) = 0$ and the secret-key capacity is given by Theorem 1.

In the high SNR and correlation regime, the following lemma shows the limiting behavior of the PDFs of $(\hat{R}_A,\hat{R}_E)$ and $(\hat{R}_B,\hat{R}_E)$, which can be used to obtain a simple closed-form expression of $I(\hat{R}_A;\hat{R}_E)$ and $I(\hat{R}_B;\hat{R}_E)$.

Lemma 4: Under $(\mathbf{As2})$*, as* $|\rho| \to 1$, $\sigma_A^2 \to 0$ *and* $\sigma_E^2 \to 0$*, the PDF* $f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E)$ *asymptotically converges to*

$$f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E) = \frac{2\hat{r}_E e^{-\frac{\hat{r}_E^2}{p}}}{p} \frac{e^{-\frac{(\hat{r}_A - |\rho|\hat{r}_E)^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}}}{\sqrt{\pi(p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2)}} + O\left(\sqrt{1-|\rho|^2+\sigma_A^2}\right),$$

which corresponds to the product of a Rayleigh and a normal distribution. The same results holds for $f_{\hat{R}_B,\hat{R}_E}(\hat{r}_B,\hat{r}_E)$*, replacing subscripts* A *by* B*, under* $(\mathbf{As3})$*.*

Proof: The proof is given in Appendix VII-D. □

Theorem 2: Under $(\mathbf{As2})$*, as* $|\rho| \to 1$, $\sigma_A^2 \to 0$ *and* $\sigma_E^2 \to 0$*, the mutual information* $I(\hat{R}_A;\hat{R}_E)$ *converges to*

$$I(\hat{R}_A;\hat{R}_E) \to \frac{1}{2}\log_2\left(\frac{p}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}\right) - \chi,$$

where the constant penalty χ *is defined in Theorem 1. The mutual information* $I(\hat{R}_B;\hat{R}_E)$ *can be similarly approximated by replacing subscripts* A *by* B*, under* $(\mathbf{As3})$*.*

Proof: The proof is given in Appendix VII-E. □

Using the result of Theorem 2, we can evaluate the lower bound on the secret-key capacity (11) in the high SNR, high correlation regime, which is given in the right column of Table I. As compared with the complex case, the only difference is the *pre-log factor* of 1/2 for envelope sampling. Note that the constant penalty χ has canceled since it is also present in $I(\hat{R}_A;\hat{R}_B)$. As for the complex case, the lower bound is not restricted to be positive, in which case it is useless. The condition (7) for having a larger-than-zero lower bound, which was derived in the complex case, also applies here.

C. Conditional Mutual Information Between Alice and Bob

As shown in (9) in the complex case, to compute the conditional mutual information $I(\hat{R}_A;\hat{R}_B|\hat{R}_E)$, we need to evaluate the joint different entropy $h(\hat{R}_A,\hat{R}_B,\hat{R}_E)$. The following lemma gives the joint PDF of $(\hat{R}_A,\hat{R}_B,\hat{R}_E)$.

Lemma 5: The joint PDF of $(\hat{R}_A,\hat{R}_B,\hat{R}_E)$ *is given by (15), as shown at the bottom of the previous page, with the definition of the function* $G(\alpha_1,\alpha_2,\alpha_3)$

$$G(.) = \int_0^{2\pi}\int_0^{2\pi} \frac{e^{\alpha_1\cos(\phi_1)+\alpha_2\cos(\phi_2)+\alpha_3\cos(\phi_2-\phi_1)}}{(2\pi)^2} d\phi_1 d\phi_2.$$

Proof: The proof is given in Appendix VII-F. □

Here again, computing an analytical expression of the joint differential entropy of $(\hat{R}_A,\hat{R}_B,\hat{R}_E)$ is intricate. However, it can be evaluated numerically,[3] so that $I(\hat{R}_A;\hat{R}_B|\hat{R}_E)$ and thus (12) can be computed.

V. NUMERICAL ANALYSIS

This section aims at numerically analyzing the analytical results presented in previous sections. The following figures plot the lower bound (LB) and the upper bound (UB) on C_s^{Cplex} and C_s^{Evlpe}. For the envelope case, most of the information theoretic quantities could not be evaluated analytically. We evaluate them by numerical integration instead. We also compare some of them to the high SNR approximations that we derived and where simple analytical expressions were obtained. We will show many cases where the bounds become tight, as foreseen by the results of Sections III and IV. The mutual information quantities $I(\hat{H}_A;\hat{H}_B)$ and $I(\hat{R}_A;\hat{R}_B)$ are also plotted for comparison, as they correspond to the secret-key capacity in the case of uncorrelated observations at Eve, *i.e.*, $C_s^{\text{Cplex}} = I(\hat{H}_A;\hat{H}_B)$ and $C_s^{\text{Evlpe}} = I(\hat{R}_A;\hat{R}_B)$ for $\rho = 0$. They can also be seen as another UB, looser than $I(\hat{H}_A;\hat{H}_B|\hat{H}_E)$ and $I(\hat{R}_A;\hat{R}_B|\hat{R}_E)$.

A. Impact of SNR

In Fig. 2, the impact of the SNR on C_s^{Cplex} and C_s^{Evlpe} is studied. The SNR is defined as $\text{SNR} = p/\sigma_A^2 = p/\sigma_B^2 = p/\sigma_E^2$. A first observation is the large performance gain of complex sampling versus envelope sampling. This graph gives a quantitative criterion to better assess the trade-off full CSI versus RSS. The full CSI approach achieves higher secret-key rates at the price of stringent practical requirements. On the other hand, the RSS approach achieves lower key rates but is much more practical to implement.

