Secrecy Transmission on Block Fading Channels: Theoretical Limits and Performance of Practical Codes

M. Baldi*, M. Bianchi*, F. Chiaraluce*, N. Laurenti°, S. Tomasin°, and F. Renna+

Abstract

We consider a system where an agent (Alice) aims at transmitting a message to a second agent (Bob), while keeping a third agent (Eve) in the dark, by using physical layer techniques. For a transmission over frequency non selective block fading channels, we assume that Alice perfectly knows the channel with respect to Bob, but she has only a statistical knowledge of the channel with respect to Eve. We derive bounds on the achievable outage secrecy rates, considering messages spanning either one or many fading blocks. Transmit power is adapted to fading conditions, with a constraint on the average power over the entire transmission. We also focus on the maximum cumulative outage secrecy rate that can be achieved. In order to assess the performance in a practical scenario, we consider transmissions encoded with practical error correcting codes. In particular, we extend the definitions of both security gap and equivocation rate – previously applied to the additive white Gaussian noise channel – to fading channels, taking into account the error rate targets. Bounds on these performance metrics are derived for a block Rayleigh fading channel. Numerical results are provided, confirming the feasibility of the considered physical layer security techniques.

Index Terms

Block fading, capacity bounds, error correcting codes, physical layer security, outage secrecy rate.

* DII, Università Politecnica delle Marche, 60131 Ancona, Italy
° Department of Information Engineering, University of Padova, 35131 Padova, Italy
+ Instituto de Telecomunicações e Departamento de Ciência de Computadores, Faculdade de Ciências da Universidade do Porto, 4169-007, Porto, Portugal

This work was supported in part by the MIUR project ESCAPADE (Grant RBFR105NLC) under the “FIRB-Futuro in Ricerca 2010” funding program.
I. INTRODUCTION

Performance of physical layer security schemes can be assessed either by evaluating secrecy capacity – which assumes, among other things, ideal coding (e.g., Gaussian codewords, infinite length limit) –, or by focusing on practical codes and considering the error probabilities for both the legitimate receiver and the eavesdropper.

For the former approach, in [1] the ergodic secrecy capacity for a fast fading scenario is derived by maximizing the ergodic secrecy rate over all power allocations that meet an average transmit power constraint. A compound parallel Gaussian wiretap channel model, in which the main channel gains are known to all parties, while the eavesdropper gains can take any value within a given finite set, was considered in [2], where a max-min coding strategy is proved to achieve secrecy capacity. In the block fading scenario of [3], only statistics of both the legitimate receiver and the eavesdropper channels are assumed known at the transmitter. Hence, a secrecy throughput is evaluated, that is achieved either with repetition coding, or with a single wiretap code over a finite number of fading blocks. The statistical distribution of the secrecy capacity and the low-rate limit to the secrecy outage probability are derived by the authors in [4], [5] for a set of independently faded parallel wiretap channels, in the OFDM context. In [6] perfect channel state information (CSI) for the main channel and statistical CSI for the eavesdropper channel are assumed: for a fast Rayleigh fading wiretap channel with a multi-antenna transmitter and a single antenna device for both the intended receiver and the eavesdropper (MISOSE channel), the ergodic secrecy capacity is then achieved with an artificial noise injection scheme. Analogously, [7] seeks the maximum secrecy rate of the MISOSE channel under statistical CSI for both the main and the eavesdropper channels.

