Abstract—We propose a new framework for determining the wiretap code rates of single-input single-output multi-antenna eavesdropper (SISOME) wiretap channels when the capacity of the eavesdropper’s channel is not available at the transmitter. In our framework we introduce the effective secrecy throughput (EST) as a new performance metric that explicitly captures the two key features of wiretap channels, namely, reliability and secrecy. Notably, the EST measures the average rate of the confidential information transmitted from the transmitter to the intended receiver without being eavesdropped on. We provide easy-to-implement methods to determine the wiretap code rates for two transmission schemes: 1) adaptive transmission scheme in which the capacity of the main channel is available at the transmitter and 2) fixed-rate transmission scheme in which the capacity of the main channel is not available at the transmitter. Such determinations are further extended into an absolute-passive eavesdropping scenario where even the average signal-to-noise ratio of the eavesdropper’s channel is not available at the transmitter. Notably, our solutions for the wiretap code rates do not require us to set reliability or secrecy constraints for the transmission within wiretap channels.

Index Terms—Physical layer security, wiretap code, wiretap channels, effective secrecy throughput, passive eavesdropping.

I. INTRODUCTION

Physical layer security for wireless communications is of growing importance since it can guarantee the information secrecy regardless of an eavesdropper’s computational capability and it eliminates the key distribution and management required by traditional cryptographic techniques [1–5]. In the pioneering studies [6–8], a wiretap channel was proposed as the fundamental model to characterize physical layer security. In the wiretap channel, an eavesdropper (Eve) attempts to intercept the communication between a transmitter (Alice) and an intended receiver (Bob). The prerequisite to achieve physical layer security is that the capacity of the channel between Alice and Bob (henceforth referred to as the main channel) is larger than the capacity of the channel between Alice and Eve (henceforth referred to as the eavesdropper’s channel).

From the perspective of wiretap code design, the knowledge of the capacities of the main channel and the eavesdropper’s channel is required at Alice in order to guarantee perfect secrecy [10]. In fact, perfect secrecy has two requirements: (i) the error probability at Bob decreases with increasing code length, and (ii) the fraction of information leakage to Eve decreases with increasing code length. These two requirements are denoted as the reliability constraint and the secrecy constraint, respectively [10–12]. A wiretap code can be designed by choosing two code rates, namely, the codeword rate, \( R_B \), and the rate of transmitted confidential information (or equivalently, the target secrecy rate), \( R_s \) [10, 11]. The redundancy rate, \( R_E = R_B - R_s \), is used to confuse Eve. In order to guarantee the reliability constraint of wiretap channels, the rate of transmitted codewords has to be chosen as \( R_B \leq C_B \), where \( C_B \) is the capacity of the main channel. In order to guarantee the secrecy constraint of wiretap channels, the redundancy rate has to be chosen as \( R_E > C_E \), where \( C_E \) is the capacity of the eavesdropper’s channel. If the values of both \( C_B \) and \( C_E \) are available at Alice, the maximum target secrecy rate is achievable, which is referred to as the secrecy capacity of a wiretap channel and is given by \( C_s = C_B - C_E \) [13–16]. However, the assumption that \( C_E \) is available at Alice is too strong since in practice Eve may not feed back her channel state information (CSI) to Alice. In addition, in practice Alice may not know \( C_B \) since Bob may not feed back \( C_B \) to Alice due to the limited feedback overhead supported by the main channel\(^1\).

We note that it is impossible for Alice to guarantee \( R_E > C_E \) and fulfill the secrecy constraint in the case where only the statistical knowledge of the eavesdropper’s channel is available at Alice. In this case, the performance of wiretap channels has been characterized in terms of the ergodic secrecy capacity [13, 17], and in terms of the existing secrecy outage probability, i.e., \( \Pr(C_s < R_s) \) [18–22]. It is important to point out that the ergodic secrecy capacity is an average performance metric, and thus cannot be utilized to set \( R_B \) or \( R_E \). The use of the existing secrecy outage probability in determining \( R_B \) or \( R_E \) has the drawback that it does not separate the quality of service (reliability requirements) from the secrecy requirements.

In this paper, we propose a new framework to determine the wiretap code rates when the capacity of the eavesdropper’s channel is not available at Alice.

\(^1\)The number of bits required to feed back \( C_B \) from Bob to Alice depends on the quantization accuracy of \( C_B \).
channel is not available at Alice. Our framework is based on a new metric, referred to as the effective secrecy throughput (EST), which explicitly captures both the reliability constraint and the secrecy constraint of wiretap channels. The EST measures the average rate of the confidential information transmitted from Alice to Bob without being eavesdropped on. As we will discuss in more details later, the key attribute of our new metric is that it encapsulates the main features of the wiretap channel, yet can be applied to a variety of transmission schemes.

In our proposed framework we provide easy-to-implement methods to determine the wiretap code rates that achieve the locally maximum EST for two system models. (i) The first model is a high complexity system where Bob feeds back the capacity of the main channel to Alice. We refer to the transmission scheme under this system model as the adaptive transmission scheme since Bob adaptively adjusts his wiretap code rates according to $C_B$. (ii) The second model is a low complexity system where Bob does not feed back the capacity of the main channel to Alice. We refer to the transmission scheme under this system model as the fixed-rate transmission scheme since Bob has to fix his wiretap code rates when $C_B$ and $C_E$ are unavailable. In the above two models, we assume that the average signal-to-noise ratio (SNR) of the eavesdropper’s channel is available at Alice. In order to relax this assumption, we consider an absolute-passive eavesdropping scenario where the average SNR of the eavesdropper’s channel is unavailable at Alice. For this latter scenario, we derive closed-form expressions for the average EST of the adaptive and the fixed-rate transmission schemes, based on which the wiretap code rates of these two schemes can be determined.

The rest of this paper is organized as follows. Section II details the system model and the proposed new framework for determining the wiretap code rates. In Section III, the determination of the redundancy rate $R_E$ for the adaptive transmission scheme is presented. Section IV presents the determination of $(R_B, R_E)$ for the fixed-rate transmission scheme. In Section V, we extend the determination of the wiretap code rates into an absolute-passive eavesdropping scheme based on a proposed annulus threat model. Numerical results are provided in Section III, Section IV, and Section V in order to verify our analysis and provide useful insights into our solutions. Finally, Section VI draws some concluding remarks.

Notation: Scalar variables are denoted by italic symbols. Vectors and matrices are denoted by lower-case and upper-case boldface symbols, respectively. Given a complex vector $x$, $\|x\|$ denotes the Euclidean norm. The $m \times m$ identity matrix is referred to as $I_m$ and $E[\cdot]$ denotes expectation.

II. SYSTEM MODEL AND NEW FRAMEWORK

In this section, we detail our system model and the new framework for determining wiretap code rates ($R_B$ and $R_E$) using the proposed EST.

A. System Model

The wiretap channel of interest is where the transmitter (Alice) and the intended receiver (Bob) are equipped with a single antenna each, and the eavesdropper (Eve) is equipped with $N_E$ antennas. This wiretap channel is referred to as the single-input single-output multi-antenna eavesdropper (SISOME) wiretap channel. We note that the deployment of multiple antennas at the eavesdropper is more conservative (from a security viewpoint) than the deployment of a single antenna at the eavesdropper. This is due to the fact that the transmitter cannot fully control the number of antennas at Eve.

We assume that the main channel and the eavesdropper’s channel are subject to independent quasi-static Rayleigh fading with equal block length. We also assume that Bob possesses the full knowledge of the instantaneous CSI of the main channel, but Alice only knows the average SNR of the main channel. We further assume that Eve knows the instantaneous CSI of the eavesdropper’s channel. As such, Eve applies maximum ratio combining (MRC) [23–25] to combine the received signals in order to exploit the $N_E$-antenna diversity and maximize the probability of successful eavesdropping. This is due to the fact that when Alice transmits a single data stream, the maximum output SNR of the eavesdropper’s channel is achieved at Eve if Eve adopts MRC. In our system model, Alice and Bob are equipped with a single antenna each and therefore Alice transmits a single data stream to Bob.