Focusing first on the uncorrelated case ($I(\hat{H}_A;\hat{H}_B)$ and $I(\hat{R}_A;\hat{R}_B)$), two penalties of envelope sampling in the high SNR regime were identified in Table I: i) a *pre-log factor* of $1/2$ inducing a smaller slope as a function of SNR and ii) a

[3]For instance, by discretization and truncation of $f_{\hat{R}_A,\hat{R}_B,\hat{R}_E}(\hat{r}_A,\hat{r}_B,\hat{r}_E)$ and replacing the integral by a Riemann sum.

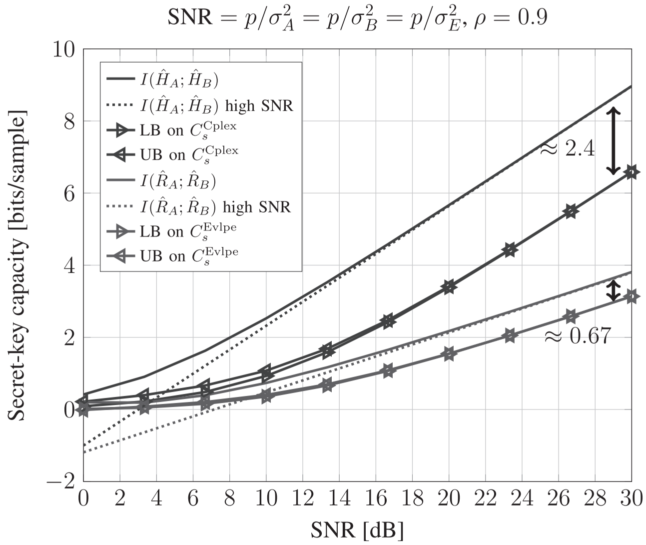


Fig. 2. Secret-key capacity for complex channel sampling versus envelope sampling as a function of SNR.

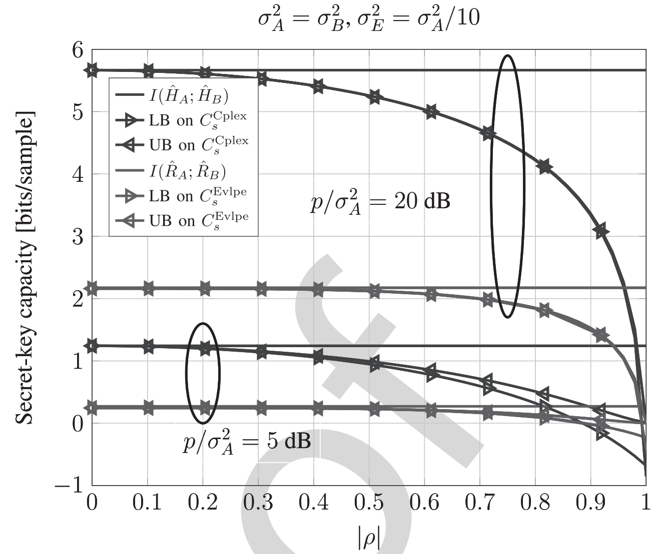


Fig. 3. Secret-key capacity for complex channel sampling versus envelope sampling as a function of correlation coefficient magnitude $|\rho|$.

constant penalty of χ bit, inducing a translation of the curve downwards of about 0.69 bit.

In the correlated case ($\rho = 0.9$), C_s^{Cplex} and C_s^{Evlpe} are reduced given the knowledge Eve has gained from her channel observations. As foreseen by Prop. 1, the bounds on C_s^{Cplex} become tight as the SNR grows large and a constant penalty of $\log_2(1 - |\rho|^2) \approx -2.4$ bits is observed as compared to the uncorrelated case. Interestingly, the bounds become tight for C_s^{Evlpe}, even for smaller values of SNR. The gap as compared to the uncorrelated case can be approximated from Table I as $\frac{1}{2}\log_2(1 - |\rho|^2) + \chi \approx -0.51$ bits. The inaccuracy with the simulated gap of -0.67 bit comes from the fact that the LB on C_s^{Evlpe} in Table I only asymptotically holds for $|\rho| \to 1$.

B. Impact of Correlation

In Fig. 3, the impact of the correlation coefficient magnitude $|\rho|$ is studied,[4] for two SNR regimes. We here consider an identical noise variance at Alice and Bob, while Eve uses a more powerful receiver so that $\sigma_A^2 = \sigma_B^2$ and $\sigma_E^2 = \sigma_A^2/10$.

One can see that, as $|\rho| \to 0$, the LB and UB become tight and converge to the mutual information between Alice's and Bob's observations. For larger values of $|\rho|$, bounds are less tight, especially in the complex case. As foreseen by Prop. 1, for a same value of $|\rho| < 1$, the LB and UB become tight for large SNR values. As already discussed in the context of equation (7), the LBs on the secret-key capacity are not restricted to be positive. This case is observed in Fig. 3 for large values of $|\rho|$. Note that this case arises here given the reduced noise power at Eve $\sigma_E^2 = \sigma_A^2/10$. In practice, the secret-key capacity cannot be lower than zero. We chose not to put negative values of the LB to zero, as it provides some physical insights on the problem.

[4]From previous analytical studies, it was shown that C_s^{Cplex} and C_s^{Evlpe} only depend on the magnitude of the correlation coefficient and not on its phase.

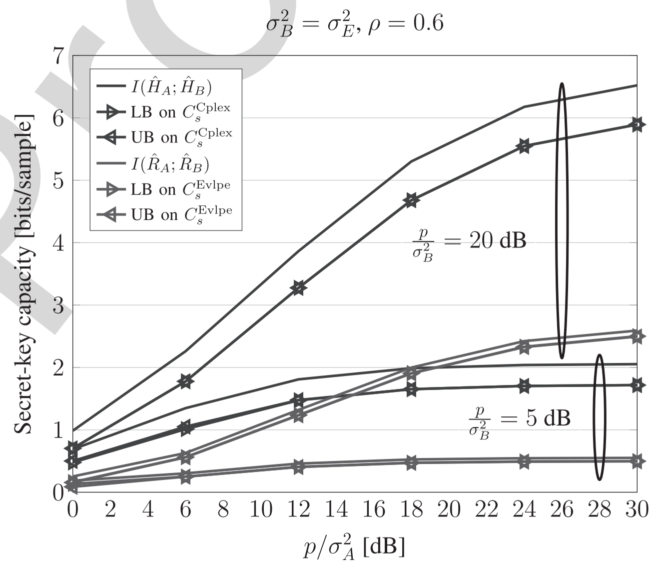


Fig. 4. Impact of a different noise variance at Alice and Bob.