For the alternative approach of using practical codes, secrecy performance can be measured by the security gap, that compares the signal-to-noise ratios (SNRs) on the main and the eavesdropper channels required to achieve both a sufficient level of secrecy and reliable decoding by the authorized receiver. In [8] the security gap has been derived for additive white Gaussian noise (AWGN) channels. In [9] it is shown that a low security gap can be obtained by using punctured low-density parity-check (LDPC) codes, i.e., by associating the secret information bits to punctured bits. In [10] the authors have proved that similar or better performance can be achieved by resorting to non-systematic codes, obtained through scrambling and codewords.
concatenation. Both LDPC and conventional Bose-Chaudhuri-Hocquenghem (BCH) codes are used for such purpose, the difference being in the involved working SNRs (much smaller for LDPC codes). Practical codes for physical layer security have also been applied over the packet erasure channel [11], where properties of the stopping sets are exploited to achieve secrecy with punctured non-systematic LDPC codes. However, the evaluation of secrecy capabilities for practical codes over fading channels is unprecedented, to the best of our knowledge.

In this paper we consider a scenario where a transmitter, Alice, and a legitimate receiver, Bob, have perfect CSI for their link, while they only have a statistical description of the channel between Alice and the eavesdropper, Eve. All channels are assumed flat block Rayleigh fading, modeling for example a single carrier transmission over a time-varying channel or the transmission of one OFDM symbol over differently faded subcarriers. As the channel gains are represented by continuous random variables, the compound parallel Gaussian wiretap channel model does not apply here [2]. Moreover, a delay-limit, short-term power constraint is imposed on the transmitted signal, thus preventing the leverage of ergodicity of the fading wiretap channel [1]. Therefore, the transmission scenario implies a nonzero secrecy outage probability, and we aim at maximizing the achievable secrecy rates while satisfying a constraint on the secrecy outage probability.

Two approaches are considered for the transmission of a message by Alice: in one case, the message is coded into a single codeword and transmitted over many fading blocks; in the other case, the message is split into sub-messages, each sub-message is encoded separately and transmitted on a different fading block. The first case is denoted as coding across sub-messages (CAS), while the second is denoted as coding per sub-message (CPS).

The main contributions of the paper are:

- the derivation of achievable secrecy rates for delay constrained transmissions over independent Rayleigh block fading channels subject to a secrecy outage probability constraint;
- the joint optimization of power and rate allocation among sub-messages for secrecy rate maximization subject to a constraint on the maximum secrecy outage probability, where the compound parallel Gaussian wiretap channel [2] model cannot be applied;
- the derivation of closed-form expressions of the outage secrecy rates for both CPS and CAS scenarios, otherwise previously available only by Monte Carlo methods [3];
- the non-trivial performance comparison between CPS and CAS, since their outage secrecy
rates are not immediately comparable;
• the derivation of bounds on the error rates for Bob and Eve with practical codes over Rayleigh block fading channels;
• the extension of the security gap and the equivocation rate metrics from AWGN to block fading channels; we use these metrics to relate the asymptotic performance provided by the analysis based on capacity and the actual performance of practical coding schemes.

The paper is organized as follows. In Section II we introduce the system model, and in Section III we derive theoretical bounds on the achievable rates, for both CAS and CPS. In Section IV we refer to the error rate as a further metric to assess the physical layer security on channels with fading, when practical codes are applied. Section V provides several numerical examples for both approaches and the various scenarios we have considered. Finally, Section VI concludes the paper.

II. SYSTEM MODEL

We consider a scenario with three agents: Alice, Bob, and Eve. Alice aims at transmitting a secret message to Bob, while Eve attempts to intercept it.

All channels are modeled as flat block fading, i.e., they remain constant for the duration of $M$ transmitted symbols and then they change for the next $M$ symbols. The resulting scheme is reported in Fig. 1 where $h_k$ is the complex (baseband equivalent) channel coefficient between Alice and Bob upon transmission of block $k$, and $g_k$ is the channel coefficient between Alice and Eve at the same time. Let us define the vector (denoted in boldface) $\mathbf{P} = [P_1, \ldots, P_K]$, where $P_k$ is the power transmitted by Alice during the $k$-th fading block, $k = 1, 2, \ldots, K$. We
denote by $H_k = |h_k|^2$, and $G_k = |g_k|^2$ the corresponding power gains, and consider Rayleigh fading channels, so that $H_k$ and $G_k$ are exponentially distributed with means $\alpha^{(B)}$ and $\alpha^{(E)}$, respectively. The thermal noise variance of both channels is assumed to be unitary.