The received signal at Bob is given by

$$y_B = hx + n_B,$$  \hspace{1cm} (1)

where $h$ is the complex coefficient of the main channel with Rayleigh fading, $x$ is the transmit signal, and $n_B$ is the Gaussian noise of the main channel with zero mean and variance $\sigma_B^2$. The transmit power constraint is given by $E[|x|^2] = P_A$, where $P_A$ is the total transmit power. Based on (1), the instantaneous SNR at Bob is obtained as

$$\gamma_B = \frac{|h|^2 P_A}{\sigma_B^2},$$  \hspace{1cm} (2)

which indicates that $\gamma_B$ follows an exponential distribution with $1/\tau_B$ as the rate parameter, where $\tau_B = E[\gamma_B]$.

The $N_E \times 1$ received signal vector at Eve is given by

$$y_E = gx + n_E,$$  \hspace{1cm} (3)

where $g$ is the $N_E \times 1$ eavesdropper’s channel vector with independent and identically distributed (i.i.d.) Rayleigh fading entries, and $n_E$ is circularly symmetric complex Gaussian noise vector of the eavesdropper’s channel with zero mean and covariance matrix $I_{N_E} \sigma_E^2$. Applying MRC to exploit the $N_E$-antenna diversity at Eve, the instantaneous SNR at Eve is obtained as

$$\gamma_E = \frac{\|g\|^2 P_A}{\sigma_E^2},$$  \hspace{1cm} (4)

which indicates that $\gamma_E$ follows a Gamma distribution with $N_E$ and $\tau_E = E[\gamma_E]/N_E$ as the shape and scale parameters, respectively.
B. New Framework for Determining Wiretap Code Rates

In wiretap channels, Alice intends to send the confidential information to Bob with a high transmission rate while guaranteeing both the reliability constraint and secrecy constraint. However, if the capacity of the eavesdropper’s channel is not available at Alice, the secrecy constraint cannot be guaranteed and a secrecy outage may occur. We define the secrecy outage probability as

\[ O_s(R_E) = \Pr(R_E < C_E). \]  

We note that \( O_s(R_E) \) is different from the existing secrecy outage probability, \( \Pr(C_s < R_s) \), since the latter includes not only the secrecy outage probability but also the reliability outage probability. As such, it is not exactly precise to name \( \Pr(C_s < R_s) \) as the secrecy outage probability.

Likewise, if the capacity of the main channel is not available at Alice, the reliability constraint cannot be guaranteed and thus a reliability outage may occur. We define the reliability outage probability as

\[ O_r(R_B) = \Pr(R_B > C_B). \]  

Based on (6), we can see that the reliability constraint can be guaranteed if \( C_B \) is available at Alice.

Incorporating both the secrecy outage probability and reliability outage probability, we present the EST in the following definition.

**Definition 1:** The EST (bit/channel) of a wiretap channel is defined as

\[ \Psi(R_B, R_E) = (R_B - R_E) \left[ 1 - O_r(R_B) \right] \left[ 1 - O_s(R_E) \right]. \]  

In order to explicitly explain the physical meaning of the EST of a wiretap channel, we present a schematic of secure transmissions within multiple fading blocks in Fig. 1. In (7), \( (R_B - R_E) \) quantifies the rate of transmitted confidential information \( R_c \) (represented by a blue block at Alice in Fig. 1), while \( \left[ 1 - O_r(R_B) \right] \left[ 1 - O_s(R_E) \right] \) quantifies the probability that the information is securely transmitted from Alice to Bob. In Fig. 1, the reliability outage probability corresponds to the probability that Bob receives a yellow block, and the secrecy outage probability corresponds to the probability that Bob receives a red block. Therefore, the EST quantifies the average secrecy rate at which the messages are transmitted from Alice to Bob without being leaked to Eve (i.e., the EST quantifies the average number of the blue blocks achieved at Bob over a large number of fading realizations). Accordingly, the EST tells us the average rate of messages that can be securely transmitted. In the following sections, we determine values of the wiretap code rates (i.e., \( R_B, R_E \)) for the adaptive and fixed-rate transmission schemes.

Knowing the average rate of confidential messages is of practical significance for the passive eavesdropping scenario, since it indicates to us how much secure data can be transmitted on average over a given period of time in a wiretap channel. We note that we cannot identify which message is secure and which is not. We would clarify that this is not due to the use of the EST, but is due to the adopted eavesdropping scenario. In our adopted scenario the instantaneous channel knowledge of Eve is not available at Alice, which leads to the fact that it is impossible to guarantee perfect secure transmission between Alice and Bob (i.e., secrecy outage possibly occurs). Due to this, previous studies adopted the secrecy outage probability (e.g., [19, 21, 26]) and/or the throughput (e.g., [27–29]) as the performance metrics. We note that the average rate of confidential messages cannot be readily evaluated by either the secrecy outage probability or the throughput. As such, the EST is more informative and is of more practical operational significance to Bob in some circumstances. For example, Bob may maximize the EST without any bound on the secrecy outage probability or the throughput.

We note here the work of [27] focused on an on-off transmission scheme for the wiretap channel and introduced a new metric that is motivated by a desire to disentangle reliability and secrecy features. The approach used in [27] is based on a new secrecy outage probability defined through a conditional probability. This is quite different from the approach adopted here where we directly maximize a key throughput rate of the wiretap channel - the EST. Importantly, our technique does not target any transmission scheme in particular and therefore is directly applicable to a wide range of schemes and system models.

III. DETERMINATION OF REDUNDANCY RATE FOR ADAPTIVE TRANSMISSION SCHEME

In this section, we first derive a closed-form expression for the EST of the adaptive transmission scheme, based on which we provide an easy-to-implement method to determine the redundancy rate \( R_E \) that achieves a locally maximum EST for this scheme. We note that applying the adaptive transmission scheme requires the capacity of the main channel to be available at Alice. As such, the complexity of the system where the adaptive transmission scheme can be applied is high since Bob has to feed back \( C_B \) to Alice.

A. Adaptive Transmission Scheme

In the adaptive transmission scheme, \( C_B \) is available at Alice and \( R_B \) is chosen as \( R_B = C_B \). As such, to design
a wiretap code for the adaptive transmission scheme we only need to determine the value of $R_E$. In the adaptive transmission scheme, $R_E$ is adjusted within the constraint $0 < R_E < C_B$ according to each $\gamma_B$. Since $R_B$ is chosen as $R_B = C_B$, the reliability constraint can always be guaranteed in the adaptive transmission scheme (reliability outage probability is zero). We note that a secrecy outage may occur since $C_E$ is not available at Alice. In the following, we first present the secrecy outage probability of the adaptive transmission scheme.

As per the definition of $O_s(R_E)$, the secrecy outage probability of the adaptive transmission scheme is

$$O_{s,a}(R_E) = \Pr (R_E < C_E) = \Pr (\gamma_E > 2R_E - 1) = 1 - F_{\gamma_E}(2R_E - 1), \quad (8)$$

where $F_{\gamma_E}(\gamma_E)$ is the cumulative distribution function (cdf) of $\gamma_E$, which is

$$F_{\gamma_E}(\gamma_E) = 1 - e^{-\frac{\gamma_E}{\gamma_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left( \frac{\gamma_E}{\gamma_E} \right)^j. \quad (9)$$

As such, the EST of the adaptive transmission scheme is given in the following lemma.

