On the Zero-Outage Secrecy-Capacity of Dependent Fading Wiretap Channels

Eduard Jorswieck *,†, Pin-Hsun Lin † and Karl-Ludwig Besser †

Institute for Communications Technology, TU Braunschweig, 38106 Braunschweig, Germany; Lin@ifn.ing.tu-bs.de (P.-H.L.); besser@ifn.ing.tu-bs.de (K.-L.B.)
* Correspondence: jorswieck@ifn.ing.tu-bs.de; Tel.: +49-531-391-2480
† These authors contributed equally to this work.

Abstract: It is known that for a slow fading Gaussian wiretap channel without channel state information at the transmitter and with statistically independent fading channels, the outage probability of any given target secrecy rate is non-zero, in general. This implies that the so-called zero-outage secrecy capacity (ZOSC) is zero and we cannot transmit at any positive data rate reliably and confidentially. When the fading legitimate and eavesdropper channels are statistically dependent, this conclusion changes significantly. Our work shows that there exist dependency structures for which positive zero-outage secrecy rates (ZOSR) are achievable. In this paper, we are interested in the characterization of these dependency structures and we study the system parameters in terms of the number of observations at legitimate receiver and eavesdropper as well as average channel gains for which positive ZOSR are achieved. First, we consider the setting that there are two paths from the transmitter to the legitimate receiver and one path to the eavesdropper. We show that by introducing a proper dependence structure among the fading gains of the three paths, we can achieve a zero secrecy outage probability (SOP) for some positive secrecy rate. In this way, we can achieve a non-zero ZOSR. We conjecture that the proposed dependency structure achieves maximum ZOSR. To better understand the underlying dependence structure, we further consider the case where the channel gains are from finite alphabets and systematically and globally solve the ZOSC. In addition, we apply the rearrangement algorithm to solve the ZOSR for continuous channel gains. The results indicate that the legitimate link must have an advantage in terms of the number of antennas and average channel gains to obtain positive ZOSR. The results motivate further studies into the optimal dependency structures.

Keywords: wiretap channel; secrecy capacity; dependent fading; copulas

1. Introduction

With the rise of new technologies and applications, e.g., in the context of 6G [1], more sensitive data are transmitted wirelessly. Thus, it is crucial to ensure a confidential transmission and protect the information against possible eavesdroppers. Besides cryptography, physical layer security [2] is a promising approach to enable secure data transmission. In contrast to cryptography, no shared key is required, but the physical properties of the wireless channel are exploited. This establishes post-quantum security by information-theoretic methods and offers better protection than many common cryptography schemes, which rely on the complexity of certain computations, that can be solved fast on quantum computers [3].

It is well-known that there exists a certain class of channel codes, which allow transmitting with zero information leakage over the standard additive white Gaussian noise (AWGN) channel. In the case that the channels to the legitimate receiver and the eavesdropper experience fading, it is possible that secrecy outages occur due to the random nature of the channel fading [4]. For slow-fading channels, the appropriate performance metrics are the (secrecy) outage probability and the \( \epsilon \)-secrecy-outage capacity, i.e., the maximum rate at which one can communicate with at most \( \epsilon \) (secrecy) outages.
In order to improve the reliability, multiple antennas are often employed at the receiver or transmitter. Spatial diversity not only improves reliability, but can also be applied at the eavesdropper to increase the information leakage. It heavily depends on the joint distributions of the fading channels, whether benefits in terms of reliability or in terms of information leakage can be achieved. While the marginal fading distributions of the individual fading links can be measured easily, the joint distribution is typically unknown. A common assumption in the literature is, therefore independence [5–7], which can have a major impact on the estimated performance [8]. If we consider the standard wiretap channel and consider the secrecy capacity, it is shown in [9] that the ergodic secrecy capacity only depends on the marginal distributions of the observations at Bob and Eve. In contrast, the outage secrecy capacity depends on the joint distribution and the same marginal property does not hold. Additionally, real measurements demonstrate that this assumption does not always hold in practice [10,11]. Especially for physical layer security systems, this can have significant consequences.

It is therefore of great interest to analyze the performance of such communication systems where independence between the marginal fading links does not hold. In [12,13], bounds on the secrecy capacity for correlated Rayleigh fading channels are derived. Similarly, the secrecy performance for correlated log-normal and Gamma fading channels is considered in [14,15], respectively. In all of this previous work, only (positive) linear correlation is considered. However, the joint fading distribution might have nonlinear dependency features [10]. A more general approach is therefore taken in [16], where the secrecy outage probability (SOP) is derived for Rayleigh fading links that follow a certain dependency structure. More generally, bounds on the SOP with respect to all possible joint distributions are derived in [17].

One particularly interesting result in [17] is that the SOP in the best case can be equal to the outage probability due to the fading of the channel to the legitimate receiver, i.e., there exists a joint fading distribution that effectively hides the eavesdropper. The analysis in [17] is for a single-input single-output (SISO) scenario where all communication parties are equipped with only a single antenna. For a point-to-point transmission without eavesdropper, it was shown in [18,19] that it is possible to have a positive zero-outage capacity with multiple dependent fading channels. A natural question will be: can we extend the concept of zero-outage capacity, to the wiretap channel, namely, the zero-outage secrecy capacity (ZOSC)? By definition, zero-outage secrecy rate (ZOSR) is the secrecy rate of any achievable scheme which guarantees zero outage probability and ZOSC is the largest ZOSR. Please note that the ZOSC is an important performance metric because it describes the transmission rate of data which is guaranteed to be delivered reliably and confidentially for every channel use, i.e., for every set of channels to the legitimate receiver and to the eavesdropper. This implies that the eavesdropper does not obtain any information about the message and it also implies that the legitimate receiver is always able to correctly decode. Physical layer security mechanisms are the first line of defense [20] for future wireless communications systems. The ZOSC provides a very strong first line of defense. Therefore, the question remains, how much lower the SOP can be when the receiver and the eavesdropper have multiple observations and, in particular, if it is possible to obtain a positive ZOSC.

In this work, we answer the aforementioned question positively and show that there exist joint distributions which support a positive ZOSC. Note that the primary goal of the work is to show the existence of dependency structures which support positive ZOSC. We will not answer the question how to realize these dependency structures in practice. However, we point out that recent developments and progress in reconfigurable intelligent surfaces (RISs) [21] could enable to transform the propagation environment to the corresponding dependency structure.

Please also note that compared to our previous works [17,18], there are major differences in this work. In [17], we only consider the SISOSE model, i.e., every user only has a single antenna. Most importantly, with this model, it is not possible to achieve a positive ZOSR,
which is the topic of the presented paper. Furthermore, it is not possible to simply apply the results from [17], since they only hold for two random variables. Since we now consider the multi-antenna case, we need to deal with more than two random variables. For a peaceful point-to-point system, we investigated the zero-outage capacity (ZOC) for systems with multiple receive antennas in [18]. However, in the previous paper, we only consider systems without the secrecy constraint and here, the secrecy constraint is considered. With this additional constraint, the rate/capacity expression is completely different. More specifically, to fulfill the secrecy constraint, wiretap coding must be used and then the secrecy rate expression in the additive white Gaussian noise (AWGN) channel has an additional negative term as the cost to fulfill the secrecy constraint. This negative term transforms the rate expression from symmetric into asymmetric in the channel gains. Due to this asymmetry, it is not possible to simply apply the results from [18] and it is therefore unclear, if the counter- and co-monotonicity of the dependence structure among the channel gains is optimal. These huge discrepancies are our main motivation to investigate the model considered in this paper and also the unique value of this work distinguished from the previous ones.