C. Impact of Different Noise Variances at Alice and Bob

In Fig. 4, the impact of a different noise variance at Alice and Bob is studied. More specifically, the SNRs at Bob and Eve are kept identical, *i.e.*, $p/\sigma_B^2 = p/\sigma_E^2$, for two SNR regimes (5 dB and 20 dB). On the other hand, the SNR at Alice p/σ_A^2 is varied from 0 to 30 dB. The correlation coefficient is set to $\rho = 0.6$.

As foreseen in Sections III and IV, the LB and UB bounds become tight as $\sigma_A^2 \to 0$ for a fixed value of σ_B^2. Moreover, as p/σ_A^2 grows large, C_s^{Cplex} and C_s^{Evlpe} saturate at a plateau. This can be explained by the fact that they enter a regime limited by the fixed noise variance at Bob σ_B^2.

D. Impact of Different Noise Variance at Eve

In Fig. 5, the impact of a different noise variance at Eve is studied. More specifically, the SNRs at Alice and Bob are kept

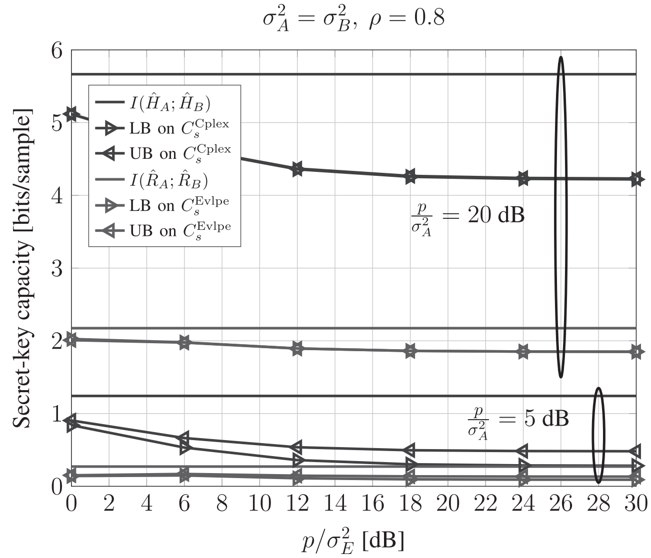


Fig. 5. Impact of a different noise variance at Eve.

identical, *i.e.*, $p/\sigma_A^2 = p/\sigma_B^2$, for two SNR regimes (5 dB and 20 dB). On the other hand, the SNR at Eve p/σ_E^2 is varied from 0 to 30 dB. The correlation coefficient is set to $\rho = 0.8$.

According to Prop. 1, the LB and UB are tight in the high SNR regime. Moreover, as p/σ_E^2 grows large, C_s^{Cplex} and C_s^{Evlpe} decrease up to a certain floor. This can be explained by the fact that Eve performance is not limited by σ_E^2 but by the fixed value of the correlation coefficient ρ.

VI. Conclusion

In this article, we have compared the secret-key capacity based on the sampling process of the entire CSI or only its envelope or RSS, taking into account correlation of Eve's observations. We have evaluated lower and upper bounds on the secret-key capacity. In the complex case, we obtain simple closed-form expressions. In the envelope case, the bounds must be evaluated numerically. In a number of particular cases, the lower and upper bounds become tight: low correlation of the eavesdropper, relatively smaller noise variance at Bob than Alice (or vice versa) and specific high SNR regimes. Finally, we have shown that, in the high SNR regime, the bounds can be evaluated in closed-form and result in simple expressions, which highlight the gain of CSI-based systems. The penalty of envelope-based versus complex-based secret-key generation is: i) a *pre-log* factor of $1/2$ instead of 1, implying a lower slope of the secret-key capacity as a function of SNR and ii) a constant penalty of about 0.69 bit, which disappears as Eve's channel gets highly correlated.

VII. Appendix

A. Upper Bound of Complex Sampling-Based Secret-Key Capacity

We need to show that $I(\hat{H}_A;\hat{H}_B|\hat{H}_E) \leq I(\hat{H}_A;\hat{H}_B)$, which is equivalent to showing that

$$0 \geq I(\hat{H}_A;\hat{H}_B|\hat{H}_E) - I(\hat{H}_A;\hat{H}_B),$$

or

$$1 \geq \frac{|\mathbf{C}_{\hat{H}_A\hat{H}_E}||\mathbf{C}_{\hat{H}_B\hat{H}_E}||\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{(p+\sigma_A^2)(p+\sigma_B^2)(p+\sigma_E^2)|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}$$

$$0 \geq \frac{|\mathbf{C}_{\hat{H}_A\hat{H}_E}||\mathbf{C}_{\hat{H}_B\hat{H}_E}||\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{(p+\sigma_A^2)(p+\sigma_B^2)(p+\sigma_E^2)} - |\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|.$$

After computing the expression of each determinant and several simplifications, we obtain

$$\begin{aligned}
&\frac{|\mathbf{C}_{\hat{H}_A\hat{H}_E}||\mathbf{C}_{\hat{H}_B\hat{H}_E}||\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{(p+\sigma_A^2)(p+\sigma_B^2)(p+\sigma_E^2)} - |\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}| \\
&\quad = -|\rho|^2 2p^3 + \frac{|\rho p|^4}{p+\sigma_E^2} + |\rho|^2 p^4 \left(\frac{1}{p+\sigma_A^2} + \frac{1}{p+\sigma_B^2}\right) \\
&\qquad - \frac{|\rho|^4\ p^6}{(p+\sigma_A^2)(p+\sigma_B^2)(p+\sigma_E^2)}.
\end{aligned}$$