**Lemma 1:** The EST of the adaptive transmission scheme is

$$\Psi_a(R_E) = (C_B - R_E) \left[ 1 - e^{-\frac{B - 2R_E}{\gamma_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left( \frac{2R_E - 1}{\gamma_E} \right)^j \right]. \quad (10)$$

**Proof:** Since the reliability outage probability of the adaptive transmission scheme is zero and $R_B$ is set as $R_B = C_B$, based on (7) the EST of the adaptive transmission scheme is given by

$$\Psi_a(R_E) = (C_B - R_E) [1 - O_{s,a}(R_E)] = (C_B - R_E) F_{\gamma_E}(2R_E - 1). \quad (11)$$

Substituting (9) into (11), we obtain the result in (10).

Based on the closed-form expression for $\Psi_a(R_E)$ given in (11), the value of $R_E$ that locally maximizes the EST of the adaptive transmission scheme can be numerically determined. To facilitate this numerical determination, we first derive the first-order derivative of (10) with respect to $R_E$ as

$$\frac{\partial \Psi_a(R_E)}{\partial R_E} = -1 + e^{-\frac{2R_E - 1}{\gamma_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left( \frac{2R_E - 1}{\gamma_E} \right)^j \times \left[ C_B - R_E \right] \left( \frac{2R_E \ln 2}{\gamma_E} \right) e^{-\frac{R_E}{\gamma_E}} \left( \frac{2R_E - 1}{\gamma_E} \right)^{N_E-1}.$$

By setting $\frac{\partial \Psi_a(R_E)}{\partial R_E} = 0$ and performing some algebraic manipulations, the value of $R_E$ that achieves a stationary point of $\Psi_a(R_E)$ can be obtained by solving the fixed-point equation given by

$$R_E^\dagger = C_B - \frac{\gamma_E(N_E - 1)!}{2R_E \ln 2} \left( \frac{\gamma_E}{2R_E - 1} \right)^{N_E-1} \times \left[ e^{-\frac{R_E - 1}{\gamma_E}} - \sum_{j=0}^{N_E-1} \frac{1}{j!} \left( \frac{2R_E - 1}{\gamma_E} \right)^j \right]. \quad (12)$$

The second-order derivative of (10) with respect to $R_E$ is derived as

$$\frac{\partial^2 \Psi_a(R_E)}{\partial R_E^2} = \left( \frac{2R_E \ln 2}{\gamma_E} \right) e^{-\frac{R_E - 1}{\gamma_E}} \left( \frac{2R_E - 1}{\gamma_E} \right)^{N_E-1} \times \left[ (C_B - R_E) \left( \frac{1 - \frac{2R_E}{\gamma_E}}{\gamma_E} \right) \ln 2 - 2 \right] \times \left[ (C_B - R_E)(N_E - 1) \right]. \quad (14)$$

An analysis of identifying stationary points via (12) and (14) is not tractable. Instead, we investigate the nature of the stationary points via detailed simulations and numerical calculations over all the anticipated operating conditions. Although such simulations do not formally prove the globally optimal solution, we find that in the value range of $R_E$ (i.e., $0 < R_E < C_B$) the stationary points obtained through (13) are identified as local maxima in all simulations. An example of our simulations is shown in Fig. 2 (see numerical results section for details). As we see, for the chosen simulation parameters locally maximum operating points are easily identified.

Substituting $R_E^\dagger$ into (10), we obtain a stationary value of $\Psi_a(R_E)$, which is denoted by $\Psi_a^\star$. We now conduct the asymptotic analysis of $R_E^\dagger$ and provide some valuable insights into $R_E^\dagger$ for $N_E = 1$ in the following remarks.

**Remark 1:** As $\gamma_E \rightarrow 0$, we obtain $R_E^\dagger \rightarrow 0$.

**Proof:** When $N_E = 1$, (10) reduces to

$$\Psi_a(R_E) = (C_B - R_E) \left[ 1 - e^{-\frac{R_E - 1}{\gamma_E}} \right]. \quad (15)$$

It is found from (13) that $\Psi_a(R_E)$ converges to $(C_B - R_E)$ as $\gamma_E \rightarrow 0$. Therefore, due to the constraint $0 < R_E < C_B$, we have $R_E^\dagger \rightarrow 0$.

It is indicated from Remark 1 that Eve can be ignored if she is far from Alice. This is mainly due to the fact that the secrecy outage probability approaches zero as Eve moves further away from Alice (i.e., as the average SNR of the eavesdropper’s channel approaches zero).

**Remark 2:** As $\gamma_E \rightarrow \infty$, $R_E^\dagger$ can be obtained by solving the fixed-point equation given by

$$R_E^\dagger = C_B - \frac{1 - \frac{2R_E^\dagger}{\gamma_E}}{\ln 2}. \quad (16)$$

**Proof:** Applying $\lim_{x \rightarrow 0} e^{-x} \approx 1 - x$ into (15), we obtain

$$\lim_{\gamma_E \rightarrow \infty} (C_B - R_E) \left[ 1 - e^{-\frac{R_E - 1}{\gamma_E}} \right] \approx (C_B - R_E) \frac{2R_E - 1}{\gamma_E}. \quad (17)$$

By setting the first-order derivative of (17) with respect to $R_E$ as zero, we obtain the fixed-point equation in (16) after some algebraic manipulations.

From Remark 2, we see that $R_E^\dagger$ does not approach $C_B$ but the effective secrecy throughput $\Psi_a(R_E)$ approaches zero as $\gamma_E \rightarrow \infty$. This is due to the fact that the secrecy outage probability of the adaptive transmission scheme approaches one as $\gamma_E \rightarrow \infty$ (i.e., the secure transmission probability approaches zero as $\gamma_E \rightarrow \infty$). Notably, $R_E^\dagger$ approaches a
constant value that is a function of $C_B$. This is due to the fact that the value of $R_E$ that enables the first-order derivative of (17) to be zero does not depend on $\gamma_E$.

B. Numerical Results

In this subsection, we present numerical results to examine the impact of the number of antennas at Eve and the SNRs of the main channel and eavesdropper’s channel, on the redundancy rate $R_E^1$.

In Fig. 2, we plot the EST of the adaptive transmission scheme, $\Psi_a(R_E)$, versus $R_E$ for $N_E = 3$, $\gamma_B = 20$ dB, and different values of $\gamma_E$. The theoretic curve is obtained from (10). In this figure, we first observe that the Monte Carlo simulations precisely match the theoretic curve, which validates our analysis in Lemma 1. We also observe that $\Psi_a(R_E)$ increases as $\gamma_E$ decreases, which demonstrates that the worse the eavesdropper’s channel is the larger EST the adaptive transmission scheme achieves. Moreover, we observe that a unique value of $R_E$ exists which maximizes $\Psi_a(R_E)$ for a given $\gamma_B$. Focusing on the peaks of the three curves, we also observe that $R_E^1$ decreases as $\gamma_E$ decreases, which demonstrates that the further Eve is from Alice the smaller redundancy rate we set in order to maximize the EST.

In Fig. 3, we plot the redundancy rate for the adaptive transmission scheme, $R_E^1$, versus $\gamma_B$ for different values of $N_E$ and $\gamma_E$. The curves represent the theoretic results for $R_E^1$ obtained from (13), and the symbols represent the simulated results for $R_E^1$ obtained from Monte Carlo simulations. The accuracy of (13) is demonstrated in this figure. As expected, we first observe that $R_E^1$ increases as $\gamma_E$ increases. We also observe that $R_E^1$ first increases as $\gamma_B$ increases and then approaches a constant as $\gamma_B$ approaches large values. Furthermore, we observe that $R_E^1$ increases as $N_E$ increases. This can be explained by the fact that a higher $N_E$ leads to a better quality of the eavesdropper’s channel.