In particular, our contributions are summarized in the following.

- First, we consider a basic wiretap channel where there are two paths to a single legitimate receiver and one single path to a single eavesdropper. The channel gains are correlated slow fading and perfectly known at the receiver and eavesdropper, but unknown to the transmitter.
- Based on copulas, we derive an analytical solution for the ZOSR when Rayleigh fading is considered. In particular, the positive ZOSR is achieved by counter-monotonically distributed channel gains between the transmitter and the legitimate receiver. In contrast, the sum of the above two channel gains is co-monotonically distributed with respect to Eve’s channel gain.
- To gain a better understanding of the optimality of the dependency structure, we further transform the original ZOSC maximization problem into an equivalent form. Using the equivalent form, we propose an algorithm which efficiently solves the case where the channel gains are from finite alphabets. Interestingly, numerical results show that the optimal joint distribution of channel gains does not follow the aforementioned counter- and co-monotonicity relation.
- Then, we consider the generalization of the wiretap setup to multiple observations at Bob and Eve. We provide an algorithm to compute an achievable ZOSR and apply the rearrangement algorithm (RA) to solve the ZOSR problem for fading gains with continuous alphabets for a general number of observations.

Notation: Throughout this work, we use the following notation. Random variables are denoted in capital letters, e.g., $X$, and their realizations in small letters, e.g., $x$. Vectors are written in boldface letters, e.g., $X = (X_1, \ldots, X_n)$. We use $F$ and $f$ for a probability distribution and its density, respectively. The expectation is denoted by $E$ and the probability of an event by $P$. The uniform distribution on the interval $[a, b]$ is denoted as $U[a, b]$. The normal distribution with mean $\mu$ and variance $\sigma^2$ is denoted as $\mathcal{N}(\mu, \sigma^2)$. As a shorthand, we use $|x|^+ = \max\{|x|, 0\}$. The real numbers, non-negative real numbers, and extended real numbers are denoted by $\mathbb{R}$, $\mathbb{R}_+$, and $\bar{\mathbb{R}}$, respectively. Logarithms, if not stated otherwise, are assumed to be with respect to the natural base.

2. System Model and Preliminaries

2.1. System Model

Throughout this work, we consider a slow-fading Gaussian wiretap channel [5], which is depicted in Figure 1.
The communication system consists of a single-antenna transmitter (Alice), a legitimate receiver (Bob), and a passive eavesdropper (Eve). Bob and Eve obtain $n_B$ and $n_E$ observations, respectively. These could stem from multiple antennas or from colluding eavesdroppers. Note that multiple colluding eavesdroppers and a single one with multiple antennas are equivalent. Alice encodes her messages, which she wants to transmit securely, and transmits symbols $S \in \mathbb{C}$. Bob’s and Eve’s received signals are then, respectively, given as

$$B = h_B S + W_B,$$

$$E = h_E S + W_E,$$

where $h_i \in \mathbb{C}^{n_i}$ and $W_i \in \mathbb{C}^{n_i}$, with $i \in \{B, E\}$, denote the fading coefficients and the independent AWGN with noise power $\sigma_i^2$, respectively. The transmission at Alice is subject to an average power constraint $P$, i.e.,

$$\mathbb{E}[|S|^2] \leq P.$$

The receiver signal-to-noise ratios (SNRs) are then given as $\rho_B = P/\sigma_B^2$ and $\rho_E = P/\sigma_E^2$ for Bob and Eve, respectively.

For one realization of the slow fading coefficients $h_B$ and $h_E$, the instantaneous secrecy capacity $C_S$ is given by ([22] Theorem 1 specialized to SIMOME wiretap channels)

$$C_S = \left[ \log_2 \left( 1 + \sum_{i=1}^{n_B} X_i \right) - \log_2 \left( 1 + \sum_{i=1}^{n_E} Y_i \right) \right]^+$$

with the shorthands $X_i = \rho_B |h_{B,i}|^2$ and $Y_i = \rho_E |h_{E,i}|^2$.

In the following, we assume perfect channel-state information (CSI) at the receivers and perfect CSI about the main channel to Bob at the transmitter. However, only statistical CSI about the channel to Eve at Alice is assumed. For transmission, we consider a constant secrecy rate $R_S$. With this, it follows that a secrecy outage event happens, if the secrecy rate is greater than the instantaneous secrecy capacity, i.e., $C_S < R_S$. This leads to the definition of the SOP $\varepsilon$ as ([2] Definition 5.1)

$$\varepsilon = P(C_S < R_S).$$

Based on the SOP, we can define the $\varepsilon$-outage secrecy capacity $R_S^\varepsilon$ as the highest rate, such that the SOP is at most $\varepsilon$, i.e.,

$$R_S^\varepsilon = \sup_{R \geq 0} \{ R \mid P(C_S < R) \leq \varepsilon \}.$$
2.2. Problem Formulation

We consider dependent fading channels, i.e., we have that the joint distribution of the fading channels does not factor into the product of marginal distributions, $F_{h_{B_1}, \ldots, h_{B_n}, h_{E_1}, \ldots, h_{E_n}} \neq F_{h_{B_1}} \cdot \ldots \cdot F_{h_{E_1}} \cdot F_{h_{E_2}} \cdot \ldots \cdot F_{h_{E_n}} \cdot F_{h_{E_n}}$. The joint distribution is unknown, however the marginals $F_{h_{B_i}}$ are assumed to be known. The marginals could be estimated from channel measurements of the corresponding point-to-point links.

With the above considerations, we can formulate the exact problem statement for the rest of this work. Our focus is on the ZOSC and we are interested in the question: is it possible to obtain a positive ZOSC for certain dependent fading channels? If yes, under what conditions and what are the values for common fading models?

For simplicity, we denote the configuration of the wiretap channel setup, which consists of $n_B$ observations at Bob, $n_E$ observations at Eve, by the notation $[n_B, n_E]$-wiretap channel. After introducing the mathematical background, we consider the simple setup of the $[2,1]$-wiretap channel first ($n_E > 1$ could correspond to the case of $n_E$ colluding eavesdroppers).

2.3. Mathematical Background

In order to answer the above questions, we need some mathematical background from copula theory [23], which we will introduce in the following.

The central elements of copula theory are copulas, which are defined as follows.

**Definition 1** (Copula). A copula is an $n$-dimensional distribution function with standard uniform marginals.

The practical relevance of copulas stems from Sklar’s theorem, which we restate in the following Theorem 1.

**Theorem 1** (Sklar’s Theorem ([23] Theorem 2.10.9)). Let $F_X$ be an $n$-dimensional distribution function with margins $F_1, \ldots, F_n$. Then there exists a copula $C$ such that for all $x \in \mathbb{R}^n$,

$$F_X(x_1, \ldots, x_n) = C(F_1(x_1), \ldots, F_n(x_n)). \quad (6)$$

If $F_1, \ldots, F_n$ are all continuous, then $C$ is unique. Conversely, if $C$ is a copula and $F_1, \ldots, F_n$ are distribution functions, then $F_X$ defined by (6) is an $n$-dimensional distribution function with margins $F_1, \ldots, F_n$.

This theorem implies that copulas can be used to describe dependency structures among random variables, regardless of their marginal distributions. We can therefore separate the joint distribution into the dependency structure (described by the copula $C$) and the marginal distributions $F_1, \ldots, F_n$.

One of the best-known copulas is the independence copula $\Pi(u_1, \ldots, u_n) = \prod_{i=1}^n u_i$, which describes independent random variables. Other relevant copulas are the Fréchet-Hoeffding bounds which we state in the following.

