entropy

MDPI

Article

Analysis of the Mutual Information of Channel Phase Observations in Line-of-Sight Scenarios

Maximilian Matthé [1,*] and Arsenia Chorti [1,2]

[1] Barkhausen Institut gGmbH, Würzburger Str. 46, 01187 Dresden, Germany; arsenia.chorti@ensea.fr
[2] ETIS UMR 8051, CY Paris University, ENSEA, CNRS, 95000 Cergy, France
* Correspondence: maximilian.matthe@barkhauseninstitut.org

Abstract: The mutual information of the observed channel phase between devices can serve as an entropy source for secret key generation in line-of-sight scenarios. However, so far only simulated and numeric results were available. This paper derives the probability distribution of the channel phase and corresponding expressions for the mutual information. Moreover, the orientation distribution is optimized in order to maximize the mutual information. All presented results are validated numerically. These outcomes serve as a basis for further analytic investigations on the secret key generation rate and subsequent physical layer security performance analysis in line-of-sight scenarios, such as those encountered in drone-aided communications.

Keywords: physical layer security; secret key generation; directional statistics; von-Mises distribution

Citation: Matthé, M.; Chorti, A. Analysis of the Mutual Information of Channel Phase Observations in Line-of-Sight Scenarios. *Entropy* **2023**, *25*, 1038. https://doi.org/10.3390/e25071038

Academic Editor: Ivan B. Djordjevic

Received: 1 June 2023
Revised: 29 June 2023
Accepted: 5 July 2023
Published: 10 July 2023

1. Introduction

Integrated ground–air–space global networks will rely heavily on the use of multi-hop wireless networking, e.g., using drones, in order to expand the performance and capabilities of future generations of wireless systems. In order to deliver the promised performance, various challenges need to be addressed, e.g., meeting aggressive latency requirements, enabling massive connectivity with low energy consumption and computational effort, jointly with the provision of explicit security guarantees. Another crucial concern arises from the widespread deployment of low-end Internet of Things (IoT) devices. These devices, often manufactured through non-uniform production processes and expected to remain operational for over 10 years, raise important questions about future security architectures. Furthermore, the extensive utilization of artificial intelligence (AI), machine learning (ML), and quantum computing advancements will increase the vulnerability of 6G systems to attacks.

Today's security architecture of connected devices mainly relies on public key infrastructure (PKI) [1] for authentication and key distribution. Such architecture has proven reliable and useful for a vast range of applications and has proven instrumental in securing both the core network as well as 5G networks incorporating TLS-based protocols. However, upcoming quantum computers are said to on one hand be able to break standard public key-encryption-based handshakes, while on the other hand post-quantum-based asymmetric cryptography can still be computationally expensive for simple, low-end IoT devices such as wireless sensors [2]. Hence, alternative methods for authentication and key distribution must be found.

Here, Physical layer security (PLS) can be a promising candidate to overcome this key distribution problem [3]. In particular, applying secret-key generation (SKG) algorithms that extract the keys from the shared physical channel between the communicating devices [4] presents a light-weight alternative to the complex logistics of PKI, especially when billions of small embedded IoT devices are deployed. In many 5G and 6G scenarios with wide-band communication, the dynamic frequency selectivity of the wireless channel

between the pairing devices can be used as a common source of entropy to generate a common secret key [5]. Unfortunately, in static line-of-sight (LOS) scenarios such as those encountered in drone-enabled multi-hop wireless networks, the wireless channels become frequency flat and less dynamic and hence another source of entropy needs to be found.

Despite these difficulties, the use of SKG in LOS conditions can be important for use cases such as drone communications and is motivated by many factors:

- Drones are expected to have widespread use in applications including surveillance, delivery services, and critical infrastructure inspections. These applications often involve the exchange of sensitive and often confidential data that need to be secure against unauthorized access. SKG emerges thus as a viable option for the ad hoc generation of secret keys between drones and critical infrastructure. These can be used in hybrid PLS-crypto systems to establish secure communication channels, ensuring that the transmitted information remains confidential and protected from eavesdropping, while respecting very strict delay constraints by avoiding conventional PKI-based key distribution.
- Secondly, drones operate in wireless environments that are susceptible to other types of malicious attacks, e.g., jamming, spoofing and tampering. Recent works on SKG robustness against such attacks provide the grounds for using such technologies in a trustworthy manner. We note in passing that jamming attacks have been analyzed in [6], tampering during pilot exchange in [7], spoofing during side information exchange in [8], while generalized channel probing has been covered in [9].
- Additionally, drones often operate in dynamic and unpredictable environments, making them vulnerable to both physical and cyber attacks. SKG provides an infrastructureless setting for enabling secure communications in such demanding scenarios.
- Moreover, SKG can lend itself to zero-touch solutions, especially when combined with location and RF-fingerprint-based authentication protocols. Protocols building on these PLS solutions have been proposed for fast authentication of IoT devices [8].

In summary, the use of SKG in drone communications can be instrumental to protect sensitive data, secure wireless communication channels, mitigate risks of physical and cyber attacks, and enable secure interactions within the IoT ecosystem. It can be used in hybrid PLS-crypto systems to ensure the confidentiality of the transmitted data, enhancing the overall security and reliability of drone operations.