IV. DETERMINATION OF WIRETAP CODE RATES FOR FIXED-RATE TRANSMISSION SCHEME

In this section, we first derive a closed-form expression for the EST of the fixed-rate transmission scheme, based on which we provide an easy-to-implement method to determine the codeword rate $R_B$ and redundancy rate $R_E$ that jointly achieve a locally maximum EST for this scheme. We note that the fixed-rate transmission scheme does not require the capacity of the main channel be available at Alice. As such, this scheme is a lower complexity system in which there is no feedback from Bob to Alice.

A. Fixed-Rate Transmission Scheme

In the fixed-rate transmission scheme, both $C_B$ and $C_E$ are unavailable at Alice, so we have to jointly determine $R_B$ and $R_E$ for given $\gamma_B$ and $\gamma_E$. Therefore, both the reliability constraint and secrecy constraint cannot be guaranteed in this scheme. In the following, we first present the reliability outage probability and secrecy outage probability.

As per the definition of $O_r(R_B)$, the reliability outage probability of the fixed-rate transmission scheme is

$$O_{r,f}(R_B) = \Pr(R_B > C_B) = F_{\gamma_B}(2^{R_B} - 1),$$

where $F_{\gamma_B}(\gamma_B)$ is the cdf of $\gamma_B$, which is

$$F_{\gamma_B}(\gamma_B) = 1 - e^{-\frac{\gamma_B}{\theta_B}}.$$  

According to the definition of $O_s(R_E)$, the secrecy outage probability of the fixed-rate transmission scheme is

$$O_{s,f}(R_E) = \Pr(R_E < C_E) = 1 - F_{\gamma_E}(2^{R_E} - 1).$$

The EST of the fixed-rate transmission scheme is presented in the following lemma.
Lemma 2: The EST of the fixed-rate transmission scheme is

\[ \Psi_j(R_B, R_E) = (R_B - R_E) e^{-\frac{R_B}{\tau_B}} \left( 1 - e^{-\frac{R_E}{\tau_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left( \frac{2R_E - 1}{\tau_E} \right)^j \right). \]  

(21)

Proof: As per the definition of \( \Psi(R_B, R_E) \), the EST of the fixed-rate transmission scheme can be written as

\[ \Psi_j(R_B, R_E) = (R_B - R_E) \left[ 1 - \mathcal{O}_{r_j}(R_B) \right] \left[ 1 - \mathcal{O}_{s_j}(R_E) \right] = (R_B - R_E) \left[ 1 - F_{\gamma_B} \left( 2^{R_B} - 1 \right) \right] F_{\gamma_E} \left( 2^{R_E} - 1 \right). \]  

(22)

Substituting (19) and (9) into (22), we obtain the result in (21) after some algebraic manipulations.

Using (22), the values of \((R_B, R_E)\) that achieve a locally maximum EST can be obtained through

\[ (R_B, R_E)^* = \arg\max_{0 < R_B, 0 < R_E < R_B} \Psi_j(R_B, R_E). \]  

(23)

To make progress let us define two functions, \( \mathcal{F}(\cdot) \) and \( \mathcal{G}(\cdot) \), as

\[ \mathcal{F}(N_E, R_E, \tau_E) = \sum_{j=0}^{N_E-1} \frac{1}{j!} \left( \frac{2R_E - 1}{\tau_E} \right)^j \]  

(24)

and

\[ \mathcal{G}(N_E, R_E, \tau_E) = \frac{2R_E \ln 2}{\tau_E(N_E - 1)!} \left( \frac{2R_E - 1}{\tau_E} \right)^{N_E-1}. \]  

(25)

We note that \( 1 - \mathcal{F}(N_E, R_E, \tau_E) e^{-\frac{R_E}{\tau_E}} \) and \( e^{\frac{R_E}{\tau_E}} \) are both positive for \( 0 < R_E < R_B \) and finite \( N_E \). Setting the first-order partial derivative of (21) with respect to \( R_B \) to zero, we obtain

\[ 1 - (R_B - R_E) e^{\frac{R_B}{\tau_B} \ln 2} = 0, \]

which results in

\[ R_E = R_B - \frac{\tau_B}{2R_B \ln 2}. \]  

(26)

Similarly, by setting the first-order partial derivative of (21) with respect to \( R_E \) to zero, we obtain

\[ \mathcal{F}(N_E, R_E, \tau_E) - (R_B - R_E) \mathcal{G}(N_E, R_E, \tau_E) = e^{\frac{R_E}{\tau_E}} \mathcal{F}(N_E, R_E, \tau_E), \]

which results in

\[ R_B = R_B + \frac{e^{R_E - 1}}{\tau_E} - \mathcal{F}(N_E, R_E, \tau_E), \]  

(27)

Substituting (26) into (27) and performing some algebraic manipulations, the value of \( R_B \) that achieves a stationary point of \( \Psi_j(R_B, R_E) \) can be obtained through solving the fixed-point equation given by

\[ R_B^* = R_B^* + \frac{e^{R_E - 1}}{\tau_E} - \mathcal{F}(N_E, R_E^*, \tau_E), \]  

(28)

where

\[ R_E^* = R_B^* - \frac{\tau_B}{2R_B^* \ln 2}. \]  

(29)

and the value of \( R_E \) that jointly achieves the stationary point of \( \Psi_j(R_B, R_E) \) can be obtained by substituting \( R_B^* \) into (29).

The Hessian matrix of (21), which is symmetric based on Young's theorem [30], is given by

\[ \mathbf{H} = \begin{bmatrix} \frac{\partial^2 \Psi_j(R_B, R_E)}{\partial R_B^2} & \frac{\partial^2 \Psi_j(R_B, R_E)}{\partial R_B \partial R_E} & \frac{\partial^2 \Psi_j(R_B, R_E)}{\partial R_E^2} \\ \frac{\partial^2 \Psi_j(R_B, R_E)}{\partial R_B \partial R_E} & \frac{\partial^2 \Psi_j(R_B, R_E)}{\partial R_E^2} & \end{bmatrix} = \begin{bmatrix} A & B \\ B & C \end{bmatrix}, \]  

(30)

where

\[ A = -2R_B \ln 2 \times D \times \left[ 2 + \ln 2(R_B - R_E) \left( 1 - \frac{2R_B}{\tau_B} \right) \right], \]  

(31)

\[ B = 2R_B \ln 2 \times e^{\frac{R_E - 1}{\tau_E}} \times D \left( 1 - (R_B - R_E) \frac{2R_B \ln 2}{\tau_B} \right) \times \mathcal{E}, \]  

(32)

\[ C = -2e^{\frac{R_E - 1}{\tau_E}} \times \mathcal{E} \times \left( R_B - R_E \right) e^{\frac{R_E - 1}{\tau_E}} \times \mathcal{E} \left( \ln 2 + (N_E - 1) \frac{2R_E \ln 2}{2R_E - 1} - \frac{2R_E \ln 2}{2R_E - 1} \right), \]  

(33)

with

\[ D = 1 - e^{\frac{R_E - 1}{\tau_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left( \frac{2R_E - 1}{\tau_E} \right)^j, \]  

(34)

\[ \mathcal{E} = \frac{2R_E \ln 2}{\tau_E(N_E - 1)!} \left( \frac{2R_E - 1}{\tau_E} \right)^{N_E-1} e^{-\frac{R_E}{\tau_E}}. \]  

(35)

If \( A < 0 \) and \( A \times C - B^2 > 0 \) when \( R_B = R_B^* \) and \( R_E = R_E^* \), we can conclude that \( R_B^* \) and \( R_E^* \) lead to a locally maximum \( \Psi_j(R_B, R_E) \). However, a rigorous analysis of identifying stationary points via (28) and (30) is not tractable. Instead, we once again investigate the nature of the stationary points via detailed simulations and numerical calculations over all the anticipated operating conditions and over the rate range \( 0 < R_E < R_B < 100 \). We find that such simulations and numerical calculations always identify the locally maximum solutions, although they do not formally identify the globally optimal solution. One exemplary numerical result is presented in Fig. 4, where there is a unique pair of \( R_B \) and \( R_E \) achieving the locally maximum \( \Psi_j(R_B, R_E) \). It is highlighted that (28) is of great significance since it is difficult to conduct numerical search to find \( R_B^* \) and \( R_E^* \) under the constraint on \((R_B, R_E)\) given by \( 0 < R_E < R_B < +\infty \). Instead, we can solve (28) iteratively by setting the initial value of \( R_E^* \) to zero. Substituting \( R_B^* \) and \( R_E^* \) into (21), we obtain the stationary value of \( \Psi_j(R_B, R_E) \), which is denoted by \( \Psi_j^* \).