**Theorem 2** (Fréchet-Hoeffding Bounds ([23] Theorem 2.10.12)). Let $C$ be a copula. Then for every $u \in [0, 1]^n$

$$W(u) \leq C(u) \leq M(u) \quad (7)$$

with

$$W(u) = \max\{u_1 + \cdots + u_n - n + 1, 0\}, \quad (8)$$

$$M(u) = \min\{u_1, \ldots, u_n\}. \quad (9)$$
In the case that \( n = 2 \), \( W \) is a copula and two random variables whose joint distribution follows the copula \( W \) are called countermonotonic. The upper bound \( M \) is a copula for all \( n \) and random variables that follow \( M \) are called comonotonic [23]. The Fréchet-Hoeffding bounds are therefore a way to describe extreme positive and negative dependencies.

With these preliminary results, we are prepared to proceed and consider a simple scenario for the achievable ZOSC for the wiretap channel with two and one observation at the legitimate receiver and the eavesdropper, respectively.

3. Achievable ZOSC for the [2,1]-Wiretap Channel

First, we start with a simple scenario in which we consider two channels to Bob, modeled by the channel gains \( X_1 \) and \( X_2 \), and one channel to Eve, modeled by the channel gain \( Y \). We consider the case with coherent combining at Bob with secrecy rate \( R_S \). As a motivating example, let us consider Rayleigh fading on all channels, such that the channel gains to Bob are both standard exponential, i.e., \( X_1, X_2 \sim \text{Exp}(1) \). The channel gain to Eve is also exponentially distributed but with mean \( \mu \), i.e., \( Y \sim \text{Exp}(1/\mu) \).

We will now show the surprising result that it is possible to achieve a positive ZOSR for dependent channels even without perfect channel-state information at the transmitter (CSI-T).

**Theorem 3.** The wiretap channel with two channels to Bob, both with marginal standard exponential distribution, and one channel to Eve exponentially distributed with mean \( \mu \geq 0 \) can support a zero-outage secrecy rate

\[
\text{ZOSR} = \begin{cases} 
0 & \mu \geq 1 \\
\log_2(1/\mu) & 1 \geq \mu \geq \frac{1}{1+\ln(2)} \\
\min_{0 \leq U \leq 1} \log_2 \left( \frac{\ln(1/4-U^2)-1}{\ln(1-U)\mu-1} \right) & 1/1+\ln(2) > \mu.
\end{cases}
\]  

**Proof.** We start with the following first choice: \( X_1 \) and \( X_2 \) are counter-monotonic. This means that they are generated by one common uniform random variable \( U \sim U[0,1] \) by

\[
X_1 = F^{-1}(U), \quad X_2 = F^{-1}(1-U),
\]  

with inverse cumulative distribution function (CDF) \( F^{-1}(z) = -\ln(1-z) \). For the sum of \( X_1 \) and \( X_2 \) we obtain

\[
S = X_1 + X_2 = -\ln(1-U) - \ln(U) = -\ln(U(1-U)).
\]  

The CDF of \( S \) is computed as

\[
F_S(s) = \mathbb{P}(S \leq s) = \mathbb{P}(U(1-U) \geq \exp(-s)).
\]  

Solving the inequality in (13) for \( U \) gives two roots \( U_{1/2} = \frac{1}{2} \pm \sqrt{\frac{1}{4} - \exp(-s)} \). This allows to compute the CDF of \( S \) by

\[
F_S(s) = \int_{U_{1/2}}^{U_2} 1 \cdot ds = 2\sqrt{\frac{1}{4} - \exp(-s)} = \sqrt{1 - 4\exp(-s)}, \quad \text{for } s \geq 2\ln(2). \tag{14}
\]

Next, we proceed with the second choice: \( S \) and \( Y \) are co-monotonic. In this case, the two random variables are generated by a common uniform random variable \( U \sim U[0,1] \) as

\[
S = F_S^{-1}(U), \quad Y = F_Y^{-1}(U) \tag{15}.
\]

Therefore, the inverse CDF of \( S \) from (13) is given by

\[
F_S^{-1}(z) = \ln \left( \frac{4}{1-z^2} \right). \tag{16}
\]

The SOP using the inverse CDF of \( Y \) with \( F_Y^{-1}(z) = -\mu \ln(1-z) \) is computed as
\[ \epsilon = \mathbb{P}(\log_2(1+S) - \log_2(1+Y) \leq R) \]
\[ = \mathbb{P}\left( \log_2 \left( \frac{1 + F_{\gamma}^{-1}(U)}{1 + F_{\gamma}^{-1}(U)} \right) \leq R \right) \]
\[ = \mathbb{P}\left( F_{\gamma}^{-1}(U) - 2R F_{\gamma}^{-1}(U) \leq 2^R - 1 \right) \]
\[ = \mathbb{P}\left( \ln(4) - \ln(1-U^2) + 2^R \mu \ln(1-U) \leq 2^R - 1 \right) \]
\[ = \mathbb{P}\left( \frac{(1-U)\mu 2^R}{1-U^2} \leq \frac{1}{4} \exp(2^R - 1) \right). \quad (17) \]

Since we are interested in the ZOSR, the inequality inside (17) should not hold true for all \( 0 \leq U \leq 1 \). Therefore, the maximum ZOSR \( R \) has to fulfill
\[ \min_{0 \leq U \leq 1} \frac{(1-U)\mu 2^R}{1-U^2} \geq \frac{1}{4} \exp(2^R - 1). \quad (18) \]

Solving (18) with respect to \( R \) gives the following characterization of the ZOSR
\[ \text{ZOSR} = \min_{0 \leq U \leq 1} \log_2 \left( \frac{\ln(1-U^2) - 1 - \ln 4}{\mu \ln(1-U) - 1} \right). \quad (19) \]

If \( \mu \geq 1 \) the RHS in (19) is zero or negative. This indicates that the achievable ZOSR is zero if \( \mu \geq 1 \). For \( \mu \geq \frac{1}{1+\ln(2)} \), the RHS in (19) is monotonically decreasing with \( U \) and the minimum value is obtained for \( U \to 1 \). In this case, we have
\[ \text{ZOSR} = \lim_{U \to 1} \log_2 \left( \frac{\ln(1-U^2) - 1 - \ln 4}{\mu \ln(1-U) - 1} \right) = \log_2(1/\mu) \quad \text{for} \quad \mu \geq \frac{1}{1+\ln(2)}. \quad (20) \]

For \( 0 \leq \mu < \frac{1}{1+\ln(2)} \), the RHS in (19) has a minimum within \( 0 \leq U \leq 1 \) and the ZOSR has to be evaluated via (19). \( \square \)

**Remark 1.** It can be observed that the channel to Eve should be worse on average compared to the channels to Bob, i.e., \( \mu \leq 1 \), in order to get a positive ZOSR. This can be interpreted as the advantage of the legitimate link over the eavesdropper’s link.

We can easily extend the above scenario to the case where the eavesdropper has two observations, which both have an exponential marginal distribution with mean \( \mu \). For this extension, we have the following result on the achievable ZOSR.