Due to the frequency flatness in LOS scenarios, in [10] the authors proposed to use the phase shift of a LOS multiple-input multiple-output (MIMO) channel as the common randomness between devices. In particular, with small wave lengths, small fluctuations in the position of transmitting and receiving antennas can already have a large effect on the channel phase and hence serve as a source of entropy. Moreover, such small changes in the position are hardly visible to malicious observers and hence the channel phase cannot be predicted. The authors in [10] numerically analyzed the mutual information (MI) $I(A;B)$ between the pairing devices, Alice and Bob. Moreover, they also simulated the conditional MI between Alice and Bob given the observer, Eve, to understand the available key generation rate for a specific geometric constellation.

As the novelty, and in contrast to the work in [10] this paper provides analytic expressions for the MI between Alice and Bob given different counts of antennas and signal-to-noise ratios (SNRs). Analytic results are important in order to understand the underlying characteristics of a system and potentially allow to generalize results beyond scenarios that where simulated numerically. In particular, the results presented in this paper are valid for single- and dual-antenna systems and provide a theoretical reasoning on the behaviour of the MI for different SNRs at Alice and Bob. We show that the results match the numeric simulations. In particular, the contributions of this paper are three-fold:

- We analyze the properties of the noise of the channel phase and provide analytic expressions for the probability density function (PDF) of the channel phase under rotating antennas. Here, we build upon the system model from [10], but introduce a

geometric approximation in order to make the expressions mathematically tractable. The obtained PDF serves as a basis for the subsequent analysis of $I(A;B)$.
- We derive a tight upper-bound expression for the MI between Alice and Bob which is valid for different SNRs and antenna constellations. This is particularly novel, as the model under consideration has previously only been studied via numeric simulations.
- Using the derived analytic results we show that the orientation distribution of Alice and Bob can be optimized such that $I(A;B)$ reaches the provided upper bound. The obtained expression of the optimal rotation is a direct consequence of the previously derived expressions and is therefore a direct application of our results.

All results are verified with numeric simulations to corroborate their validity. The shown results can serve as a basis for subsequent performance analysis of LOS SKG algorithms in different scenarios, e.g., in drone-aided communications. The remainder of this paper is structured as follows. Section 2 describes the system model in terms of signal and geometry and derives the PDF for the channel phase between Alice and Bob. Analytic expressions for MI between Alice and Bob are derived in Section 3. Section 4 verifies the analytic results with numeric simulations. Finally, concluding remarks are provided in Section 5.

2. System Model

2.1. Signal Model

Consider the two-dimensional model in Figure 1. Alice is located at the origin and Bob's center is at position $\vec{d}$ and both have multiple antennas, at positions $\vec{a}_i$ and $\vec{b}_k$, respectively, where i,k are the antenna indices at Alice and Bob, respectively. From the geometry we see that $\vec{a}_i = r_A \mathbf{R}_{\alpha_i} \vec{e}$ and $\vec{b}_k = \vec{d} + r_B \mathbf{R}_{\beta_k} \vec{e}$, where α_i and β_k are the antenna rotations of the i-th and k-th antenna at Alice and Bob, $\mathbf{R}_\gamma$ is a rotation matrix that rotates around the angle γ, r_A, r_B are the antenna radius for Alice and Bob, respectively, and $\vec{e}$ is the unit vector pointing towards the right.

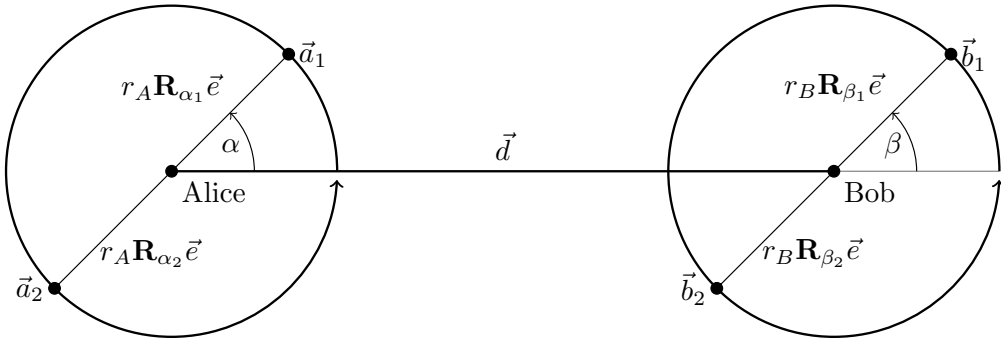

Figure 1. Geometry of the 2D setup.

Assuming that Alice sends a non-modulated carrier $x(t)$ from antenna i, the received signal $y_{ik}(t)$ at Bob's kth antenna is given by

$$x(t) = \exp(j2\pi f_c t) \tag{1}$$

$$y_{ik}(t) = \exp\left(j2\pi f_c \left(t - \frac{d_{ik}}{c}\right)\right) + \tilde{n}_{ik}(t) \tag{2}$$

$$= \exp(j2\pi f_c t)\exp(j\phi_{ik}) + \tilde{n}_{ik}(t) \tag{3}$$

where c is the speed of light, f_c is the carrier frequency and

$$d_{ik} = \|\vec{d} + \vec{b}_k - \vec{a}_i\| \tag{4}$$

is the distance between the ith and kth antenna and $\phi_{ik} = d_{ik}/c \bmod 2\pi$ is the phase of the channel between these antennas (Note that in reality, real-valued signals are transmitted

and received. However, for the mathematical presentation, the complex passband representation is more compact.). $\tilde{n}_{ik}(t)$ is AWGN. Letting Bob employ an ideally synchronized matched filter receiver which integrates the received signal over a period of the carrier frequency we have

$$y_{B,ik} = \int_0^{1/f_c} y_{B,ik}(t) \exp(-j2\pi f_c t) dt \tag{5}$$

$$= \tfrac{1}{f_c} \exp(j\phi_{ik}) + \tilde{n}_{B,ik} \tag{6}$$

There, $\tilde{n}_{B,ik}$ is once again complex AWGN with variance σ_B^2 since the integration happens over a full period of the carrier. Without loss of generality we assume $f_c = 1$ and hence we define the SNR at Bob by $\mathrm{SNR}_B = 1/\sigma_B^2$. A similar consideration can be performed for signals transmitted from Bob to Alice. In particular, we note that the phase between antennas i and k is reciprocal, meaning that the channel phase from Alice to Bob is equal to the phase from Bob to Alice.