As stated in Section II, two transmission approaches are considered:

**Coding per sub-message (CPS):** In this case Alice first splits the message into $K$ sub-messages; each of them is encoded into $M$ symbols and then transmitted on a different fading block. The secrecy rate for sub-message $k = 1, 2, \ldots, K$ is $R_k$.

**Coding across sub-messages (CAS):** In this case the message is coded and transmitted on $K$ fading blocks. The secrecy rate in this case is the same in all blocks and is denoted as $R_1$.

In order to ease notation, we denote by $\mathcal{K}$ the set of indexes of the secrecy rates for the two schemes, i.e.,

$$\mathcal{K} = \begin{cases} 
1 & \text{for CAS}, \\
1, 2, \ldots, K & \text{for CPS}.
\end{cases}$$

### III. Secrecy Rate Bounds

We first consider the performance that can be achieved in the above described scenarios by assessing bounds on their secrecy rate. In particular, we suppose that Alice knows the channel with respect to Bob before transmission, while the Alice-Eve channel is unknown\footnote{In Appendix A we consider the case where also the Alice-Bob channel is known only statistically.}. This is a very realistic assumption, since in most of the practical cases we do not know the eavesdropper precise location, thus we can only make assumptions on the statistics of her channel. In this situation we cannot ensure perfect secrecy, but we can impose that the probability that the eavesdropper can obtain non negligible information on the secret message (secrecy outage probability) is below a given threshold $\varepsilon$, that can be chosen to ensure a desired level of secrecy. We then aim at allocating the power and rates for the two coding schemes in order to maximize the secrecy rate while ensuring the target outage probability.

Let us define the vector $\mathbf{R} = [R_1, \ldots, R_K]$. Let $p_s(P, R)$ be the secrecy outage probability for a given power and secrecy rate allocation, i.e., the probability that either Bob cannot reliably decode the message or Eve succeeds in partially decoding the message. We aim at finding $\mathbf{R}$
and $P$ that satisfy the following constraints

$$p_s(P, R) \leq \varepsilon,$$

(2a)

$$\frac{1}{K} \sum_{k=1}^{K} P_k \leq P_{\max},$$

(2b)

$$P_k \geq 0, \quad k = 1, 2, \ldots, K,$$

(2c)

$$R_k \geq 0, \quad k \in \mathcal{K}.$$  

(2d)

Constraint (2a) sets the maximum allowed secrecy outage probability to $\varepsilon$; constraint (2b) imposes a bound on the average transmit power to $P_{\max}$, while (2c) and (2d) ensure that the obtained powers and rates are not negative.

We are also interested in finding the maximum outage secrecy rate that can be achieved, as the solution of the following problem

$$\max_{\{P_k, R_k\}} \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} R_k,$$

subject to (2).

A. Coding Across Sub-Messages

In this case, we assume that coding is performed by Alice across the $K$ sub-messages and the secrecy outage probability can be written as \[1\]

$$p_s(P, R_1) = \mathbb{P}\left[ \frac{1}{K} \sum_{k=1}^{K} \left[ \log(1 + H_k P_k) - \log(1 + G_k P_k) \right] \leq R_1 \right],$$

(4)

where $\log(\cdot)$ is the base-2 logarithm and $\mathbb{P}[\cdot]$ denotes the probability operator, in this case with respect to the random variables $G_k$, while channel gains $H_k$ are assumed known.