**Corollary 1.** The wiretap channel with two channels to Bob, both with marginal standard exponential distribution and two channels to Eve, both with marginal exponential distribution with mean \( \mu \geq 0 \) can support a zero-outage secrecy rate
\[ \text{ZOSR} = [\log_2(1 + 2 \ln(2)) - \log_2(1 + 2 \ln(2)\mu)]^+. \quad (21) \]

**Proof.** The proof follows similar lines as the proof of Theorem 3. \( \square \)

We conjecture that the dependency structure which leads to the achievable ZOSR in Theorem 3 is optimal. The intuition behind the result in Theorem 3 is to separate the two dependencies, the one between the legitimate channel gains \( X_1, X_2 \), and the other between the resulting legitimate joint channel gains \( S_X = X_1 + X_2 \) and the eavesdropper channel gain \( Y \). We know from [24] that counter-monotonicity of \( X_1 \) and \( X_2 \) is the best case for the ZOC. The resulting sum \( S_X \) and the observation at Eve \( Y \) should be co-monotonic as will be shown in Lemma 1. Since a converse is not available yet, we proceed with the analysis of the ZOSR in the case of discrete alphabets.
4. An Equivalent Outage Problem Formulation for the [2,1]-Wiretap Channel

In this section, we first formulate equivalent expressions of the ZOSC for both cases where the channel gain is either continuous- or finite-alphabet. Then we solve the case in which the channel gain has finite alphabets from this equivalent expression.

An optimization problem to solve the ZOSC with continuous alphabet can be equivalently formulated as follows:

\[
P_0: \sup_{f_{X_1X_2Y} \in \mathcal{F}} \inf_{x_1,x_2,y \in \text{supp}(f_{X_1X_2Y})} \log_2 \left( \frac{1 + x_1 + x_2}{1 + y} \right)
\]
\[\text{s.t. } f_{X_1X_2Y}(x_1, x_2, y) > 0 \quad \text{for some } r > 0,
\]
\[f_{X_1X_2Y}(x_1, x_2, y) \text{ is cont. in the } r\text{-neighborhood of } (x_1^*, x_2^*, y^*) \quad \text{for some } r > 0,
\]

where a feasible set of joint probability density functions \( \mathcal{F} \) is defined as follows

\[\mathcal{F} := \left\{ f_{X_1X_2Y}(x_1, x_2, y) \mid f_{X_1X_2Y}(x_1, x_2, y) = 0, \text{ if } x_1 + x_2 < y, \right\}
\]
\[\int_{X_1 \times Y} f_{X_1X_2Y}(x_1, x_2, y) \, dx_2 \, dy = f_{X_1}(x_1),
\]
\[\int_{X_2 \times Y} f_{X_1X_2Y}(x_1, x_2, y) \, dx_1 \, dy = f_{X_2}(x_2),
\]
\[\int_{X_1 \times X_2} f_{X_1X_2Y}(x_1, x_2, y) \, dx_1 \, dx_2 = f_Y(y),
\]

where (25) is to avoid non-positive secrecy rate, (26)–(28) are used to guarantee that the marginals are fixed as the given ones \( \tilde{f}_{X_1}(x_1), \tilde{f}_{X_2}(x_2), \) and \( \tilde{f}_Y(y); (x_1^*, x_2^*, y^*) \) is the tuple optimizing (22) while fulfilling (23); (23) and (24) together are to guarantee that \( (x_1^*, x_2^*, y^*) \) occurs with a non-zero probability. In particular, a singular point in the probability density function (PDF) has a zero probability.

However, solving the functional optimization problem \( P_0 \) is involved. Therefore, instead of directly solving \( P_0 \), in the following, we first consider the case with discrete channel gains, which can be obtained from the continuous one by quantization. Afterward, we propose to use the rearrangement algorithm to solve the ZOSR.

**Discrete Alphabets**

We will now take a closer look at a simplified example where \( X_1, X_2, \) and \( Y \) are discrete random variables. In the simplest case, all of them are binary and either 0 or 1. The marginal distributions are again fixed and known. This yields the combinations and resulting secrecy capacities that are listed in Table 1. The joint probabilities of \( (X_1, X_2, Y) \) for each combination are given in the last column as \( F_{X_1X_2Y} \). First, since we want to achieve a positive ZOSC, we need to have zero probability for all combinations at which the secrecy capacity is zero. This leaves us with three degrees of freedom \( a, b, \) and \( c \), as listed in Table 1.

**Table 1.** A binary example.

| \( X_1 \) | \( X_2 \) | \( Y \) | Secrecy Capacity | \( F_{X_1X_2Y} \) |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | \( a \) |
| 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | \( b \) |
| 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1.585 | \( c \) |
| 1 | 1 | 1 | 0.585 | \( 1 - a - b - c \) |
From the fixed marginal distributions, we get the following conditions
\[ F_{X_1}(0) = a, \quad (29) \]
\[ F_{X_2}(0) = b, \quad (30) \]
\[ F_Y(0) = a + b + c, \quad (31) \]
which in turn yields
\[ c = F_Y(0) - F_{X_1}(0) - F_{X_2}(0). \]
Since \( c \) describes a joint probability, it needs to be non-negative and, therefore, the joint distribution in Table 1 is only valid for
\[ F_Y(0) \geq F_{X_1}(0) + F_{X_2}(0), \quad (32) \]
which is equivalent to
\[ E[X_1] + E[X_2] \geq 1 + E[Y] \quad (33) \]
in terms of the expected values. The ZOSC is then equal to \((\log_2(3) - \log_2(2)) \approx 0.585\).

In order to extend the above discussion to cases with general finite alphabet sizes, we first define two sets as follows:
\[ J := \{ j : \log_2(g(E_j)) \leq 0, \text{ where } g(E_j) := \frac{1 + E_{j,1} + E_{j,2}}{1 + E_{j,3}} \}, \quad (34) \]
\[ L := [1, |M|^3] - J, \quad (35) \]
where \( E \) is the \(|M|\)-ary expansion matrix, e.g., the rows of \( E \) in order are as \((x_1, x_2, y) = (0, 0, 0), (0, 0, 1), \ldots, (0, 0, |M| - 1), (0, 1, 0), \ldots, (|M| - 1, |M| - 1, |M| - 1)\), if \( M = \{0, 1, 2, \ldots, |M| - 1\} \). We then define a constant binary marginalization matrix \( A \in [0, 1]^{3|M| \times |M|^3} \), while the terminology comes from the fact that each row on the left hand side in the following expression
\[ Ap = P \quad (36) \]
is a marginalization to derive the marginal probability from the joint probability mass function (PMF), where the \( j \)-th entry of \( p \) is defined as follows
\[ p_j := E[\mathbb{I}_{E_j}], \quad (37) \]
which is the probability that the \( j \)-th row of \( E \) happens, \( j = 1, \ldots, |M|^3 \). \( P \) is a predefined marginal probability vector, which can be explicitly shown as follows:
\[ P := [P_1^T, P_2^T, \ldots, P_{|M|^3}^T]^T, \quad (38) \]
where \( P_k^T := [P_{X_1}(k - 1), P_{X_2}(k - 1), P_y(k - 1)], k = 1, \ldots, |M| \). Note that \( A \) is known due to the defined structure of \( E \). Note also that \( A_{i,j} = 0, \) if \( j \in J \) and then \( p_j \) will not be used in calculating the marginal probability \( P_i \), where \( P_i \) is the \( i \)-th row of \( P, i = 1, \ldots, 3|M| \).

Based on the above definitions, we can formulate the following optimization problem to derive the ZOSC:
\[ \mathbf{P1:} \quad \max_{\{p_i\}} \min \log_2 g(E_\ell) \quad (39) \]
s.t. \[ Ap = P \quad (40) \]
\[ \sum_{\ell \in L} p_\ell = 1 \quad (41) \]
\[ 0 \leq p_\ell \leq 1, \ell \in L, \quad (42) \]
where the objective function is to maximize the minimum instantaneous secrecy rate derived from all combinations of channel gains that have non-zero probabilities, by finding the PMF which fulfills the marginal probability constraint (40) and the feasibility constraints of the PMF (41) and (42). Note that \( p_I = 0 \), if \( l \in \mathcal{L}' \). Note also that we do not need to take \( k \in \mathcal{L}' \) into account in the objective function, since those \( E_l \) with \( l \in \mathcal{L}' \) will happen with probability zero, and do not affect the ZOSC.