Now, to estimate the phase of the channel, Bob takes the angle of the matched filter output, yielding

$$\hat{\phi}_{B,ik} = \arg(y_{B,ik}) = \phi_{ik} + n_{B,ik}, \tag{7}$$

where $n_{B,ik}$ is the measurement noise which is not Gaussian distributed anymore. Instead, (7) describes the phase of the non-zero mean complex Gaussian random variable $y_{B,ik} \sim \mathcal{CN}(e^{j\phi_{ik}}, \sigma_B^2)$. The distribution of this phase has been thoroughly analyzed in [11] and the authors have shown that for high SNR the distribution matches a Gaussian distribution as $n_{B,ik} \sim \mathcal{N}(0, \frac{\sigma^2}{2})$. In fact, for high SNR the periodic von-Mises distribution [12] $y_{B,ik} \sim \mathcal{M}(\kappa) = \frac{1}{2\pi I_0(\kappa)} \exp(\kappa \cos(\phi))$ with $\kappa = 2\sigma_B^{-2}$ matches as well and provides the avantageous property of being periodic with 2π. For lower SNR, both the Gaussian and the von-Mises distribution do not fully reflect the original distribution, however the von-Mises distribution better follows the longer tail of the actual distribution, see Figure 2 for an illustration. Therefore, in the sequel we assume $n_{B,ik}$ to be von-Mises distributed and we will point out the numerical consequences later on. Note that analogous considerations can be done for the measurements at Alice, yielding the same results, which we omit here for brevity.

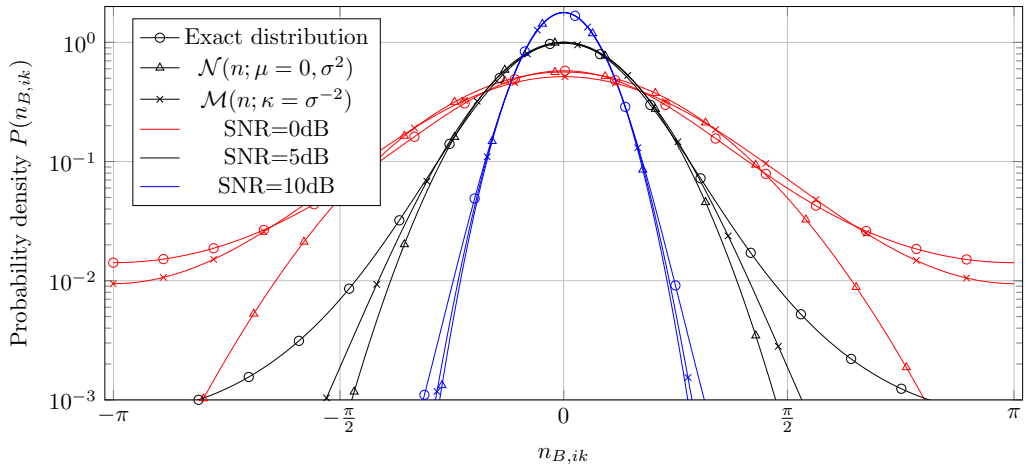

Figure 2. Probability distribution of the real phase error $n_{B,ik}$ and approximations by Gaussian and von-Mises distributions for different SNR. For high SNR, both Gaussian and von-Mises match the exact distribution well, whereas for low SNR, the von-Mises distribution is advantageous.

2.2. Geometry Model

The channel phase between Alice and Bob for varying α, β is given by

$$\phi_{ik} = 2\pi \frac{d_{ik}}{\lambda} \mod 2\pi \tag{8}$$

where $\lambda = cf_c$ is the carrier's wavelength. Using (4) we get

$$d_{ik} = \sqrt{(d - r_A \cos\alpha_i + r_B \cos\beta_k)^2 + (r_A \sin\alpha_i - r_B \sin\beta_k)^2} \tag{9}$$

Assuming that $d \gg r_A$ and $d \gg r_B$ we omit the second part under the square root and find

$$\phi_{ik} \approx 2\pi \frac{d}{\lambda} - 2\pi \frac{r_A \cos\alpha_i}{\lambda} + 2\pi \frac{r_B \cos\beta_i}{\lambda} \mod 2\pi \tag{10}$$

$$= \phi_0 + \phi_{A,i} + \phi_{B,k} \mod 2\pi. \tag{11}$$

Here, ϕ_0 is a constant due to the average distance and $\phi_{A,i}, \phi_{B,k}$ describe the phase contributions due to the rotation of Alice and Bob.