We next conduct the asymptotic analysis for \( N_E = 1 \) and offer some valuable insights into \( R_B^* \) and \( R_E^* \) in the following remarks.

Remark 3: As \( \tau_E \to 0 \), \( R_B^* \) for a given \( \tau_B \) can be obtained through solving the fixed-point equation given by

\[ R_B^* = \frac{\tau_B}{2R_B^* \ln 2}, \]  

(36)

and the corresponding \( R_E^* \) approaches zero.
Proof: As \( \gamma_E \to 0 \), we obtain \( O_{s,f}(R_E) \to 0 \). Accordingly, (21) with \( N_E = 1 \) reduces to
\[
\Psi_f(R_B, R_E) = (R_B - R_E) e^{-\frac{2R_B - 1}{2R_E}}. \tag{37}
\]
Setting the first-order derivative of (37) with respect to \( R_B \) as zero, we obtain the result in (36) after some algebraic manipulations. \( \blacksquare \)

From Remark 3, we see that Eve can be ignored if she is far from Alice since \( R_E \to 0 \) as \( \gamma_E \to 0 \). This is due to the fact that the secrecy outage probability of the fixed-rate transmission scheme, \( O_{s,f}(R_E) \), approaches zero as \( \gamma_E \to 0 \). We also note that \( R_B^* \) is a function of \( \gamma_B \) only, which can be explained by the fact that \( R_B^* \) is determined through maximizing \( R_B [1 - O_{r,f}(R_B)] \). We further note that \( \Psi_f^* \) approaches a constant value which is determined by \( \gamma_B \) as \( \gamma_E \to 0 \), due to that \( O_{s,f}(R_E) \to 0 \) as \( \gamma_E \to 0 \).

Remark 4: As \( \gamma_E \to \infty \), \( R_B^* \) for a given \( \gamma_B \) can be obtained through solving the fixed-point equation given by
\[
R_B^* = R_E^* + \frac{2R_E - 1}{2R_E \ln 2}, \tag{38}
\]
where
\[
R_E^* = R_B^* - \frac{\gamma_B}{2R_B \ln 2}, \tag{39}
\]
and \( R_E^* \) can be obtained by substituting \( R_B^* \) into (39).

Proof: When \( N_E = 1 \), (21) reduces to
\[
\Psi_f(R_B, R_E) = (R_B - R_E) e^{-\frac{2R_B - 1}{2R_E}} \left( 1 - e^{-\frac{2R_E - 1}{2R_E}} \right). \tag{40}
\]
Since \( R_E \) is still finite as \( \gamma_E \to \infty \), we apply \( \lim_{x \to 0} e^{-x} \approx 1 - x \) into (40) and obtain
\[
\lim_{\gamma_E \to \infty} \Psi_f(R_B, R_E) \approx (R_B - R_E) e^{-\frac{2R_B - 1}{2R_E} - \frac{2R_E - 1}{\gamma_E}}. \tag{41}
\]
We note \( e^{-\frac{2R_E - 1}{\gamma_E}} > 0 \) due to \( R_E > 0 \) as \( \gamma_E \to \infty \). Setting the first-order derivative of (41) with respect to \( R_B \) as zero, we obtain
\[
(R_B - R_E) \frac{2R_B \ln 2}{\gamma_B} = 1. \tag{42}
\]
Likewise, setting the first-order derivative of (41) with respect to \( R_E \) as zero, we obtain
\[
-\frac{2R_E - 1}{\gamma_E} + (R_B - R_E) \frac{2R_E \ln 2}{\gamma_E} = 0, \tag{43}
\]
which results in (due to \( \gamma_E \neq 0 \))
\[
1 - 2R_E + (R_B - R_E) 2R_E \ln 2 = 0. \tag{44}
\]
Substituting (42) into (44), we obtain the fixed-point equation in (38) after some algebraic manipulations. \( \blacksquare \)

It is highlighted from Remark 4 that (38) and (39) are independent of \( \gamma_E \), which indicates that \( R_B^* \) and \( R_E^* \) are not functions of \( \gamma_E \) as \( \gamma_E \to \infty \). This is due to the fact that the secrecy outage probability \( O_{s,f}(R_E) \) approaches 1 as \( \gamma_E \to \infty \).

B. Numerical Results

In this subsection, we present numerical results to examine the impact of the number of antennas at Eve and the SNRs of the main channel and eavesdropper’s channel, on \( R_B^* \) and \( R_E^* \). We also conduct a thorough performance comparison between the adaptive transmission scheme and the fixed-rate transmission scheme in terms of the EST.

In Fig. 4, we plot the EST of the fixed-rate transmission scheme, \( \Psi_f(R_B, R_E) \), versus \( R_B \) and \( R_E \). The theoretic \( \Psi_f(R_B, R_E) \) curve is generated via (21). In this figure, we first observe that the Monte Carlo simulation result precisely matches the theoretic curve. Moreover, we observe that there is indeed a unique pair of \( R_B \) and \( R_E \) that achieves a locally maximum value of \( \Psi_f(R_B, R_E) \). This demonstrates that we can determine the values of \( (R_B, R_E) \) that achieve a locally maximum \( \Psi_f(R_B, R_E) \) based on our proposed framework.

In Fig. 5, we plot the wiretap code rates of the fixed-rate transmission scheme, \( R_B^* \) and \( R_E^* \), versus \( \gamma_E \). The exact curves of \( R_B^* \) and \( R_E^* \) are obtained by solving (28) and (29), respectively. The curve of \( R_B^* \) for \( \gamma_E \to 0 \) is generated by solving (36), and \( R_E^* \) for \( \gamma_E \to 0 \) is approximated as zero. The curves of \( R_B^* \) and \( R_E^* \) for \( \gamma_E \to \infty \) are achieved by solving (38) and (39), respectively. As we have checked, in Fig. 5 \( R_B^* \) and \( R_E^* \) jointly achieve a locally maximum \( \Psi_f(R_B, R_E) \). In this figure, we first observe that the Monte Carlo simulated \( R_B^* \) and \( R_E^* \) precisely match the theoretic \( R_B^* \) and \( R_E^* \), respectively. We also observe that the exact curves of \( R_B^* \) and \( R_E^* \) approach the asymptotic curves of \( R_B^* \) and \( R_E^* \), respectively, as \( \gamma_E \to 0 \) and \( \gamma_E \to \infty \). This observation confirms the accuracy of our asymptotic analysis given in Remark 3 and Remark 4. Finally, we observe that both \( R_B^* \) and \( R_E^* \) increase as \( \gamma_E \) increases, but \( (R_B^* - R_E^*) \) decreases as \( \gamma_E \) increases.

In Fig. 6, we plot \( R_B^* \) and \( R_E^* \) versus \( \gamma_E \) for different values of \( N_E \), which have been confirmed as the values of \( R_B \) and \( R_E \) that jointly achieve a locally maximum \( \Psi_f(R_B, R_E) \).
Theoretic curve for $\Psi^E$ versus $\gamma_E$ for $N_E = 1$ and $\gamma_B = 5$ dB.