Because \( E_l \) is an implicit function of \( \{p_{l_i}\}_{i \in \mathcal{L}} \) we transform \( \mathbf{P}_I \) in the following equivalent form. We first re-order the rows of \( \mathbf{E} \) such that values of the entries in \( \{\log_2 g(E_l)\}_{l \in \mathcal{L}} \) are in an increasing manner, where the PMF defined in (37) becomes \( \tilde{\mathbf{p}} \): \( \mathbf{P} = [p_{l_1}, p_{l_2}, \ldots, p_{l_{|\mathcal{L}'|}}] \).

The re-ordered \( \mathbf{E} \) is defined as \( \tilde{\mathbf{E}} \). Note that this re-ordering does not change the ZOSC since the joint distribution of the channel gains remains unchanged but just the indexing is changed. Then the equivalent problem when the ZOSC is non-zero, is described as follows:

\[
\mathbf{P}_I': \quad \min \quad L \tag{43}
\]
\[
\text{s.t.} \quad \tilde{A} \tilde{p} = \tilde{P} \tag{44}
\]
\[
\sum_{i \in \mathcal{L}} p_{l_i} = 1 \tag{45}
\]
\[
0 < p_{l_i} < 1, \quad i \in \mathcal{L} \tag{46}
\]
\[
3 |M| \leq L \leq |L| \tag{47}
\]

where \( \tilde{A} \) and \( \tilde{P} \) are column-wise and row-wise re-ordered from \( A \) and \( P \), respectively, due to the re-ordering of the rows of \( \mathbf{E} \), \( \tilde{\mathbf{p}} := \{p_{l_i}\}_{i \in \mathcal{L}'} \), \( \tilde{\mathcal{L}} := \{|L| - L + 1, \ldots, |L|\} \). Note that \(|\mathcal{L}| = L\), as the number of non-zero probabilities of the instantaneous secrecy rate, is lower bounded by the number of rows in \( \tilde{A} \), which results in the first inequality in (47). Otherwise, (44) will be over-determined. Please note that it may be possible that \( \mathbf{P}_I \) gives us the ZOSC as 0 and then there is no feasible solution from \( \mathbf{P}_I' \).

The formulation of \( \mathbf{P}_I' \) can be explained intuitively as follows: ZOSC increases with decreasing \(|\mathcal{L}| = L\) due to the fact that values in \( \{\log_2 g(E_l)\}_{l \in \mathcal{L}} \) are ordered in an increasing manner and if we decrease \( L \), the number of the smallest \(|\mathcal{L}| - L\) instantaneous secrecy rates being removed increases, which increases the ZOSC, as shown in (39). Then the smallest \( L \), namely \( L^* \), gives us the ZOSC as follows:

\[
\text{ZOSC} = \log_2 g(\tilde{E}_{|\mathcal{L}| - L^* + 1}) \tag{48}
\]

We define the ZOSC based on \( \{p_{l_i}\}_{i \in \mathcal{L}} \) as follows.

**Definition 2 (ZOSR and ZOSC).** Any feasible \( \{p_{l_i}\}_{i \in \mathcal{L}} \) results in an achievable ZOSR. The largest achievable ZOSR is the ZOSC.

Based on Definition 2 and given a PMF \( \{p_{l_i}\}_{i \in \mathcal{L}} \) which is feasible to (40)–(42), we can try to increase the achievable ZOSR as follows: We first define \( \hat{l} := \arg \min_{l \in \mathcal{L}} g(E_l) \). Then let the \( \hat{l} \)-th column of \( A \) as a zero vector. After that, we solve the corresponding \( \mathbf{P}_I \) again. This means that we re-allocate the non-zero probabilities to the instantaneous secrecy rates except the smallest one. If there exists a feasible PMF \( \{p_{l_i}'\} \) such that the resulting achievable ZOSR is larger than \( \ln g(E_l) \), then \( \frac{1}{2} \log_2 g(E_l) \) cannot be the ZOSC. In contrast, if there does not exist a feasible \( \{p_{l_i}'\} \), then \( \frac{1}{2} \log_2 g(E_l) \) is the ZOSC. Based on these steps, we solve \( \mathbf{P}_I' \) alternatively by using the following finite deterministic Algorithm 1. Note that even if \( A\tilde{p} = \tilde{P} \) is under-determined, after considering the constraints \( 0 \leq p_{l_i} \leq 1, j = 1, \ldots, |M|^3 \text{ and } \sum_{j=1}^{|M|^3} p_{l_i} = 1 \), the overall problem can also have no solution, depending on the initial values of \( \tilde{P} \).

When constructing an algorithm to solve \( \mathbf{P}_I' \), we should preset those joint probabilities whose corresponding instantaneous secrecy rates are the smallest to zero, such that the length of \( \tilde{\mathbf{p}} \) is the same as the number of rows of \( A \). Then we gradually increase the length.
of $\tilde{p}$, solve the constrained linear system, and see if we can have a feasible solution and then we stop.

Based on Algorithm 1, we can obtain the ZOSC as illustrated in Figure 2, where we consider the following marginal distributions:

- $\mathcal{M} = \{0, 1\}: P_X(0) = 0.2, P_X(1) = 0.8$.
- $\mathcal{M} = \{0, 1, 2\}: P_X(0) = 0.2, P_X(1) = 0.3, P_X(2) = 0.1$.
- $\mathcal{M} = \{0, 1, 2, 3\}: P_X(0) = 0.2, P_X(1) = 0.3, P_X(2) = 0.1, P_X(3) = 0.1$.
- $\mathcal{M} = \{0, 1, 2, 3, 4\}: P_X(0) = 0.2, P_X(1) = 0.3, P_X(2) = 0.1, P_X(3) = 0.1, P_X(4) = 0.1$.

In the following we prove the optimality of reaching ZOSC.

**Algorithm 1** Solve globally optimal ZOSC with channel gains from finite alphabet $\mathcal{M}$

0. Initialize the marginal distributions $P_X \in \mathbb{R}^{1 \times |\mathcal{M}|}$, $P_Y \in \mathbb{R}^{1 \times |\mathcal{M}|}$ and define $P := [P_X^T, P_Y^T]^T$.
1. Construct the $|\mathcal{M}|$-ary expansion matrix $E$, where each row of $E$ is a tuple $(x_1, x_2, y) \in \mathcal{M}^3$ (the 1st row is (0,0,0) and the proceedings follow an increasing order with respect to the $|\mathcal{M}|$-ary expansion).
2. Construct $A \in [0, 1]^{3 \times |\mathcal{M}|}$, where $A_{ij} = 0$, if by the $j$-th row of $E$, $x_1 + x_2 \leq y$ and $p_j$ is not used in calculating the marginal probability $P_j$, where $P_i$ is the $i$-row of $P$, $i = 1, \ldots, 3 \times |\mathcal{M}|$, $j = 1, \ldots, |\mathcal{M}|$. Define $L = 3 |\mathcal{M}|$.
3. Reorder $A$ and $E$ as $\hat{A}$ and $\hat{E}$, respectively, such that $\{1/2 \ln g(E_j)\}_{i \in \mathcal{L}}$ are in an increasing manner.

repeat
4. Update $\hat{A}$: set $\hat{A} = \hat{P}$, $0 < \hat{p}_i \leq 1$, $\sum p_i = 1$, $i \in \mathcal{L}$, by CVX.
5. Solve $\hat{A} \hat{p} = \hat{P}$, $0 < \hat{p}_i \leq 1$, $\sum p_i = 1$, $i \in \mathcal{L}$, by CVX.
6. Set $L = L + 1$.
until $\hat{A} \hat{p} = \hat{P}$ is feasible.
7. ZOSC $= \min_{(x_1, x_2, y) \in \mathcal{F}} \frac{1}{2} \left[ \log_2 (1 + x_1 + x_2) - \log_2 (1 + y) \right]$, where $\mathcal{F} := \{E_j\}$ if $p_j > 0$, $j = 1, \ldots, |\mathcal{M}|^3$.