Let us assume α_i and β_k are uniformly distributed, i.e., $P(\beta_k) = (2\pi)^{-1}$ and Alice and Bob have no preferred orientation. Then, applying random variable transformation to $\phi(\beta_k)$ yields

$$\phi_{B,k}(\beta_k) = 2\pi \frac{r_B \cos(\beta_k)}{\lambda} \mod 2\pi \tag{12}$$

$$= 2\pi \frac{r_B \cos(\beta_k)}{\lambda} + n \cdot 2\pi \text{ s.t. } \phi_{B,k} \in [-\pi, \pi] \tag{13}$$

$$\beta_k(\phi_{B,k}) = \cos^{-1}\left(\frac{\lambda \cdot \phi_{B,k}}{2\pi r_B} - \frac{\lambda \cdot n}{r_B}\right) \tag{14}$$

$$\frac{d\beta_k(\phi_{B,k})}{d\phi_{B,k}} = \frac{\lambda}{2\pi} \frac{1}{\sqrt{1 - (\frac{\lambda \cdot \phi_{B,k}}{2\pi r_B} - \frac{\lambda \cdot n}{r})^2}} \tag{15}$$

and thus

$$P_{\phi_{B,k}}(\phi_{B,k}) = P_\beta(\beta_k(\phi_{B,k})) \frac{d\beta_k(\phi_{B,k})}{d\phi_{B,k}} \tag{16}$$

$$= \frac{\lambda}{2\pi^2 r_B} \sum_n \frac{1}{\sqrt{1 - \left(\frac{\lambda(\phi_B - 2\pi n)}{2\pi r_B}\right)^2}}, \tag{17}$$

where the summation is over all n such that the square root is real. In particular, for $r_B \leq \lambda/2$ the expression simplifies to

$$P_{\phi_{B,k}}(\phi_{B,k}) = \frac{1}{\pi^2 \sqrt{1 - (\frac{\lambda \cdot \phi_{B,k}}{2\pi r_B})^2}}, \tag{18}$$

where for $r_B < \lambda/2$ not even all channel phases are reached.

On the other hand, taking the limit for infinite r_B we obtain

$$\lim_{r_B \to \infty} P_{\phi_{B,k}}(\phi) = \frac{1}{2\pi^2 U} \sum_n \frac{1}{\sqrt{1 - \left(\frac{k}{U}\right)^2}} \tag{19}$$

$$= \frac{1}{2\pi^2 U} \int_{-1}^{1} \frac{U dx}{\sqrt{1 - x^2}} = \frac{1}{2\pi}, \tag{20}$$

where $U = \frac{r_B}{\lambda}$ and $dx = \frac{n}{U} - \frac{n+1}{U} = \frac{1}{U}$ and hence for large r_B the distribution approaches uniformity.

Figure 3 shows the phase distribution for different ratios of λ/r_B. As visible, for $\lambda/r_B = \frac{1}{4}$, the channel phase does not reach the entire range of angles, because the antenna radius is too small. On the other hand, the bigger the r_B, the more the distribution approaches a uniform distribution, and already for $\lambda/r_B = \frac{1}{2}$ the real distribution is very close to uniform. Note that analogous considerations can be carried for the distribution of $\phi_{A,i}$, yielding the analog expressions.

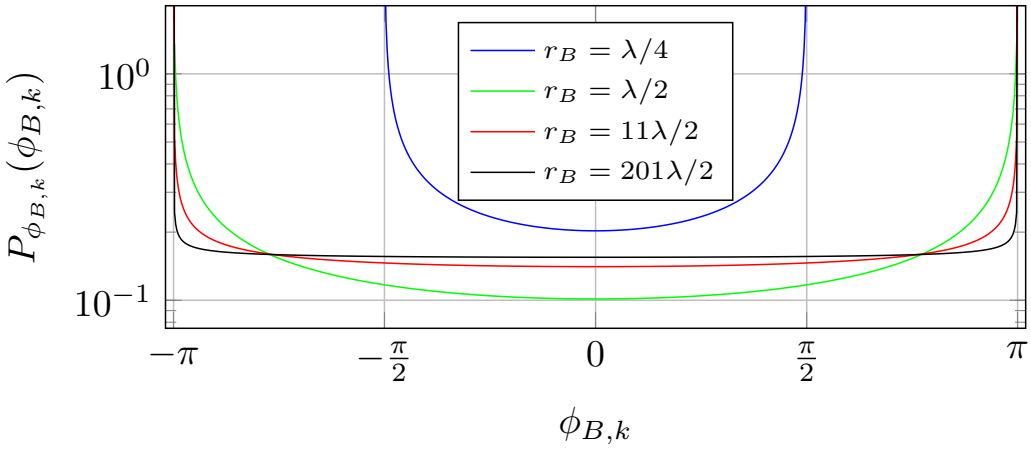

Figure 3. PDF of $\phi_{B,k}$ for different antenna rotation radii. With increasing radius, the PDF approaches the uniform distribution.

3. Mutual Information

For calculating the mutual information $I(A;B)$ we assume $\phi_0 = 0$, since a constant angle offset does not influence the mutual information between Alice and Bob. Moreover, in the sequel we assume that if Alice or Bob have two antennas, then $\alpha_1 = \alpha_2 + \pi = \alpha$ and $\beta_1 = \beta_2 + \pi = \beta$, i.e., the antennas at both Alice and Bob have an angle offset of 180 degree. In this case, $\phi_{A,1} = -\phi_{A,2}$ and $\phi_{B,1} = -\phi_{B,2}$.