We still need to prove that this quantity is smaller or equal to zero. We can first simplify the inequality by dividing by $|\rho|^2 p^3$. We then need to show that

$$\begin{aligned}
0 \geq &-2 + \frac{1}{1+\sigma_A^2/p} + \frac{1}{1+\sigma_B^2/p} \\
&+ |\rho|^2 \frac{1}{1+\sigma_E^2/p}\left(1 - \frac{1}{(1+\sigma_A^2/p)(1+\sigma_B^2/p)}\right).
\end{aligned}$$

It is easy to see that the term on the right is maximized for $\sigma_E^2 = 0$ and $|\rho| = 1$ ($|\rho| \leq 1$ by definition). It is then sufficient to focus on that critical case and in particular to show that

$$\begin{aligned}
1 &\geq \frac{1}{1+\sigma_A^2/p} + \frac{1}{1+\sigma_B^2/p} - \frac{1}{(1+\sigma_A^2/p)(1+\sigma_B^2/p)} \\
&= \frac{1+\sigma_A^2/p+\sigma_B^2/p}{1+\sigma_A^2/p+\sigma_B^2/p+\sigma_A^2\sigma_B^2/p^2},
\end{aligned}$$

which is always smaller or equal to one given that σ_A^2, σ_B^2 and σ_E^2 and p are positive by definition.

B. Proof of (In)Dependence of Random Variables in Propositions 2 and 3

This section derives a set of results on the dependence of random variables, required in the proofs of Propositions 2 and 3. Note that, in the following sections, we conduct all the proofs considering Alice case. However, they can be straightforwardly extended to Bob's case by replacing subscript A by B in all of the following expressions.

A starting point is to write the PDF of the channel observations at Alice and Eve. We know that $\hat{H}_A$ and $\hat{H}_E$ follow a ZMCSG with covariance matrix $\mathbf{C}_{\hat{H}_A\hat{H}_E}$, which gives

$$f_{\hat{H}_A,\hat{H}_E}(\hat{h}_A,\hat{h}_E) = \frac{e^{-\frac{|\hat{h}_A|^2(p+\sigma_E^2)+|\hat{h}_E|^2(p+\sigma_A^2)-2p\Re(\rho^*\hat{h}_A\hat{h}_E^*)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}}{\pi^2|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}.$$

We can express this PDF in polar coordinates using the change of variables $\hat{H}_A = \hat{R}_A\exp(\jmath\hat{\Phi}_A)$, $\hat{H}_E = \hat{R}_E\exp(\jmath\hat{\Phi}_E)$. Doing this, we obtain the joint PDF

$$\begin{aligned}
&f_{\hat{R}_A,\hat{\Phi}_A,\hat{R}_E,\hat{\Phi}_E}(\hat{r}_A,\hat{\phi}_A,\hat{r}_E,\hat{\phi}_E) \\
&\quad = \frac{\hat{r}_A\hat{r}_E e^{-\frac{\hat{r}_A^2(p+\sigma_E^2)+\hat{r}_E^2(p+\sigma_A^2)-2p\hat{r}_A\hat{r}_E|\rho|\cos(\hat{\phi}_A-\hat{\phi}_E-\angle\rho)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}}{\pi^2|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}. \quad (21)
\end{aligned}$$

We now prove each of the results, relying on (21). Firstly, the random vector $(\hat{\Phi}_A, \hat{\Phi}_E)$ is not independent from $(\hat{R}_A, \hat{R}_E)$, if $|\rho| > 0$. Indeed, by simple inspection of (21), we can see that $f_{\hat{R}_A,\hat{\Phi}_A,\hat{R}_E,\hat{\Phi}_E}(\hat{r}_A, \hat{\phi}_A, \hat{r}_E, \hat{\phi}_E) \neq f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) f_{\hat{\Phi}_A,\hat{\Phi}_E}(\hat{\phi}_A, \hat{\phi}_E)$. The same result holds for $(\hat{\Phi}_A, \hat{\Phi}_B)$ and $(\hat{R}_A, \hat{R}_B)$, as a particularization to the case $\rho = 1$ and replacing subscripts E by B.

Secondly, $\hat{\Phi}_E$ and $(\hat{R}_A, \hat{R}_E)$ are independent. This can be shown by integrating (21) over $\hat{\phi}_A$ giving

$$\begin{aligned} &f_{\hat{R}_A,\hat{R}_E,\hat{\Phi}_E}(\hat{r}_A, \hat{r}_E, \hat{\phi}_E) \\ &= \int_0^{2\pi} f_{\hat{R}_A,\hat{\Phi}_A,\hat{R}_E,\hat{\Phi}_E}(\ldots) d\hat{\phi}_A \\ &= \frac{2\hat{r}_A\hat{r}_E}{\pi|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} I_0\left(\frac{2p|\rho|\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) e^{-\frac{\hat{r}_A^2(p+\sigma_E^2)+\hat{r}_E^2(p+\sigma_A^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}, \quad (22) \end{aligned}$$

where $I_0(.)$ is the zero order modified Bessel function of the first kind. Since the phase $\hat{\phi}_E$ does not appear, it implies that it is uniformly distributed and thus $f_{\hat{R}_A,\hat{R}_E,\hat{\Phi}_E}(\hat{r}_A, \hat{r}_E, \hat{\phi}_E) = f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) f_{\hat{\Phi}_E}(\hat{\phi}_E)$. The same result holds for $\hat{\Phi}_B$ and $(\hat{R}_A, \hat{R}_B)$, as a particularization to the case $\rho = 1$ and replacing subscripts E by B.