![Figure 2](image-url) ZOSCs of the following alphabet sets $\mathcal{M}$: $\{0, 1\}$, $\{0, 1, 2\}$, $\{0, 1, 2, 3\}$, and $\{0, 1, 2, 3, 4\}$.

**Theorem 4.** Algorithm 1 computes the ZOSC for discrete alphabets in a finite number of steps.
Proof. We use the following steps to prove. First, in order to obtain a positive ZOSC, a number of entries of the probabilities whose indices belonged to \( J \) have to be set to zero. Then we use the programming problem \( \textbf{P}_1 \) to determine the ZOSC. We further transform problem \( \textbf{P}_1 \) into the equivalent programming problem \( \textbf{P}_1' \). The implementation in Algorithm 1 efficiently solves \( \textbf{P}_1' \). Note that the greedy-like algorithm guarantees to find the ZOSC instead of only a ZOSR. This is because, in the equivalent problem \( \textbf{P}_1 \), the secrecy rate is ordered and therefore, at each step the greedy algorithm in fact, accesses the global information to reach the global optimum. \( \square \)

Remark 2. Due to the affine and linear properties in the set of constraints, we can easily extend the setting of \( \textbf{P}_1' \) and Algorithm 1 to parallel channels.

Remark 3. When comparing secure systems to cases without secrecy constraint, we can observe an obvious difference in the optimal joint distribution. For the latter case, the ZOC happens when the channel gains are counter-monotonic. The missing counter- or co-monotonicity property is mainly due to the missing symmetry of the objective function with respect to the random variables.

5. Positive ZOSR for \( [n_B, n_E] \)-Wiretap Channels

After exploring a particular dependency structure to achieve a positive ZOSR for \( n_B = 2 \) and \( n_E = 1 \) in Section 3, we will now generalize the approach to multiple observations at Bob and Eve.

First, recall that the secrecy capacity \( C_S \) in this case is given by (3) as

\[
C_S = \log_2 \left( \frac{1 + S_B}{1 + S_E} \right),
\]

(49)

where we introduce the shorthand notations \( S_B = \sum_{i=1}^{n_B} X_i \) and \( S_E = \sum_{i=1}^{n_E} Y_i \).

In order to specify an appropriate joint distribution for a positive ZOSR, we need the following observation.

Lemma 1. For fixed distributions of \( S_B \) and \( S_E \), the ZOSR in (49) is maximized for comonotonic \( S_B \) and \( S_E \), i.e., for

\[
S_B = F_{S_B}^{-1}(U) \quad \text{and} \quad S_E = F_{S_E}^{-1}(U),
\]

(50)

with \( U \sim U[0,1] \).

Proof. Assuming fixed joint distributions of Bob’s and Eve’s channel gains, respectively, we obtain fixed distributions of \( S_B \) and \( S_E \). Based on (5), the ZOSR can then be formulated as

\[
\text{ZOSR} = \sup_{s} \{ s \mid \mathbb{P}(\log_2(1+S_B) - \log_2(1+S_E) \leq s) = 0 \}.
\]

(51)

We can rewrite this optimization problem as

\[
\text{ZOSR} = \sup_{s} \{ s \mid \mathbb{P}(\hat{S}_B + \hat{S}_E \leq s) = 0 \},
\]

(52)

where we use

\[
\hat{S}_B = \log_2(1+S_B), \quad \hat{S}_E = -\log_2(1+S_E).
\]

Since the inner function is now a sum, we can apply ([25] Theorem 3.1) and derive that (52) is solved for counter-monotonic \( \hat{S}_B \) and \( \hat{S}_E \), i.e., for \( \hat{S}_B = F_{\hat{S}_B}^{-1}(U) \) and \( \hat{S}_E = F_{\hat{S}_E}^{-1}(1-U) \), with \( U \sim U[0,1] \).
It is straightforward to see that \( F_{SB}^{-1}(U) = \log_2 \left( 1 + F_{SB}^{-1}(U) \right) \). For \( S_E \), we get
\[
F_{S_E}^-(s) = \mathbb{P}(S_E \geq 2^{-s} - 1) = 1 - F_{S_E}(2^{-1} - 1)
\]
and thus
\[
F_{S_E}^{-1}(U) = -\log_2 \left( 1 + F_{S_E}^{-1}(1 - U) \right).
\]
Therefore, for counter-monotonic \((S_B, S_E)\), we get
\[
F_{SB}^{-1}(U) = \log_2 \left( 1 + F_{SB}^{-1}(U) \right)
\]
\[
F_{S_E}^{-1}(1 - U) = -\log_2 \left( 1 + F_{S_E}^{-1}(U) \right),
\]
i.e., co-monotonic \((S_B, S_E)\).

Based on Lemma 1, we next fix the dependency structure in the following way, in order to achieve a positive ZOSR.

1. First, we find the joint distribution between Bob’s channels \(X_1, \ldots, X_{n_S}\) that maximizes the ZOC. The simple reason behind this first step is that we cannot find a positive ZOSC, if we do not have a positive ZOC to the legitimate receiver. In fact, the ZOSC is upper bounded by the ZOC to Bob.

2. Next, we find the same dependency structure for Eve’s channels \(Y_1, \ldots, Y_{n_E}\) that maximizes the ZOC. It may seem counter-intuitive to choose a joint distribution for which \(S_E\) is always greater than a positive constant. However, the reasoning behind this particular choice is to balance the realizations of Eve’s channels such that only little probability mass is placed on high realizations of \(S_E\). Otherwise, there could be a positive probability that \(S_E > S_B\), which would result in a ZOC of zero. It should be emphasized that this is a particular choice for this scheme and might not be the optimal dependency for the general case.

3. Finally, we set \(S_B\) and \(S_E\) as co-monotonic in order to maximize the ZOSR for fixed \(F_{S_B}\) and \(F_{S_E}\) as shown in Lemma 1.

It is apparent that the first two steps are difficult to solve in general [18]. However, there exists a RA [26] that can be used to approximate the ZOC along with the corresponding joint distribution. In the following, we apply the RA to solve the optimization problems
\[
\min_{r \in X \sim F_i} F_{X_1 + \cdots + X_d}(r) \quad \text{and} \quad \max_{r \in X \sim F_i} F_{X_1 + \cdots + X_d}(r),
\]
as shown in [26]. In particular, we apply the RA to solve Steps 1 and 2 from above.

The idea behind the RA is to find a multi-variate version of counter-monotonicity between multiple random variables [27]. Due to the numerical nature of the algorithm, we first need to introduce some required approximations and notations. Detailed explanations of the algorithm and individual steps, which are described in the following, can be found in [26].