3.1. Single-Antenna Case

In the most basic 1×1-case, where Alice and Bob have one antenna each and only Bob rotates their antenna, the measurement model can be written as

$$\hat{\phi}_{A,11} = \phi_{B,1} + n_{A,11} \qquad \hat{\phi}_{B,11} = \phi_{B,1} + n_{B,11}, \tag{21}$$

where both summations are performed mod 2π. Here, we consider $\phi_{A,0} = 0$ since $\phi_{A,0}$ is constant and any constant angle will not influence $I(A;B)$. We substract both equations and get

$$\hat{\phi}_{A,11} = \hat{\phi}_{B,11} + n_{B,11} - n_{A,11}, \tag{22}$$

and therefore

$$\begin{aligned} I(\hat{\phi}_{A,11}; \hat{\phi}_{B,11}) &= I(\hat{\phi}_{B,11} + n; \hat{\phi}_{B,11}) && (23)\\ &= H(\hat{\phi}_{B,11} + n) - H(\hat{\phi}_{B,11} + n | \hat{\phi}_{B,11}) && (24)\\ &= H(\phi_{B,1} + n_{A,11}) - H(n), && (25) \end{aligned}$$

where $n = n_{B,11} - n_{A,11}$ is the sum of the measurement noise at Alice's and Bob's antenna.

In (17) it was shown that the distribution of $\phi_{B,1}$ is already nearly uniform. Since additive noise results equalizes the distribution more, we assume $\hat{\phi}_{A,11}$ to be nearly uniformly

distributed. Therefore, the first component of the mutual information can be approximated (and upper bounded) by the entropy of the uniform distribution on $[-\pi, \pi)$:

$$H(\phi_{B,1} + n_{A,11}) \lessapprox \log_2(2\pi) \tag{26}$$

For the second part, $H(n_{B,11} - n_{A,11})$ we consider that both $n_{A,11}, n_{B,11}$ are independent and, for higher SNR, nearly Gaussian distributed. Hence, the difference of both is also distributed according to a Gaussian with variance $\mathrm{Var}(n) = \sigma_A^2 + \sigma_B^2$. However, before we saw that the periodice von-Mises distribution approximates the real phase distribution better for lower SNRs, and therefore we assume that n is von-Mises distributed with

$$n \sim \mathcal{M}(\kappa = \tfrac{2}{\sigma_A^2 + \sigma_B^2}). \tag{27}$$

Note, that this expression does not hold exactly for lower SNR, since in this case the variances do not add completely due to the summation mod 2π. The deviation will be pointed out in the simulation results. Hence, $I(\hat{\phi}_{A,11}; \hat{\phi}_{B,11})$ can be calculated by

$$\begin{aligned} I(\hat{\phi}_{A,11}; \hat{\phi}_{B,11}) &\leq \log_2(2\pi) - H_M(\kappa = \tfrac{2}{\sigma_A^2 + \sigma_B^2}) && (28)\\ &= \frac{1}{\ln 2} \frac{\kappa I_1(\kappa)}{I_0(\kappa)} - \log_2(I_0(\kappa))\Big|_{\kappa = \frac{2}{\sigma_A^2 + \sigma_B^2}} && (29)\\ &=: I_{1\times 1}(\sigma_A^2, \sigma_B^2), && (30) \end{aligned}$$

where $H_M(\kappa)$ is the differential entropy of a von-Mises distributed random variable with parameter κ.

3.2. 1×2 *System*

The case with multiple antennas can be directly derived from the fundamental single-antenna case. First, we consider a 1×2 system where Bob has 2 antennas, and Alice has 1 antenna, and only Bob rotates their antennas, the measurement equations become:

$$\hat{\phi}_{A,11} = \phi_{B,1} + n_{A,11}, \qquad \hat{\phi}_{B,11} = \phi_{B,1} + n_{B,11}, \tag{31}$$

$$\hat{\phi}_{A,12} = -\phi_{B,1} + n_{B,12}, \qquad \hat{\phi}_{B,12} = -\phi_{B,1} + n_{B,12}. \tag{32}$$

Essentially, now Bob and Alice have two independent noisy observations of the same underlying random variable $\phi_{B,1}$. Therefore, the mutual information can be calculated from the fundamental case by a simple SNR shift:

$$\begin{aligned} I_{1\times 2}(\sigma_A^2, \sigma_B^2) &:= I(\hat{\phi}_{A,11}, \hat{\phi}_{A,12}; \hat{\phi}_{B,11}, \hat{\phi}_{B,12}) && (33)\\ &= I_{1\times 1}(\tfrac{\sigma_A^2}{2}, \tfrac{\sigma_B^2}{2}). && (34) \end{aligned}$$

3.3. 2×2 *System*

Eventually, the 2×2-case where both Alice and Bob have two antennas each, and both Alice and Bob rotate their antennas yields the following measurement equations for Alice,

$$\begin{aligned} \hat{\phi}_{A,11} &= \phi_{A,1} + \phi_{B,1} + n_{A,11} && (35)\\ \hat{\phi}_{A,12} &= \phi_{A,1} - \phi_{B,1} + n_{A,12} && (36)\\ \hat{\phi}_{A,21} &= -\phi_{A,1} + \phi_{B,1} + n_{A,21} && (37)\\ \hat{\phi}_{A,22} &= -\phi_{A,1} - \phi_{B,1} + n_{A,22}, && (38) \end{aligned}$$

and similar equations can be formulated for Bob's reception. Compared to the case where only Bob rotated their antennas, the system now has two degrees of freedom, namely $\phi_{A,1}$ and $\phi_{B,1}$. Therefore, we expect the mutual information to be double compared to the case with a single degree of freedom. At the same time, each side has four measurements