Thirdly, the envelope and the phase of a ZMCSG are independent. Take for instance the PDF of $\hat{H}_E$, which can be written in polar coordinates, using a change of variable $\hat{H}_E = \hat{R}_E \exp(\jmath\hat{\Phi}_E)$, as

$$f_{\hat{R}_E,\hat{\Phi}_E}(\hat{r}_E, \hat{\phi}_E) = \frac{\hat{r}_E}{\pi(p+\sigma_E^2)} e^{-\frac{\hat{r}_E^2}{p+\sigma_E^2}},$$

which shows that $f_{\hat{R}_E,\hat{\Phi}_E}(\hat{r}_E, \hat{\phi}_E) = f_{\hat{R}_E}(\hat{r}_E) f_{\hat{\Phi}_E}(\hat{\phi}_E)$, with $\hat{\Phi}_E$ uniformly distributed, implying independence. The same result holds for $\hat{H}_A$ and $\hat{H}_B$.

C. Proof of Lemma 3

The joint PDF $f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E)$ can be obtained by integrating (22) over $\hat{\phi}_E$, which gives

$$\begin{aligned} &f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) \\ &= \int_0^{2\pi} f_{\hat{R}_A,\hat{R}_E,\hat{\Phi}_E}(\hat{r}_A, \hat{r}_E, \hat{\phi}_E) d\hat{\phi}_E \\ &= \frac{4\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} I_0\left(\frac{2p|\rho|\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right) e^{-\frac{\hat{r}_A^2(p+\sigma_E^2)+\hat{r}_E^2(p+\sigma_A^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}, \quad (23) \end{aligned}$$

and leads to the result of Lemma 3.

D. Proof of Lemma 4

From Bessel function theory [46, Eq. 10.40.1], we know that, as $r \to +\infty$,

$$I_0(r) = \frac{e^r}{\sqrt{2\pi r}} + \epsilon_0, \ |\epsilon_0| = O\left(\frac{e^r}{r^{3/2}}\right). \quad (24)$$

In our case, we have

$$r = \frac{2p|\rho|\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} = \frac{2p|\rho|\hat{r}_A\hat{r}_E}{(1-|\rho|^2)p^2 + p(\sigma_E^2+\sigma_A^2) + \sigma_E^2\sigma_A^2}. \quad (25)$$

The Bessel asymptotic expansion is thus accurate when r becomes large. This is precisely the case as $\sigma_A^2 \to 0$, $\sigma_E^2 \to 0$ and $|\rho| \to 1$, for $\hat{r}_A > 0$ and $\hat{r}_E > 0$. Using the Bessel asymptotic expansion of $I_0(.)$ in (23), we get

$$\begin{aligned} f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) = \frac{2}{p}\sqrt{\frac{\hat{r}_A\hat{r}_E}{|\rho|}} e^{-\frac{\hat{r}_A^2\sigma_E^2+\hat{r}_E^2(\sigma_A^2+p(1-|\rho|^2))}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}} \\ \frac{1}{\sqrt{\pi|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}} e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}} + \epsilon_1, \quad (26) \end{aligned}$$

where ϵ_1 is the approximation error

$$\epsilon_1 = \frac{4\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} \exp\left(-\frac{\hat{r}_A^2(p+\sigma_E^2)+\hat{r}_E^2(p+\sigma_A^2)}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}\right)\epsilon_0.$$

Note that, in the particular cases $\hat{r}_A = 0$ or $\hat{r}_E = 0$, $\epsilon_1 = 0$ since (26) = (23) = 0. Using (24) and the definition of r in (25), we can bound the error ϵ_1 as follows

$$\begin{aligned} |\epsilon_1| &= O\left(\frac{\left(|\mathbf{C}_{\hat{H}_A\hat{H}_E}|\right)^{1/2} e^{-\frac{\hat{r}_A^2\left(p+\sigma_E^2\right)+\hat{r}_E^2\left(p+\sigma_A^2\right)-2p|\rho|\hat{r}_A\hat{r}_E}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}}{(p|\rho|)^{3/2}\left(\hat{r}_A\hat{r}_E\right)^{1/2}}\right) \\ &= O\left(\sqrt{1-|\rho|^2+\sigma_A^2+\sigma_E^2}\right), \end{aligned}$$

where we used the fact that the exponential can be bounded in the asymptotic regime by an independent constant. The second exponential term of (26) suggests the following approximation $\hat{r}_A \approx |\rho|\hat{r}_E$. We thus obtain

$$\begin{aligned} f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A, \hat{r}_E) = \frac{2\hat{r}_E e^{-\hat{r}_E^2\frac{p(1-|\rho|^2)+|\rho|^2\sigma_E^2+\sigma_A^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}} e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}}}{p\sqrt{\pi|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}} \\ +\epsilon_1+\epsilon_2, \quad (27) \end{aligned}$$

where ϵ_2 is the approximation error related to this second approximation

$$\begin{aligned} \epsilon_2 = \frac{2}{p}\frac{e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}}}{\sqrt{\pi|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}}\left(\sqrt{\frac{\hat{r}_A\hat{r}_E}{|\rho|}} e^{-\frac{\hat{r}_A^2\sigma_E^2+\hat{r}_E^2(\sigma_A^2+p(1-|\rho|^2))}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}\right. \\ \left. -\hat{r}_E e^{-\hat{r}_E^2\frac{p(1-|\rho|^2)+|\rho|^2\sigma_E^2+\sigma_A^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}}\right). \end{aligned}$$

When $\hat{r}_A = |\rho|\hat{r}_E$, the term in parenthesis is exactly zero and so $\epsilon_2 = 0$. In other cases, it can be bounded by an independent constant as $\sigma_A^2 \to 0$, $\sigma_E^2 \to 0$ and $|\rho| \to 1$, giving

$$|\epsilon_2| = O\left(\frac{e^{-\frac{\beta}{(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}}}{\sqrt{1-|\rho|^2+\sigma_A^2+\sigma_E^2}}\right),$$

where β is some real strictly positive constant. Moreover, we can still simplify (27) by performing the two following approximations $|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p \approx p(1-|\rho|^2) + \sigma_A^2 + \sigma_E^2$ and