Given a matrix \(A \in \mathbb{R}^{N \times n}\), we obtain the matrix \(A_{(-j)} \in \mathbb{R}^{N \times n-1}\) by deleting the \(j\)-th column \(A_{(j)}\) from \(A\). Each column of the matrix represents a random variable \(X_i\) with given marginal distribution \(F_{X_i}\). This is achieved by quantizing the CDF into \(N\) steps by the following two ways
\[
\varrho_{i,j} = F_{X_i}^{-1} \left( \frac{i-1}{N} \right) \quad \text{and} \quad \pi_{i,j} = F_{X_i}^{-1} \left( \frac{i}{N} \right), \quad 1 \leq i \leq N.
\]
This yields the matrices \(A\) and \(\overline{A}\), respectively. The quantization \(\varrho_{i,j}\) serves as a lower bound on \(F_{X_i}\), while \(\pi_{i,j}\) is an upper bound. It can be seen that the quantization becomes closer
to the original CDF with increasing $N$. Starting with the initial matrices $A$ and $A^*$, these matrices are rearranged iteratively such that in each step the $j$-th column $A_{(j)}$ is oppositely ordered to the row-wise sum of $A_{(-j)}$. This opposite rearrangement makes the random variables represented by $A_{(j)}$ and the sum of $A_{(-j)}$ countermonotonic. The rearrangement step is repeated for each column until convergence. The final output of the RA are the matrices $A^*$ and $A^*$ resulting from the rearrangement of $A$ and $A$, respectively.

Each row of $A^*$ and $A^*$ represents an $n$-dimensional point of the joint distribution function of $(X_1, \ldots, X_n)$. From this approximation of the optimal joint distribution, the final approximation of the ZOC is derived.

The algorithm was originally developed to calculate bounds on the distribution of functions of dependent risks [28] and it is applied in the area of actuarial science and quantitative risk management [26]. In communications, it has already been used to numerically approximate the best and worst case ergodic capacity for dependent fading channels [29].

The source code to reproduce all of the following numerical results can be found at [30]. The RA is implemented in Python [31] based on [32].

**Remark 4.** The idea of achieving a positive ZOC is closely connected to the concept of joint mixability [27,33]. If the fading gains would be jointly mixable, their sum would almost surely add up to a constant, i.e., the overall fading becomes deterministic. If this is possible for both Bob’s and Eve’s channels, the resulting secrecy capacity would be a constant, i.e., it corresponds to the ZOSC. Unfortunately, distributions with one-sided unbounded support can not be jointly mixable ([33] Rem. 2.2), which includes most of the common fading gain distributions. It should be noted that the scheme described above only finds an achievable positive ZOSR, which might not be the maximum. When taking the joint distribution of all channel gains into account—without separately optimizing Bob’s and Eve’s joint distributions—there might arise a similar mixability structure where high realizations of $Y_i$ are compensated by high realizations of $X_i$, resulting in a constant secrecy rate.

**Example: Rayleigh Fading**

In order to demonstrate the effectiveness of the RA, we now consider the scenario of homogeneous Rayleigh fading, analogue to Section 3. In this case, all $n_B$ channel gains to Bob are distributed according to an exponential distribution with mean 1, i.e., $X_i \sim \text{Exp}(1)$ for all $i = 1, \ldots, n_B$. In order to reflect an SNR difference between Bob and Eve, we assume that the channel gains of Eve’s channels have mean $\mu$, i.e., $Y_i \sim \text{Exp}(1/\mu)$ for all $i = 1, \ldots, n_E$.

In Figure 3, we show the calculated ZOSRs over the number of Eve’s antennas $n_E$ using the RA with the scheme described above. The results are presented for multiple values of $\mu$ and $n_B$. The first expected observation is that the ZOSR decreases with an increasing number of antennas at Eve, while it increases when $n_B$ is increased. Similarly, if the channel quality of Eve’s channels $\mu$ improves, the achievable ZOSR decreases. Interestingly, the slope of decreasing ZOSR is steeper for $n_E > n_B$, which is particularly visible in Figure 3 for $n_B = 4$. It can also be seen that the ZOSR is equal to zero above a certain number of antennas at Eve, depending on $n_B$ and $\mu$. However, the results in Figure 3 demonstrate that it is generally possible to find joint distributions supporting a positive ZOSR by applying the RA. It should also be noted that this is not limited to the homogeneous case, but arbitrary marginal distributions are supported.

**Remark 5.** As described at the beginning of this section, the RA returns a lower and an upper bound on the exact value. The results in Figure 3 are obtained with $N = 10^4$ quantization steps. With this number of quantization steps, the resulting bounds from the RA cannot be distinguished in Figure 3 and are therefore shown as one single curve.
6. Conclusions and Future Work

In this paper, we consider the setting that there are two paths from the transmitter to the legitimate receiver and one path (or multiple co-monotonic paths) to the eavesdropper. We show that we can achieve a zero SOP for some positive secrecy rate by introducing a proper dependence structure among the fading gains of the three paths. Thereby, we can achieve a non-zero ZOSR. To better understand the underlying dependence structure, we further consider the case where the channel gains are from finite alphabets and systematically and globally solve the zero outage secrecy capacity. In order to obtain positive ZOSR, an advantage in terms of average channel gains must exist. In addition, the results are underlined with numerical constructions by the RA to solve the ZOSR for continuous channel gains. The generalized results to multiple observations at Bob and Eve indicate that positive ZOSR can be achieved if the legitimate link has an advantage in terms of the number of observations and the average channel gains.

For future work, we have the open problem to determine the global optimal dependency structure for the continuous distributions. We conjecture that the dependency structure that leads to Theorem 3 is the global optimal to maximize the ZOSR. Another open question is how to connect the model and results for the discrete alphabet case to the continuous distribution case. Furthermore, the construction of an improved algorithm for the multi-observation case based on joint mixability and tail distribution analyses is open for future work, too.

The last but not the least point for the future work is on how to practically implement the designed joint distribution. RIS [34], a recently hot research topic, shows the high possibility of manipulating the channels, artificially. However, the inter-relation between the fundamental properties of RIS and the designed joint distribution is still missing, which can be a critical issue to achieve our design goal discussed in this paper.

Author Contributions: Writing—original draft, E.J., P.-H.L. and K.-L.B. All authors have read and agreed to the published version of the manuscript.

Funding: The work of K.-L. Besser is supported in part by the German Research Foundation (DFG) under grant JO 801/23-1. The work of E. Jorswieck is supported in part by the German Research Foundation (DFG) under grant JO 801/25-1.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.
Data Availability Statement: The source code of all used algorithms and calculations is publicly available under the GPLv3 license at [30]. This allows reproducing all of the presented results.