to estimate two parameters. Compared to the single-antenna case, where each side had one measurement to estimate one parameter, the SNR is again doubled. Consequently, the mutual information in the multi-antenna case is given by

$$I_{2\times 2}(\sigma_A^2, \sigma_B^2) := I\left(\begin{pmatrix}\hat{\phi}_{A,11}\\ \hat{\phi}_{A,12}\\ \hat{\phi}_{A,21}\\ \hat{\phi}_{A,22}\end{pmatrix}; \begin{pmatrix}\hat{\phi}_{B,11}\\ \hat{\phi}_{B,12}\\ \hat{\phi}_{B,21}\\ \hat{\phi}_{B,22}\end{pmatrix}\right) \tag{39}$$

$$= 2 \cdot T_{1\times 1}(\tfrac{\sigma_A^2}{2}, \tfrac{\sigma_B^2}{2}). \tag{40}$$

3.4. Optimal Rotation Distribution

Before, we saw that (25) is maximized, if $\phi_{A,i}$ and $\phi_{B,k}$ are uniformly distributed. Hence, finding a distribution for α, β that yields a uniform channel phase will maximize $I(A;B)$. When Alice and Bob have no preferred orientation and hence α, β are uniformly distributed, ϕ is distributed according to (17). On the other hand, for $r_B = \lambda/2$, if

$$P_\beta = \frac{1}{4}\sqrt{1-\cos^2(\beta)} \tag{41}$$

is inserted into (16) it becomes apparent that $\phi_{B,k}$ is uniformly distributed for the given optimal rotation distribution in (41).

4. Simulation Results

This section shows simulated MI between Alice and Bob along with the analytic results from above. The results were obtained in Python by simulating (6) and then taking the phase according to (7). We assume ideal synchronization and no hardware impairments like phase noise of the oscillators. The distances d_{ik} that are used to generate $\phi_{ik} = d_{ik}/c$ have been obtained by using the exact geometry expression from (4) for random rotations of the antennas at Alice and Bob. The distribution of the rotation angle of Alice and Bob was uniform except for the optimized rotation distribution described in the previous section. The mutual information was estimated using the Python NPEET package [13]. For each SNR point, sufficiently many samples were obtained until the curves became smooth and the upper bound of calculatable mutual information imposed by the NPEET algorithm [14] was not reached. In particular, this corresponded to 500.000 angle realizations per SNR point. The source code used for obtaining the results is contained in the supplementary material of this paper.

Figure 4 shows the $I(A;B)$ for the single-antenna system with different r_B. The distance between Alice and Bob was set to $d = 100\lambda$. As mentioned before, with increasing r_B, the distribution of $\phi_{B,1}$ nears the uniform distribution and the uniform distribution of $\phi_{B,1}$ maximizes the obtained mutual information. Figure 4 also shows the simulated MI curve, when $\phi_{B,1}$ is truly uniformly distributed. For $r_B = \lambda$ these curves are reasonably close and they virtually overlap for $r_B = 5\lambda$. Moreover, we show that for SNR > 5 dB the curve for uniform $\phi_{B,1}$ overlaps the theoretic curve $I_{1\times 1}$.

Figure 5 shows the simulated MI for the single and multi-antenna systems with $r_B = \lambda, d = 100\lambda$ along with the theoretic curves. As can be seen, for SNR > 5 dB the simulated curves are closely upper bounded by the theory, whereas for the lower SNR the theoretic curves estimate the mutual information too low. This is due to the fact that in lower SNR $\mathrm{Var}(n) \neq \sigma_A^2 + \sigma_B^2$ because the noise samples are added $\mod 2\pi$ and their entropy is upper bounded by the uniform distribution. Therefore, $H(n)$ in (25) is estimated too high. However, the approximation is still very close.

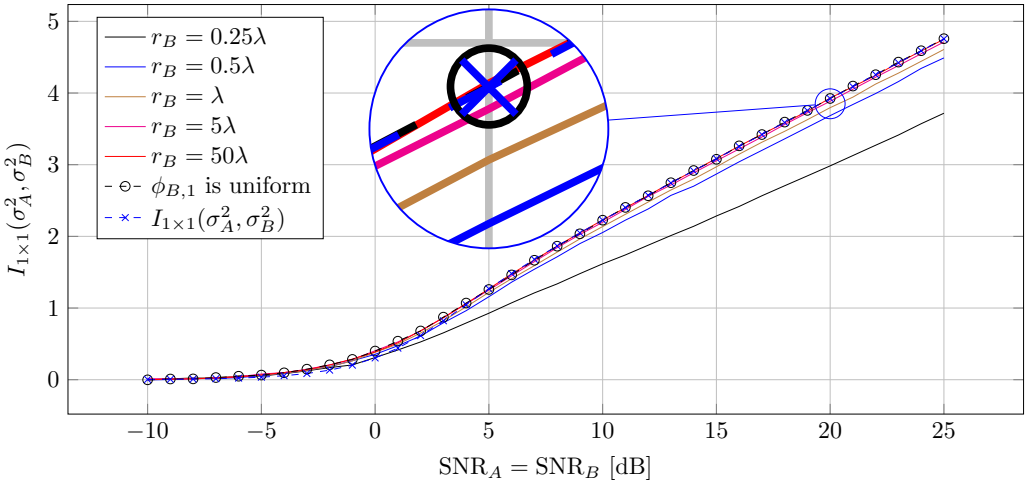

Figure 4. Mutual information for different antenna radius. The higher the antenna radius, the closer the simulated MI approaches the theoretic curve.