- $R^*_B$ and $R^*_E$, versus $\gamma_E$ for $N_E = 1$ and $\gamma_B = 5$ dB.

- $R^*_B$ and $R^*_E$, versus $\gamma_E$ for $N_E = 1$.

- $R^*_B$ and $R^*_E$, versus $\gamma_E$ for $N_E = 2$.

- $R^*_B$ and $R^*_E$, versus $\gamma_E$ for $N_E = 4$.

In this figure, we first observe that both $R^*_B$ and $R^*_E$ increase as $\gamma_B$ increases, and $(R^*_B - R^*_E)$ increases as $\gamma_B^*$ increases. We also observe that as $\gamma_B^* \to 0$ both $R^*_B$ and $R^*_E$ approach zero, which indicates that a positive EST cannot be achieved when Bob is very far from Alice. Furthermore, we observe that $R^*_B$ is still a function of $\gamma_B^*$ as $\gamma_B^* \to \infty$, but $R^*_E$ approaches a specific constant value. Finally, we observe that both $R^*_B$ and $R^*_E$ increase as $N_E$ increases, but $(R^*_B - R^*_E)$ decreases as $N_E$ increases.

Now, we conduct a thorough comparison between the adaptive transmission scheme and the fixed-rate transmission scheme. The results are presented in Fig. 7, where $\Psi^E$ is the average locally maximum EST of the adaptive transmission scheme, obtained by $\Psi^E = E_{\gamma_B}[\Psi^*_a]$. We first observe that both $\Psi^E$ and $\Psi^*_E$ increase as $\gamma_B^*$ increases, but decrease as $\gamma_E$ increases. This indicates that the locations of Alice, Bob, and Eve are of importance in wiretap channels. As expected, we observe that the adaptive transmission scheme achieves higher EST than the fixed-rate transmission scheme. In addition, we observe that the EST gain of the adaptive transmission scheme over the fixed-rate transmission scheme is negligible in the regime of low $\gamma_B^*$ (relative to $\gamma_E$), but significant in the regime of high $\gamma_B^*$. Of course, the EST is enhanced at the cost of feeding back $C_B$ to Alice and adjusting $R_B$ and $R_E$ for each realization of the main channel.

V. DETERMINATION OF WIREDTAP CODE RATES WITHIN AN ABSOLUTE-PASSIVE EAVESDROPPING SCENARIO

In this section, we extend the determination of the wiretap code rates for the adaptive and fixed-rate transmission schemes into an absolute-passive eavesdropping scenario, where no SNR information of the eavesdropper’s channel (not even the average value) is made available to Alice. To relax the assumption in the previous two sections that $\gamma_E$ is known at Alice, we propose a new threat model, referred to as the annulus threat model. For this threat model, we derive closed-form expressions for the average EST of the adaptive and fixed-rate transmission schemes, based on which the wiretap code rates can be determined.

A. Annulus Threat Model

Fig. 8 depicts a practical scenario where physical layer security may apply. In this scenario, the Wi-Fi point (Alice) and the legitimate user (Bob) are located inside a property (e.g., a house), but the eavesdropper (Eve) is bounded outside the property. In practice, Eve cannot be infinitely far from Alice. As such, in practical wiretap channels the distance between Alice and Eve should be larger than a specific value and less than another specific value. This motivates us to propose an annulus threat model. In the annulus threat model,
we assume that Eve’s location is uniformly distributed inside an annulus bounded by two concentric circles, where \( \rho_i \) and \( \rho_o \) are the radii of the inner circle and the outer circle, respectively, and Alice is at the center of the two concentric circles.

In our annulus threat model, we denote the distance between Alice and Eve as \( \rho \). Based on the path loss model, the average SNR of the eavesdropper’s channel is a function of \( \rho \), which can be expressed as [25]

\[
\Psi_E = c_0 \rho^{-\eta},
\]

(45)

where \( c_0 = \bar{\gamma}/\rho_i^{-\eta} \), \( \bar{\gamma} \) is the reference average SNR of the eavesdropper’s channel at the reference distance \( \rho_i \), and \( \eta \) is the path loss exponent. In the previous sections, the EST is derived as a function of \( \Psi_E \). In this section, we derive the average secrecy throughput over \( \Psi_E \) under the annulus threat model. To this end, we first present the probability density function (pdf) of \( \rho^2 \) in the following lemma.

**Lemma 3:** The square of the distance between Alice and Eve, \( \rho^2 \), follows a uniform distribution with \( \rho_i^2 \) and \( \rho_o^2 \) as the lower bound and upper bound, respectively, i.e., \( \rho^2 \sim U(\rho_i^2, \rho_o^2) \).

**Proof:** See Appendix.

B. Adaptive Transmission Scheme

We note that the adaptive transmission scheme represents a high complexity system where Bob feeds back \( C_B \) to Alice, and we only need to determine the value of \( R_E \) for this scheme since \( R_B = C_B \). We derive the average secrecy throughput of the adaptive transmission scheme for the annulus threat model in the following theorem.

**Theorem 1:** The average EST of the adaptive transmission scheme for the annulus threat model is

\[
\tilde{\Psi}_a(R_E, \rho_i, \rho_o) = (C_B - R_E) \times \left(1 - \frac{\eta \gamma(v, u \rho_i^2) - \gamma(v, u \rho_o^2)}{j!} \right)
\]

(46)

where \( u = (2^{R_E} - 1)/c_0 \), \( v = j + 2/\eta \), and \( \gamma(\cdot, \cdot) \) is the incomplete gamma function [31, Eq. (8.350.1)].

**Proof:** Under the annulus threat model, the average EST of the adaptive transmission scheme is

\[
\tilde{\Psi}_a(R_E, \rho_i, \rho_o) = \mathbb{E}_\rho[\tilde{\Psi}_a(R_E)] = \int_{\rho_i^2}^{\rho_o^2} \frac{\tilde{\Psi}_a(R_E)}{\rho_o^2 - \rho_i^2} d\rho^2.
\]

(47)

Substituting (10) and (45) into (47), we obtain

\[
\tilde{\Psi}_a(R_E, \rho_i, \rho_o) = \int_{\rho_i^2}^{\rho_o^2} \frac{\tilde{\Psi}_a(R_E)}{\rho_o^2 - \rho_i^2} d\rho^2 = \frac{(C_B - R_E)}{\rho_o^2 - \rho_i^2} \int_{\rho_i^2}^{\rho_o^2} \left[1 - e^{-\frac{R_E - 1}{c_0 \rho^{-\eta}}} \sum_{j=0}^{N_E-1} \frac{\left(\frac{2^{R_E-1}}{c_0}\right)^j}{j!} \right] d\rho^2
\]

\[
= \frac{(C_B - R_E)}{\rho_o^2 - \rho_i^2} \sum_{j=0}^{N_E-1} \frac{\left(\frac{2^{R_E-1}}{c_0}\right)^j}{j!} \int_{\rho_i^2}^{\rho_o^2} \rho^j e^{-\frac{R_E - 1}{c_0 \rho^{-\eta}}} d\rho^2
\]

\[
= \frac{(C_B - R_E)}{\rho_o^2 - \rho_i^2} \sum_{j=0}^{N_E-1} \frac{\left(\frac{2^{R_E-1}}{c_0}\right)^j}{j!} \int_{0}^{\rho_o^2} \rho^j e^{-\frac{R_E - 1}{c_0 \rho^{-\eta}}} d\rho^2 - \int_{0}^{\rho_i^2} \rho^j e^{-\frac{R_E - 1}{c_0 \rho^{-\eta}}} d\rho^2
\]

(48)

We solve the integrals in (48) with the aid of [31, Eq. (3.381.8)], and obtain the desired result in (46) after some algebraic manipulations.