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

Abbreviations
The following abbreviations are used in this manuscript:

- AWGN: additive white Gaussian noise
- CDF: cumulative distribution function
- CSI: channel-state information
- CSI-T: channel-state information at the transmitter
- PDF: probability density function
- PMF: probability mass function
- RA: rearrangement algorithm
- RIS: reconfigurable intelligent surface
- SISO: single-input single-output
- SNR: signal-to-noise ratio
- SOP: secrecy outage probability
- ZOC: zero-outage capacity
- ZOSC: zero-outage secrecy capacity
- ZOSR: zero-outage secrecy rate

References
1. Saad, W.; Bennis, M.; Chen, M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. *IEEE Netw.* 2019, 34, 134–142. [CrossRef]
2. Bloch, M.; Barros, J. *Physical-Layer Security*; Cambridge University Press: Cambridge, UK, 2011. [CrossRef]
3. Gidney, C.; Ekerå, M. How to factor 2048 bit RSA integers in 8 h using 20 million noisy qubits. *Quantum* 2021, 5, 433. [CrossRef]
4. Gungor, O.; Tan, J.; Koksal, C.E.; El-Gamal, H.; Shroff, N.B. Secrecy Outage Capacity of Fading Channels. *IEEE Trans. Inf. Theory* 2013, 59, 5379–5397. [CrossRef]
5. Bloch, M.; Barros, J.; Rodrigues, M.R.D.; McLaughlin, S.W. Wireless Information-Theoretic Security. *IEEE Trans. Inf. Theory* 2008, 54, 2515–2534. [CrossRef]
6. Gopala, P.K.; Lai, L.; El Gamal, H. On the Secrecy Capacity of Fading Channels. *IEEE Trans. Inf. Theory* 2008, 54, 4687–4698. [CrossRef]
7. Zhao, H.; Liu, Y.; Sultan-Salem, A.; Alouini, M.S. A Simple Evaluation for the Secrecy Outage Probability Over Generalized-K Fading Channels. *IEEE Commun. Lett.* 2019, 23, 1479–1483. [CrossRef]
8. Biglieri, E.; Lai, I.W. The impact of independence assumptions on wireless communication analysis. In Proceedings of the 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, Spain, 10–15 July 2016; pp. 2184–2188. [CrossRef]
9. Liang, Y.; Poor, H.V.; (Shitz), S.S. Information Theoretic Security. *Found. Trends Commun. Inf. Theory* 2009, 5, 355–580. [CrossRef]
10. Peters, G.W.; Myrvoll, T.A.; Matsui, T.; Nevat, I.; Septier, F. Communications meets copula modeling: Non-standard dependence features in wireless fading channels. In Proceedings of the 2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Atlanta, GA, USA, 3–5 December 2014; pp. 1224–1228. [CrossRef]
11. Lee, W.Y. Effects on correlation between two mobile radio base-station antennas. *IEEE Trans. Veh. Technol.* 1973, 22, 130–140. [CrossRef]
12. Jeon, H.; Kim, N.; Choi, J.; Lee, H.; Ha, J. Bounds on Secrecy Capacity Over Correlated Ergodic Fading Channels at High SNR. *IEEE Trans. Inf. Theory* 2011, 57, 1975–1983. [CrossRef]
13. Sun, X.; Wang, J.; Xu, W.; Zhao, C. Performance of Secure Communications Over Correlated Fading Channels. *IEEE Signal Process. Lett.* 2012, 19, 479–482. [CrossRef]
14. Liu, X. Outage Probability of Secrecy Capacity over Correlated Log-Normal Fading Channels. *IEEE Commun. Lett.* 2013, 17, 289–292. [CrossRef]
15. Alexandropoulos, G.C.; Peppas, K.P. Secrecy Outage Analysis Over Correlated Composite Nakagami-m/Gamma Fading Channels. *IEEE Commun. Lett.* 2018, 22, 77–80. [CrossRef]
16. Ghadi, F.R.; Hodtani, G.A. Copula-Based Analysis of Physical Layer Security Performances Over Correlated Rayleigh Fading Channels. *IEEE Trans. Inf. Forensics Secur.* 2021, 16, 431–440. [CrossRef]
17. Besser, K.L.; Jorswieck, E.A. Bounds on the Secrecy Outage Probability for Dependent Fading Channels. *IEEE Trans. Commun.* 2021, 69, 443–456. [CrossRef]
18. Besser, K.L.; Lin, P.H.; Jorswieck, E.A. On Fading Channel Dependency Structures with a Positive Zero-Outage Capacity. *IEEE Trans. Commun.* 2021, 69, 6561–6574. [CrossRef]
19. Besser, K.L.; Jorswieck, E.A. Reliability Bounds for Dependent Fading Wireless Channels. *IEEE Trans. Wirel. Commun.* 2020, 19, 5833–5845. [CrossRef]

20. Mucchi, L.; Jayousi, S.; Caputo, S.; Panayirci, E.; Shahabuddin, S.; Bechtold, J.; Morales, I.; Stoica, R.A.; Abreu, G.; Haas, H. Physical-Layer Security in 6G Networks. *IEEE Open J. Commun. Soc.* 2021, 2, 1901–1914. [CrossRef]

21. Basar, E.; Poor, H.V. Present and Future of Reconfigurable Intelligent Surface-Empowered Communications [Perspectives]. *IEEE Signal Process. Mag.* 2021, 38, 146–152. [CrossRef]

22. Khisti, A.; Wornell, G.W. Secure Transmission With Multiple Antennas—Part II: The MIMO Wiretap Channel. *IEEE Trans. Inf. Theory* 2010, 56, 5515–5532. [CrossRef]

23. Mucchi, L.; Jayousi, S.; Caputo, S.; Panayirci, E.; Shahabuddin, S.; Bechtold, J.; Morales, I.; Stoica, R.A.; Abreu, G.; Haas, H. Physical-Layer Security in 6G Networks. *IEEE Open J. Commun. Soc.* 2021, 2, 1901–1914. [CrossRef]

24. Jorswieck, E.; Lin, P.H. Ultra-Reliable Multi-Connectivity with Negatively Dependent Fading Channels. In Proceedings of the 2019 16th International Symposium on Wireless Communication Systems (ISWCS), Oulu, Finland, 27–30 August 2019; pp. 373–378. [CrossRef]

25. Frank, M.J.; Nelsen, R.B.; Schweizer, B. Best-possible Bounds for the Distribution of a Sum—A Problem of Kolmogorov. *Probab. Theory Relat. Fields* 1987, 74, 199–211. [CrossRef]

26. Embrechts, P.; Puccetti, G.; Rüschendorf, L. Model uncertainty and VaR aggregation. *J. Bank. Financ.* 2013, 37, 2750–2764. [CrossRef]

27. Puccetti, G.; Wang, R. Extremal Dependence Concepts. *Stat. Sci.* 2015, 30, 485–517. [CrossRef]

28. Puccetti, G.; Rüschendorf, L. Computation of sharp bounds on the distribution of a function of dependent risks. *J. Comput. Appl. Math.* 2012, 236, 1833–1840. [CrossRef]

29. Besser, K.L.; Jorswieck, E.A. Calculation of Bounds on the Ergodic Capacity for Fading Channels with Dependency Uncertainty. In Proceedings of the ICC 2021—2021 IEEE International Conference on Communications (ICC), Montreal, QC, Canada, 14–23 June 2021.

30. Besser, K.L.; Lin, P.H. Zero-Outage Secrecy-Capacity of Dependent Fading Wiretap Channels—Supplementary Material. Available online: https://gitlab.com/klb2/zero-outage-secrecy-capacity (accessed on 16 November 2021).

31. Besser, K.L. Rearrangement Algorithm: Python Implementation. Version 0.1.1. Available online: https://pypi.org/project/rearrangement-algorithm/ (accessed on 28 October 2021).

32. Hofert, M. Implementing the Rearrangement Algorithm: An Example from Computational Risk Management. *Risks* 2020, 8, 47. [CrossRef]

33. Wang, B.; Wang, R. Joint Mixability. *Math. Oper. Res.* 2016, 41, 808–826. [CrossRef]

34. Di Renzo, M.; Debbah, M.; Phan-Huy, D.T.; Zappone, A.; Alouini, M.S.; Yuen, C.; Sciancalepore, V.; Alexandropoulos, G.C.; Hoydis, J.; Gacanin, H.; et al. Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come. *EURASIP J. Wirel. Commun. Netw.* 2019, 2019, 129. [CrossRef]