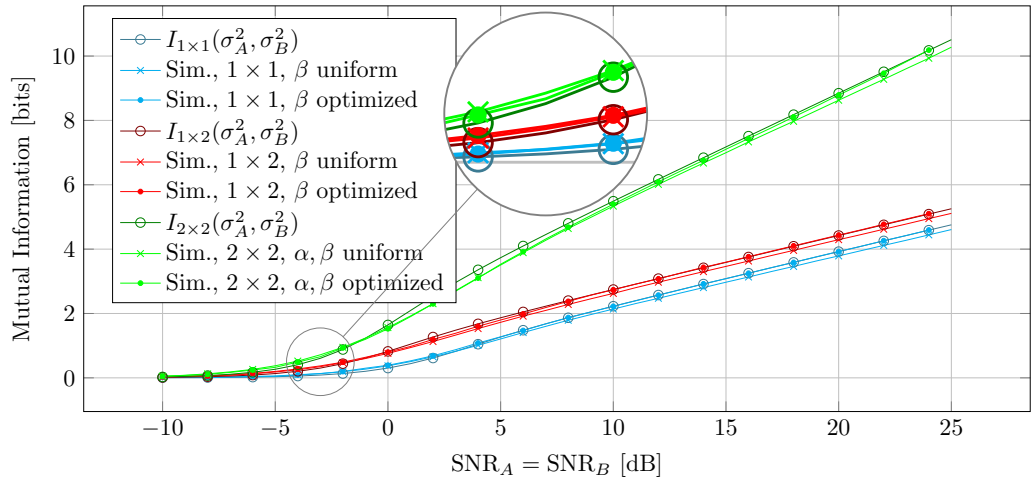

Figure 5. Mutual Information for equal SNR for Alice and Bob.

Figure 6 shows the measured and theoretic mutual information for single and multi-antenna systems where the SNR at Alice and Bob is different. This can, e.g., happen in a non-symmetric scenario like in an up- and downlink of a celluar system. Naturally, when the SNR of Bob is fixed, $I(A;B)$ approaches a finite limit for high SNR_A. The theoretic and simulated curves match well, and still the theoretic curve is an upper bound for $I(A;B)$ for $\mathrm{SNR} > 5$ dB.

Figure 5 also shows the simulated curves for $I(A;B)$ when Alice and Bob distribute their orientation according to (41). As can be seen, in this case $I(A;B)$ is above that of a uniform orientation of Alice and Bob. Moreover, the simulated curves overlap the curves for the analytic upper bound and hence prove that the MI between Alice and Bob indeed has been maximized.

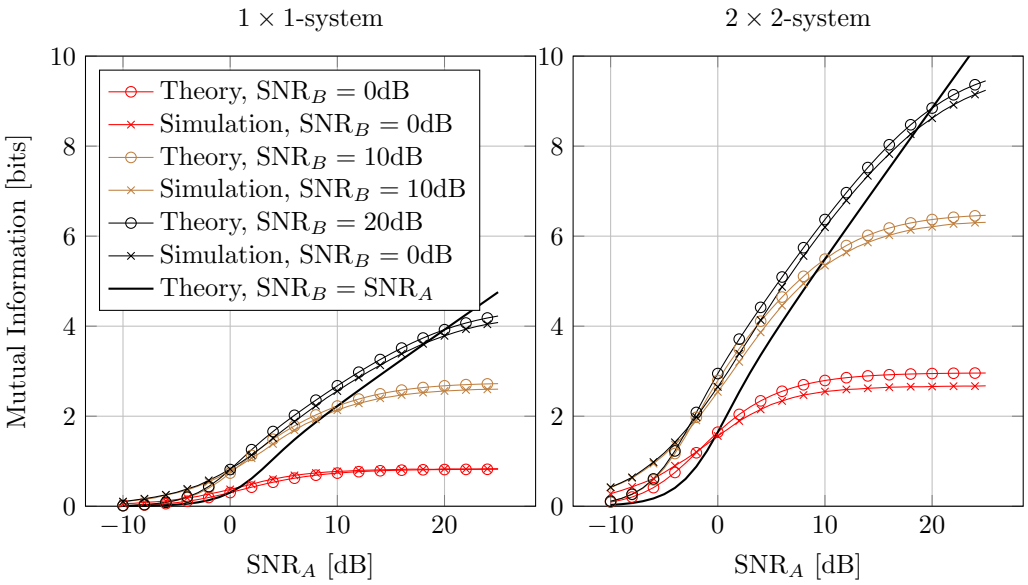

Figure 6. Mutual Information for different SNR for Alice and Bob.

5. Conclusions

In this paper, we derive analytic expressions for the mutual information between two communicating devices, where the shared information is the phase of the reciprocal line-of-sight MIMO channel between both devices. Using randomly moving antennas, the channel phase becomes a random variable that is estimated at both sides. Such commonly estimated information can be used for example as an entropy source for key-generation in physical-layer-based security schemes.

The derived expressions match well with the simulation results, proving their validity. The results can be calculated much faster and more flexibly compared to running tedious numerical simulations for different SNR combinations. Moreover, we derived an antenna rotation scheme which maximizes the mutual information and proved the validity with simulation results. The results are valid for one or two transmit antennas only, and cannot be straightforwardly extended to four or more antennas. Another open point is the extension of the geometry to the three-dimensional space, where Alice and Bob have two degrees of freedom in their rotation, respectively.