The value of \( R_E \) that achieves a locally maximum \( \tilde{\Psi}_a(R_E, \rho_i, \rho_o) \) can be determined through

\[
R_E^* = \arg\max_{0 < R_E < C_B} \tilde{\Psi}_a(R_E, \rho_i, \rho_o).
\]

(49)
Theorem 2: The average EST of the fixed-rate transmission scheme for the annulus threat model is

\[
\tilde{\Psi}_f(R_B, R_E, \rho_i, \rho_o) = (R_B - R_E) e^{-\frac{2R_B}{\rho_o}} \times \left( 1 - \sum_{j=0}^{N_E-1} \frac{2w^j \gamma(v, w \rho_o^j) - \gamma(v, w \rho_i^j)}{j! (\rho_o^j - \rho_i^j) \eta w^j} \right),
\]

(50)

where \( w = (2R_E - 1) / \gamma(0) \).

Proof: Under the annulus threat model, the average EST of the fixed-rate transmission scheme is

\[
\tilde{\Psi}_f(R_B, R_E, \rho_i, \rho_o) = \mathbb{E}[\tilde{\Psi}_f(R_B, R_E)] = \int_{\rho_i^2}^{\rho_o^2} \frac{\tilde{\Psi}_f(R_B, R_E)}{\rho_o^2 - \rho_i^2} d\rho^2.
\]

Substituting (21) and (45) into (51), we obtain

\[
\tilde{\Psi}_f(R_B, R_E, \rho_i, \rho_o) = \int_{\rho_i^2}^{\rho_o^2} \frac{\Psi_f(R_B, R_E)}{\rho_o^2 - \rho_i^2} d\rho^2.
\]

One exemplary numerical result is presented in Fig. 9, which shows that there is a unique value of \( R_E \) within \( 0 < R_E < C_B \) achieving the locally maximum \( \tilde{\Psi}_a(R_E, \rho_i, \rho_o) \). Substituting \( \tilde{R}_E \) into (46), we obtain the locally maximum value of \( \tilde{\Psi}_a(R_E, \rho_i, \rho_o) \), denoted by \( \tilde{\Psi}_a^\dagger(\rho_i, \rho_o) \).

C. Fixed-Rate Transmission Scheme

We remind the reader that the fixed-rate transmission scheme represents a lower complexity system where Bob does not need feedback \( C_B \) to Alice, and we have to jointly determine the values of \( R_B \) and \( R_E \). We derive the average EST of the fixed-rate transmission scheme for the annulus threat model in the following theorem.

The values of \( (R_B, R_E) \) that achieve a locally maximum \( \tilde{\Psi}_f(R_B, R_E, \rho_i, \rho_o) \) can be determined through

\[
(R_B, R_E)_{\rho}^\dagger = \arg\max_{0 < R_B, 0 < R_E < R_B} \tilde{\Psi}_f(R_B, R_E, \rho_i, \rho_o).
\]

(53)

The values of \( R_B \) and \( R_E \) in \( (R_B, R_E)_{\rho}^\dagger \) are denoted as \( \tilde{R}_B \) and \( \tilde{R}_E \), respectively. Our numerical results show that there is a unique pair of \( \tilde{R}_B^\dagger \) and \( \tilde{R}_E^\dagger \) that achieves a locally maximum \( \tilde{\Psi}_f(R_B, R_E, \rho_i, \rho_o) \) over all the anticipated operating conditions. One exemplary numerical result is presented in Fig. 10. Substituting \( \tilde{R}_B^\dagger \) and \( \tilde{R}_E^\dagger \) into (50), we obtain the locally maximum value of \( \tilde{\Psi}_f(R_B, R_E, \rho_i, \rho_o) \), denoted by \( \tilde{\Psi}_f^\dagger(\rho_i, \rho_o) \).

D. Numerical Results

In this subsection, we present numerical results to examine the impact of \( \rho_i \) and \( \rho_o \) on the determined wiretap code rates and the locally maximum average EST of the adaptive and fixed-rate transmission schemes.

In Fig. 11, we plot the redundancy rate, \( \tilde{R}_E \), and the locally maximum average EST, \( \tilde{\Psi}_a^\dagger(\rho_i, \rho_o) \), of the adaptive transmission scheme versus \( \rho_i \) and \( \rho_o \). In this figure, we first observe that \( \tilde{R}_E \) decreases as \( \rho_i \) increases, which reveals that the redundancy rate used to confuse Eve can be reduced by increasing the inner boundary. We also observe that \( \tilde{R}_E \) decreases as \( \rho_o \) increases. This can be explained by the fact that a larger outer boundary \( \rho_o \) means Eve is statistically further from Alice. Moreover, we observe \( \tilde{\Psi}_a^\dagger(\rho_i, \rho_o) \) increases as \( \rho_i \) increases, which indicates that the further the inner boundary is from Alice, the better secrecy performance the adaptive transmission scheme achieves. As such, a higher average EST can be achieved through enlarging the inner boundary. We further observe that \( \tilde{\Psi}_a^\dagger(\rho_i, \rho_o) \) increases as \( \rho_o \) increases. This can be explained by the fact that \( \tilde{\Psi}_a^\dagger(\rho_i, \rho_o) \) is averaged over \( \gamma_E \) in the annulus threat model, and a larger \( \rho_o \) means that Eve is further from Alice on average since in the annulus threat model Eve’s location is uniformly distributed in the annulus.

In Fig. 12, we plot the wiretap code rates, \( \tilde{R}_B^\dagger \) and \( \tilde{R}_E^\dagger \), and the locally maximum average EST, \( \tilde{\Psi}_f^\dagger(\rho_i, \rho_o) \), of the fixed-rate transmission scheme versus \( \rho_i \) and \( \rho_o \). In this figure, we
first observe that both $\tilde{R}_B^*$ and $\tilde{R}_E^*$ decrease as $\rho_i$ increases, and $\tilde{R}_E^*$ is more sensitive to $\rho_i$ than $\tilde{R}_B^*$, which results in $\tilde{\Psi}_f^*(\rho_i, \rho_o)$ increasing as $\rho_i$ increases. The above observation indicates that the further the inner boundary is from Alice, the better secrecy performance the fixed-rate transmission scheme achieves. We also observe that both $\tilde{R}_B^*$ and $\tilde{R}_E^*$ increase as $\rho_o$ increases, and $\tilde{R}_E^*$ is more sensitive to $\rho_o$ than $\tilde{R}_B^*$, which results in $\tilde{\Psi}_f^*(\rho_i, \rho_o)$ increasing as $\rho_o$ increases. This is can be explained by the fact that $\tilde{\Psi}_f^*(\rho_i, \rho_o)$ is averaged over $\tau_E$, and a larger $\rho_o$ means that Eve is statistically further from Alice.

We note that the issue of the unknown average SNR of the eavesdropper’s channel $\tau_E$ can be investigated via the consideration of a general average SNR model. In such an average SNR model, a specific distribution (e.g., a uniform distribution or a Gaussian distribution) can be assigned to $\tau_E$ and then thorough analysis of the average effective secrecy throughput of the adaptive and fixed-rate transmission schemes can be conducted. We find that the specific distribution of $\tau_E$ has to be carefully selected based on practical application scenarios and corresponding system parameters. This is due to the fact that the distribution of $\tau_E$ may depend on some specific system parameters. For example, the distribution type of $\tau_E$ is dependent on the path loss exponent $\eta$ within our annulus threat model.

VI. CONCLUSION

In this paper, we proposed a new framework to determine the wiretap code rates for the SISO-M wiretap channel. We considered several scenarios including the case of the absolute-passive eavesdropping scenario in which even the average SNR of the eavesdropper’s channel is unknown at the transmitter. The framework is based on a new performance metric, the EST, which captures explicitly the reliability constraint and secrecy constraint of wiretap channels. The framework does not require a determination of the secrecy outage probability \textit{a priori} or subjectively, and therefore is very pragmatic.