$\frac{p(1-|\rho|^2)+|\rho|^2\sigma_E^2+\sigma_A^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|} \approx 1/p$ so that we get

$$\begin{aligned} f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E) = & \frac{2\hat{r}_E e^{-\frac{\hat{r}_E^2}{p}}}{p} \frac{e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}}}{\sqrt{\pi(p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2)}} \\ & +\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4, \end{aligned}$$

which gives the asymptotic distribution of Lemma 4 and where ϵ_3 and ϵ_4 are the approximation errors related to the approximations

$$\begin{aligned} \epsilon_3 = & \frac{2\hat{r}_E}{p\sqrt{\pi|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}} \left(e^{-\hat{r}_E^2\frac{p(1-|\rho|^2)+|\rho|^2\sigma_E^2+\sigma_A^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}-\frac{p(\hat{r}_A-|\rho|\hat{r}_E)^2}{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|}} \right. \\ & \left. -e^{-\frac{\hat{r}_E^2}{p}} e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}} \right) \\ \epsilon_4 = & \frac{2\hat{r}_E e^{-\frac{\hat{r}_E^2}{p}} e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}}}{p\sqrt{\pi}} \left(\frac{1}{\sqrt{|\mathbf{C}_{\hat{H}_A\hat{H}_E}|/p}} \right. \\ & \left. -\frac{1}{\sqrt{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}} \right). \end{aligned}$$

To bound ϵ_3 and ϵ_4, we can use a first order Taylor expansion of the exponential and the inverse of a square root respectively. We find

$$\begin{aligned} |\epsilon_3| &= O\left(\frac{(1-|\rho|^2)\sigma_E^2+\sigma_A^2\sigma_E^2}{(1-|\rho|^2+\sigma_A^2+\sigma_E^2)^{3/2}}\right) \\ |\epsilon_4| &= O\left(\frac{\sigma_A^2+\sigma_E^2}{\sqrt{1-|\rho|^2+\sigma_A^2+\sigma_E^2}}\right). \end{aligned}$$

Finally, combining the bounds on the approximation errors $\epsilon_1,\epsilon_2,\epsilon_3$ and ϵ_4, we find that the total approximation error can be bounded as

$$|\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4| = O\left(\sqrt{1-|\rho|^2+\sigma_A^2}\right),$$

where we used (**As2**). This completes the proof.

E. Proof of Theorem 2

Let us define the asymptotic PDF of $f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E)$ as

$$f^{\text{High}}_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E) = \frac{2\hat{r}_E e^{-\frac{\hat{r}_E^2}{p}}}{p} \frac{e^{-\frac{(\hat{r}_A-|\rho|\hat{r}_E)^2}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}}}{\sqrt{\pi(p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2)}}.$$

We can see that the PDF factorizes as $f^{\text{High}}_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E) = f_1(\hat{r}_E)f_2(\hat{r}_A|\hat{r}_E)$. We can identify $f_1(\hat{r}_E)$ to be a Rayleigh distribution with parameter $\frac{p}{2}$, while the conditional PDF $f_2(\hat{r}_A|\hat{r}_E)$ is a normal centered in $|\rho|\hat{r}_E$ and of variance $(p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2)/2$.

Results such as [47, Th. 1] can be used to prove that, for a sequence of PDFs such that $f_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E) \to f^{\text{High}}_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E)$ pointwise, their differential entropy also converges provided that: i) their second order moments are bounded from above and ii) their PDF is bounded from above. These two conditions are satisfied in our case as long as p, σ_A^2 and σ_E^2 are bounded from above, which makes practical sense. In the pathological case $\sigma_A^2=0$, $\sigma_E^2=0$ or $|\rho|=1$, $|\mathbf{C}_{\hat{H}_A\hat{H}_E}|=0$ and the PDFs are unbounded, which makes practical sense since $h(\hat{R}_A,\hat{R}_E)\to-\infty$. Unfortunately, finding the analytical rate of convergence of the differential entropy is intricate.

All of the following expressions should be understood in the asymptotic sense as $\sigma_A^2\to 0$ and $\sigma_E^2\to 0$ and $|\rho|\to 1$. Using the chain rule for the differential entropy $h(X,Y)=h(X)+h(Y|X)$, the general expression of the differential entropies of Rayleigh and normal distributions, the joint differential entropy of the distribution $f^{\text{High}}_{\hat{R}_A,\hat{R}_E}(\hat{r}_A,\hat{r}_E)$ can be easily computed and we find

$$\begin{aligned} h(\hat{R}_A,\hat{R}_E) \to & \frac{1}{2}\log_2\left(p^2(1-|\rho|^2)+p(\sigma_A^2+\sigma_E^2)\right) \\ & +\frac{1}{2}\log_2\left(\frac{\pi e^{3+\gamma}}{4}\right). \end{aligned}$$

Inserting this expression in (19), together with the expressions of $h(\hat{R}_A)$ and $h(\hat{R}_E)$ given in (17) and (20) respectively, we finally obtain

$$\begin{aligned} I(\hat{R}_A;\hat{R}_E) &\to \frac{1}{2}\log_2\left(\frac{(p+\sigma_A^2)(p+\sigma_E^2)}{p^2(1-|\rho|^2)+p(\sigma_A^2+\sigma_E^2)}\right)+\chi \\ &\to \frac{1}{2}\log_2\left(\frac{p}{p(1-|\rho|^2)+\sigma_A^2+\sigma_E^2}\right)+\chi, \end{aligned}$$

with the definition of χ introduced in Theorem 1, which concludes the proof.