The obtained results indicate that the channel phase of an LOS MIMO channel contains sufficient information to synchronously generate random keys. At a high SNR, which can be well assumed in LOS scenarios, each antenna can provide up to five bits of entropy per measurement under ideal conditions. The obtained results help engineers estimate the required SNR for real-world experiments and the presented derivations enable researchers to elaborate on more sophisticated system models including higher dimensions and more antennas.

Future Works

In future works, the presented results shall be verified with real-world measurements to validate the obtained expressions. Here, a solution using software-defined radios and offline signal processing shall be the first step to compare theoretic and simulated results with real-world measurements.

On the theoretical side, it is of utmost importance to derive expressions when an eavesdropper "Eve" enters the stage, because a secret key generation algorithm needs to not only consider common information between Alice and Bob but also what information is available to an eavesdropper [4]. Here, the position of Eve relative to Alice and Bob will have a major influence on the dropped information, because, as this paper has shown, some rotation angles exhibit more information than others. Hence, expressions involving the position of Alice, Bob and Eve need to be developed.

Finally, an actual key generation algorithm that exploits the channel phase between devices should be designed, theoretically and numerically evaluated and eventually validated with real measurements. Here, a multi-step approach as described in [15] consisting of Randomness Extraction, Quantization, Information Reconciliation and Privacy Amplification can be a promising solution.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/e25071038/s1, Source code for regenerating the simulation results.

Author Contributions: Conceptualization, M.M. and A.C.; software, M.M.; writing, M.M. and A.C.; supervision, A.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work is financed on the basis of the budget passed by the Saxon State Parliament.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Source code to regenerate the simulation results is provided as supplementary material to this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zhang, J.; Li, G.; Marshall, A.; Hu, A.; Hanzo, L. A New Frontier for IoT Security Emerging from Three Decades of Key Generation Relying on Wireless Channels. *IEEE Access* **2020**, *8*, 138406–138446. [CrossRef]
2. Mosca, M. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Secur. Priv.* **2018**, *16*, 38–41. [CrossRef]
3. Chorti, A.; Barreto, A.N.; Köpsell, S.; Zoli, M.; Chafii, M.; Sehier, P.; Fettweis, G.; Poor, H.V. Context-Aware Security for 6G Wireless: The Role of Physical Layer Security. *IEEE Commun. Stand. Mag.* **2022**, *6*, 102–108.
4. Maurer, U.M. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742. [CrossRef]
5. Mitev, M.; Barreto, A.N.; Pham, T.M.; Fettweis, G. Secret Key Generation Rates over Frequency Selective Channels. In Proceedings of the IEEE Vehicular Technology Conference, Helsinki, Finland, 19–22 June 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–5. [CrossRef]
6. Veronica Belmega, E.; Chorti, A. Protecting Secret Key Generation Systems Against Jamming: Energy Harvesting and Channel Hopping Approaches. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2611–2626. [CrossRef]
7. Pham, T.M.; Mitev, M.; Chorti, A.; Fettweis, G.P. Pilot Randomization to Protect MIMO Secret Key Generation Systems Against Injection Attacks. *IEEE Wirel. Commun. Lett.* **2023**, 1. [CrossRef]
8. Mitev, M.; Shakiba-Herfeh, M.; Chorti, A.; Reed, M.; Baghaee, S. A Physical Layer, Zero-Round-Trip-Time, Multifactor Authentication Protocol. *IEEE Access* **2022**, *10*, 74555–74571. [CrossRef]
9. Hua, Y. Generalized Channel Probing and Generalized Pre-Processing for Secret Key Generation. *IEEE Trans. Signal Process.* **2023**, *71*, 1067–1082. [CrossRef]
10. Pham, T.M.; Barreto, A.N.; Mitev, M.; Matthe, M.; Fettweis, G. Secure Communications in Line-of-Sight Scenarios by Rotation-based Secret Key Generation. In Proceedings of the 2022 IEEE International Conference on Communications Workshops, ICC Workshops 2022, Seoul, Republic of Korea, 16–20 May 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1101–1106. [CrossRef]
11. Luo, Z.; Zhan, Y.; Jonckheere, E. Analysis on Functions and Characteristics of the Rician Phase Distribution. In Proceedings of the 2020 IEEE/CIC International Conference on Communications in China, ICCC 2020, Chongqing, China, 9–11 August 2020; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2020; pp. 306–311. [CrossRef]
12. Mardia, K.V.; Jupp, P.E. *Directional Statistics*; John Wiley & Sons: Hoboken, NJ, USA, 1999. [CrossRef]
13. Steeg, G.V. Non-Parametric Entropy Estimation Toolbox. 2023. Available online: https://github.com/gregversteeg/NPEET (accessed on 31 May 2023).
14. Mitev, M.; Barreto, A.N.; Pham, T.M.; Matthé, M.; Fettweis, G. Filterbank Secret Key Generation Rates in Multipath Channels. In Proceedings of the 2022 IEEE Global Communications Conference, GLOBECOM 2022—Proceedings, Rio de Janeiro, Brazil, 4–8 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 4057–4062. [CrossRef]
15. Amitha Mayya Miroslav Mitev, A.C.G.F. Effects of Channel Characteristics and Design Parameters on Secret Key Generation Rates. In Proceedings of the European Conference on Networks and Communications, Gothenburg, Sweden, 6–9 June 2023.