ACKNOWLEDGEMENT

This work was funded by the Australian Research Council Grant DP120102607. We thank the three anonymous referees for their valuable comments and suggestions on improving the quality of the paper.

APPENDIX: PROOF OF LEMMA 3

In the Cartesian coordinate system, we denote the location of Eve by $(u, v)$. In the annulus threat model, the joint pdf of $u$ and $v$ is

$$f_{U,V}(u,v) = \begin{cases} \frac{1}{\pi(\rho_i^2-\rho_o^2)}, & \rho_i^2 \leq u^2 + v^2 \leq \rho_o^2, \\ 0, & \text{otherwise}. \end{cases}$$  (54)

In the polar coordinate system, we denote the location of Eve by $(\rho, \theta)$. As such, we obtain $u = \rho \cos \theta$ and $v = \rho \sin \theta$. The Jacobian matrix for this coordinate change is given by

$$J(\rho, \theta) = \frac{\partial(u,v)}{\partial(\rho, \theta)} = \begin{bmatrix} \cos \theta & -\rho \sin \theta \\ \sin \theta & \rho \cos \theta \end{bmatrix}. \quad (55)$$

Using (55), the determinant of $J(\rho, \theta)$ is calculated as $|J(\rho, \theta)| = \rho$. Based on Jacobian techniques for the transformation of random variables [32], the joint pdf of $\rho$ and $\theta$ is given by

$$f_{\rho, \theta}(\rho, \theta) = f_{U,V}(u,v)|J(\rho, \theta)| = \begin{cases} \frac{\rho}{\pi(\rho_i^2-\rho_o^2)}, & 0 \leq \theta \leq 2\pi, \rho_i \leq \rho \leq \rho_o, \\ 0, & \text{otherwise}. \end{cases}$$  (56)

Using (56), the marginal pdf of $\rho$ is derived as

$$f_\rho(\rho) = \int_0^{2\pi} f_{\rho, \theta}(\rho, \theta) d\theta = \begin{cases} \frac{2\rho}{\pi(\rho_i^2-\rho_o^2)}, & \rho_i \leq \rho \leq \rho_o, \\ 0, & \text{otherwise}. \end{cases}$$
In order to derive the pdf of $\rho^2$, we denote $\lambda = \rho^2$. As per the rules on the transformation of random variables, the pdf of $\rho^2$ is given by

$$f_{\rho^2}(\rho^2) = \frac{d\rho}{d\lambda} f_{\lambda}(\rho) = \begin{cases} \frac{1}{\rho^4 - \rho^2}, & \rho_1^2 \leq \rho^2 \leq \rho_2^2, \\ 0, & \text{otherwise.} \end{cases} \quad (57)$$

This completes the proof.

REFERENCES

[1] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, “Physical layer security in wireless networks: A tutorial,” IEEE Commun. Mag., vol. 18, no. 5, pp. 66–74, Apr. 2011.

[2] A. Mukherjee and A. L. Swindlehurst, “Robust beamforming for secrecy in MIMO wiretap channels with imperfect CSI,” IEEE Trans. Signal Process., vol. 59, no. 1, pp. 351–361, Jan. 2011.

[3] G. Zheng, P. Arapoglou, and B. Ottersten, “Physical layer security in multibeam satellite systems,” IEEE Trans. Wireless Commun., vol. 11, no. 2, pp. 852–863, Dec. 2011.

[4] H. Wang, X. Zhou, and M. Reed, “Physical layer security in cellular networks: A stochastic geometry approach,” IEEE Trans. Wireless Commun., vol. 12, no. 6, pp. 2776–2787, May 2013.

[5] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, “Physical Layer Security in Downlink Multi-Antenna Cellular Networks,” IEEE Trans. Commun., vol. 62, no. 6, pp. 2006–2021, Jun. 2014.

[6] C. E. Shannon, “Communication theory of secrecy systems,” Bell Syst. Techn. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

[7] A. Wyner, “The wire-tap channel,” Bell Syst. Techn. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[8] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap channel,” IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[9] S. Khisti and G. W. Wornell, “On the target secrecy rate for SISOME wiretap channels,” in Proc. IEEE ICC, Jun. 2014, pp. 987–992.

[10] A. Khisti, S. Dhillon, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, “Applications of LDPC codes to the wiretap channel,” IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[11] D. Kipnis, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, “LDPC codes for the Gaussian wiretap channel,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 532–540, Sep. 2011.

[12] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, “Coding for secrecy: an overview of error-control coding techniques for physical-layer security,” IEEE Signal Process. Mag., vol. 30, no. 5, pp. 41–50, Sep. 2013.

[13] P. K. Gopala, L. Lai, and H. E. Gamal, “On the secrecy capacity of fading channels,” IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[14] S. Shahfiee, N. Liu, and S. Ulukus, “Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 Channel,” IEEE Trans. Inf. Theory, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[15] K. Khisti and G. W. Wornell, “Secure transmission with multiple antennas–Part II: The MIMOME wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[16] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[17] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas I: The MISOME wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[18] A. Parada and R. Bhatia, “Secrecy capacity of SIMO and slow fading channels,” in Proc. IEEE ISIT, Sep. 2005, pp. 2152–2155.

[19] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin. “Wireless information-theoretic security,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[20] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, “Performance of transmit antenna selection physical layer security schemes,” IEEE Signal Process. Lett., vol. 19, no. 6, pp. 372–375, Jun. 2012.

[21] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, “Transmit antenna selection for security enhancement in MIMO wiretap channels,” IEEE Trans. Commun., vol. 61, no. 1, pp. 144–154, Jan. 2013.

[22] W. X. Yuan, N. Yang, R. Malaney, and J. Yuan, “Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels,” IEEE Trans. Wireless Commun., vol. 13, no. 3, pp. 1656–1667, Mar. 2014.

[23] A. Shah and A.M. Haimovich, “Performance analysis of maximal ratio combining and comparison with optimum combining for mobile radio communications with cochannel interference,” IEEE Trans. Veh. Technol., vol. 49, no. 4, pp. 1454–1463, Jul. 2000.

[24] Z. Chen, J. Yuan, and B. Vucetic, “Analysis of transmit antenna selection/maximal-ratio combining in Rayleigh fading channels,” IEEE Trans. Veh. Technol., vol. 54, no. 4, pp. 1312–1321, Jul. 2005.

[25] A. Goldsmith, Wireless Communications, Cambridge, U.K.: Cambridge Univ. Press, 2005.

[26] F. He, H. Man, and W. Wang, “Maximal ratio diversity combining enhanced security,” IEEE Comm. Lett., vol. 15, no. 5, pp. 509–511, May 2011.

[27] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, “Rethinking the secrecy outage formulation: A secure transmission design perspective,” IEEE Commun. Lett., vol. 15, no. 3, pp. 302–304, Mar. 2011.

[28] Y. Abdallah, M. A. Latif, M. Youssef, A. Sultan, and H. El Gamal, “Keys through ARQ: Theory and practice,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 757–751, Sep. 2011.

[29] X. Zhang, X. Zhou, and M. R. McKay, “On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels,” IEEE Trans. Veh. Technol., vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[30] N. J. Young, “Orbits of the unit sphere of L(H, K) under symplectic transformations,” J. Operator Theory 11 (1984), pp. 171–191.

[31] J. S. Gudmundson and I. M. Ryazhik, Table of Integrals, Series and Products, 7th ed., Academic, San Diego, CA, 2007.

[32] A. Leon-Garcia, Probability and Random Processes for Electrical Engineering, 2nd ed. Cambridge, MA: Addison-Wesley, 1994.