F. Proof of Lemma 5

We know that $\hat{H}_A$, $\hat{H}_B$ and $\hat{H}_E$ follow a ZMCSG with covariance matrix $\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}$, which gives

$$\begin{aligned} & f_{\hat{H}_A,\hat{H}_B,\hat{H}_E}(\hat{h}_A,\hat{h}_B,\hat{h}_E) \\ & = \frac{e^{\frac{2p(p(1-|\rho|^2)+\sigma_E^2)\hat{h}_A\hat{h}_B^*+2\ p\sigma_B^2\Re(\hat{h}_A\rho^*\hat{h}_E^*)+2\ p\sigma_A^2\Re(\hat{h}_B\rho^*\hat{h}_E^*)}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}}}{\pi^3|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|} \\ & \quad e^{-\frac{|\hat{h}_A|^2|\mathbf{C}_{\hat{H}_B\hat{H}_E}|+|\hat{h}_B|^2|\mathbf{C}_{\hat{H}_A\hat{H}_E}|+|\hat{h}_E|^2|\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}}. \end{aligned}$$

This PDF can be expressed in polar coordinates as

$$\begin{aligned} & f_{\hat{R}_A,\hat{R}_B,\hat{R}_E,\hat{\Phi}_A,\hat{\Phi}_B,\hat{\Phi}_E}(\hat{r}_A,\hat{r}_B,\hat{r}_E,\hat{\phi}_A,\hat{\phi}_B,\hat{\phi}_E) \\ & = \frac{\hat{r}_A\hat{r}_B\hat{r}_E}{\pi^3|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|} e^{-\frac{\hat{r}_A^2|\mathbf{C}_{\hat{H}_B\hat{H}_E}|+\hat{r}_B^2|\mathbf{C}_{\hat{H}_A\hat{H}_E}|+\hat{r}_E^2|\mathbf{C}_{\hat{H}_A\hat{H}_B}|}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}} \\ & \quad e^{\frac{2p(p(1-|\rho|^2)+\sigma_E^2)\hat{r}_A\hat{r}_B\cos(\hat{\phi}_A-\hat{\phi}_B)}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}} e^{\frac{2p\sigma_B^2\hat{r}_A\hat{r}_E|\rho|\cos(\hat{\phi}_A-\hat{\phi}_E-\angle\rho)}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}} \\ & \quad e^{\frac{2p\sigma_A^2\hat{r}_B\hat{r}_E|\rho|\cos(\hat{\phi}_B-\hat{\phi}_E-\angle\rho)}{|\mathbf{C}_{\hat{H}_A\hat{H}_B\hat{H}_E}|}}. \end{aligned} \tag{28}$$

The joint PDF $f_{\hat{R}_A,\hat{R}_B,\hat{R}_E}(\hat{r}_A,\hat{r}_B,\hat{r}_E)$ can be obtained by integrating (28) over the phases $\hat{\phi}_A$, $\hat{\phi}_B$ and $\hat{\phi}_E$, which leads to the result of Lemma 5. Indeed the first two terms do not depend on the phases, so that they can be put out of the integrals. The third term however does. One can easily see that the phase of ρ does not impact the result, so that it can be removed. One can further notice that the cosines do not depend on the absolute phases $\hat{\phi}_A,\hat{\phi}_B,\hat{\phi}_E$ but on their differences.

Making a change of variable $\phi_1 = \hat{\phi}_A - \hat{\phi}_B$, $\phi_2 = \hat{\phi}_A - \hat{\phi}_E$, we see that the last difference is $\hat{\phi}_B - \hat{\phi}_E = \phi_2 - \phi_1$. Hence, one integral simplifies.

References

[1] F. Rottenberg, P. De Doncker, F. Horlin, and J. Louveaux, "Impact of realistic propagation conditions on reciprocity-based secret-key capacity," in *Proc. IEEE 31st Annu. Int. Symp. Pers., Indoor Mobile Radio Commun.*, Aug. 2020, pp. 1–6.

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[5] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[7] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[8] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[9] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proc. IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct. 2015.

[10] 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.

[11] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key generation using correlated sources and channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 652–670, Feb. 2012.

[12] G. Bassi, P. Piantanida, and S. Shamai (Shitz), "The secret key capacity of a class of noisy channels with correlated sources," *Entropy*, vol. 21, no. 8, p. 732, Jul. 2019.

[13] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 401–410, doi: 10.1145/1315245.1315295.

[14] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw.*, 2009, p. 321, doi: 10.1145/1614320.1614356.

[15] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[16] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[17] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proc. 4th Eur. Workshop Syst. Secur.*, 2011, doi: 10.1145/1972551.1972559.

[18] R. Guillaume, F. Winzer, A. Czylwik, C. T. Zenger, and C. Paar, "Bringing PHY-based key generation into the field: An evaluation for practical scenarios," in *Proc. IEEE 82nd Veh. Technol. Conf.*, Sep. 2015, pp. 1–5.

[19] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, "The passive eavesdropper affects my channel: Secret-key rates under real-world conditions," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–6.

[20] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.

[21] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[22] M. Jacovic, M. Kraus, G. Mainland, and K. R. Dandekar, "Evaluation of physical layer secret key generation for IoT devices," in *Proc. IEEE 20th Wireless Microw. Technol. Conf. (WAMICON)*, Apr. 2019, pp. 1–6.

[23] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 2593–2597.

[24] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[25] T. F. Wong, M. Bloch, and J. M. Shea, "Secret sharing over fast-fading MIMO wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, Dec. 2009, Art. no. 506973.

[26] J. W. Wal and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[27] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.

[28] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret key generation from reciprocal spatially correlated MIMO channels," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2013, pp. 1245–1250.

[29] B. T. Quist and M. A. Jensen, "Optimal channel estimation in beamformed systems for common-randomness-based secret key establishment," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1211–1220, Jul. 2013.

[30] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[31] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 3048–3056.

[32] X. Wu, Y. Peng, C. Hu, H. Zhao, and L. Shu, "A secret key generation method based on CSI in OFDM-FDD system," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2013, pp. 1297–1302.

[33] J. Zhang, M. Ding, D. Lopez-Perez, A. Marshall, and L. Hanzo, "Design of an efficient OFDMA-based multi-user key generation protocol," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8842–8852, Sep. 2019.

[34] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "An efficient OFDM-based encryption scheme using a dynamic key approach," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 361–378, Feb. 2019.

[35] J. Zhang *et al.*, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[36] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, Sep. 2008, pp. 128–139, doi: 10.1145/1409944.1409960.

[37] M. Ghoreishi Madiseh, S. He, M. L. Mcguire, S. W. Neville, and X. Dong, "Verification of secret key generation from UWB channel observations," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–5.

[38] T.-H. Chou, S. C. Draper, and A. M. Sayeed, "Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2518–2522.

[39] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. 3rd Eur. Conf. Antennas Propag.*, Mar. 2009, pp. 1499–1503.

[40] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, Apr. 2017.

[41] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "Experimental aspects of secret key generation in indoor wireless environments," in *Proc. IEEE 14th Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2013, pp. 669–673.

[42] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "The effect of Eavesdropper's statistics in experimental wireless secret-key generation," 2013, *arXiv:1312.3304*. [Online]. Available: http://arxiv.org/abs/1312.3304

[43] G. D. Durgin, *Space-Time Wireless Channels*. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[44] B. Sklar, "Rayleigh fading channels in mobile digital communication systems.I. Characterization," *IEEE Commun. Mag.*, vol. 35, pp. 90–100, Jul. 1997.

[45] J. V. Michalowicz, J. M. Nichols, and F. Bucholtz, *Handbook of Differential Entropy*. Boca Raton, FL, USA: CRC Press, 2013.

[46] *NIST Digital Library of Mathematical Functions*. W. J. Olver *et al.*, Eds. 2020. http://dlmf.nist.gov/

[47] M. Godavarti and A. Hero, "Convergence of differential entropies," *IEEE Trans. Inf. Theory*, vol. 50, no. 1, pp. 171–176, Jan. 2004.

François Rottenberg (Member, IEEE) received the M.Sc. degree in electrical engineering from the Université Catholique de Louvain (UCLouvain), Louvain-la-Neuve, in 2014, and the Ph.D. degree jointly from UCLouvain and the Université Libre de Bruxelles (ULB), Brussels, in 2018. From September 2018 to August 2019, he was a Post-Doctoral Researcher with the University of Southern California (USC), Los Angeles, USA, leading the 5G massive MIMO research efforts. He is currently a Post-Doctoral Researcher affiliated with UCLouvain and ULB, funded by the Belgian National Science Foundation (FRS-FNRS). He participated to various national, European, and international projects. Since 2015, he has been a Regular Visitor and a Collaborator with the Centre Tecnològic Telecomunicacions Catalunya (CTTC), Castelldefels, Spain, and the National Institute of Information and Communications Technology (NICT), Tokyo, Japan. His main research interests include signal processing for next generations of communication systems, including novel modulation formats, multi-antenna systems, and physical-layer security.

Trung-Hien Nguyen (Member, IEEE) received the B.Sc. degree in electronics and telecommunications from the Hanoi Posts and Telecommunications Institute of Technology (PTIT), Vietnam, in 2010, and the Ph.D. degree in physics from the University of Rennes 1, France, in 2015. Since December 2015, he has been a Post-Doctoral Researcher with the OPERA Department, Université Libre de Bruxelles (ULB), Belgium. His research interests include optical fiber communication systems and localization based on 5G signals.

Jean-Michel Dricot (Member, IEEE) received the Ph.D. degree in network engineering with a focus on wireless sensor networks protocols and architectures. He leads research on network security with a specific focus on the Internet of Things (IoT) and wireless networks. He teaches communication networks, mobile networks, the Internet of Things, and network security. After his Ph.D. degree, he joined France Telecom Research and Development (Orange Labs), Grenoble, France, as a Research Engineer. He started there a project aiming at securing lightweight communication protocols, with a specific focus on wireless smart meters and body area networks. Next, he moved back to the Machine Learning Group, ULB, where he worked on the IoT-based localization techniques. In 2010, he was appointed as a Professor with the Université Libre de Bruxelles, with a tenure in mobile and wireless networks. He is the author or a coauthor of more than 100 papers published in peer-reviewed international journals and conferences. He served as a reviewer for European projects.

François Horlin (Member, IEEE) received the Ph.D. degree from the Université Catholique de Louvain (UCL) in 2002. He specialized in the field of signal processing for digital communications. After his Ph.D. degree, he joined the Inter-University Micro-Electronics Center (IMEC). He led the project aiming at developing a 4G cellular communication system in collaboration with Samsung Korea. In 2007, he became a Professor with the Université Libre de Bruxelles (ULB). He is currently supervising a Research Team working on next-generation communication systems. His current research interests include localization based on 5G signals, filterbank-based modulations, massive MIMO, and passive radars. He has been an Academic Representative to the executive board of ULB from 2010 to 2015. Since 2017, he has been the Vice Dean for research at the Ecole Polytechnique de Bruxelles (EPB).

Jérôme Louveaux (Member, IEEE) received the Electrical Engineering degree and the Ph.D. degree from the Université Catholique de Louvain (UCL), Louvain-la-Neuve, Belgium, in 1996 and 2000, respectively. From 2000 to 2001, he was a Visiting Scholar with the Electrical Engineering Department, Stanford University, CA, USA. From 2004 to 2005, he was a Post-Doctoral Researcher with the Delft University of Technology, The Netherlands. Since 2006, he has been a Professor with the ICTEAM Institute, UCL. His research interests include signal processing for digital communications, and in particular: multicarrier modulations, xDSL systems, resource allocation, synchronization, and estimation. He was a co-recipient of the Prix biennal Siemens 2000 for a contribution on filter-bank based multi-carrier transmission and the Prix Scientifique Alcatel 2005 for a contribution in the field of powerline communications.