Let $\Phi(P, R_1) = 2^{\sum_{k=1}^{K} \log(1+H_k P_k) - K R_1}$ and let us define

$$\zeta(P) = \prod_{k=1}^{K} P_k^{\alpha_{E}}, \quad \phi(P) = \left[ \prod_{k=1}^{K} \left( \frac{1}{P_k^{\alpha_{E}}} \right) \right]^{-1}.$$  

(5)

As derived in Appendix B the secrecy outage probability can be written as

$$p_s(P, R_1) = 1 - \frac{\zeta(P)}{\phi(P)} \left\{ \Phi(P, R_1) \mathcal{G} \left( \frac{\Phi(P, R_1)}{\phi(P)} \right) \right\} - \mathcal{G} \left( \frac{1}{\phi(P)} \right),$$

(6)
where

\[ G(a) = \mathcal{H}_{1,K+1}^{K,1} \begin{bmatrix} \{0, 1, 0\} \\ \{(0, 1, 0)\}_{k=1,\ldots,K}, (-1, 1, 0) \end{bmatrix} \]  

(7)

and \( \mathcal{H}[\cdot] \) is the generalized Fox H-function, whose definition is recalled in Appendix B.

Then (2a) can be rewritten as

\[ 0 \leq R_1 \leq p_s^{-1}(P, \varepsilon), \]

(8)

where \( p_s^{-1}(P, \varepsilon) \) is the inverse of (6) with respect to \( R_1 \).

When the outage secrecy rate is maximized, \( R_1 \) equals the right hand side in (8), therefore we can remove \( R_1 \) from the optimization variables and the maximum outage secrecy rate problem (3) can be rewritten as

\[ \frac{1}{K} \max_P p_s^{-1}(P, \varepsilon), \]

(9)

subject to (2b) and (2c).

This problem cannot be solved in closed form and we must resort to numerical methods. Examples will be given in Section V.

B. Coding Per Sub-Message

In this case, each sub-message is coded independently of the others, with a target secrecy rate \( R_k \). The secrecy outage probability is given by

\[ p_s(P, R) = 1 - \prod_{k=1}^{K} (1 - p_k), \]

(10)

where \( p_k \) is the secrecy outage probability for sub-message \( k \), given that the actual realization of \( H_k \) is known, i.e.,

\[ p_k = \mathbb{P} \left[ \log(1 + H_k P_k) - \log(1 + G_k P_k) \leq R_k \right] \]

\[ = \begin{cases} 1 \\ 1 - F_G \left( \frac{1 + H_k P_k}{P_k 2^{R_k}} - \frac{1}{P_k} \right) \end{cases} \]

(11)

\[ = \begin{cases} 1 \\ 1 - F_G \left( \frac{1 + H_k P_k}{P_k 2^{R_k}} - \frac{1}{P_k} \right) \end{cases} \] \text{, otherwise}

and \( F_G(x) \) denotes the cumulative distribution function (CDF) of the eavesdropper power gain \( G_k \) over the \( k \)-th block, which is the same for all blocks.
For the Rayleigh fading assumptions on the channel we obtain
\[ p_s(P, R) = 1 - \prod_{k=1}^{K} \left\{ 1 - \exp \left[ -\frac{1}{\alpha(E)} \left( \frac{1 + H_k P_k}{P_k 2 R_k} - \frac{1}{P_k} \right) \right] \right\}. \] (12)

Note that the secrecy outage probability for each sub-message \( k \) is a function of both the power \( P_k \) and the target secrecy rate \( R_k \). Therefore, the rate maximization problem (3) cannot be formulated as a special instance of the compound parallel Gaussian wiretap channel [2], since the allocation of the target secrecy rates \( R_k \) adds \( K \) variables to the rate maximization problem. In fact, constraint (2a) can be met by different sets of rates.

As for the CAS case, the secrecy rates \( R_k \) are related to the transmit power. In particular, we restrict the constraints (2c)–(2d) to hold without equality, i.e.,
\[ P_k > 0, \quad R_k > 0. \] (13)
and we denote by \( \bar{p}_k \) the target secrecy outage probability for each sub-message, i.e.
\[ \exp \left[ -\frac{1}{\alpha(E)} \left( \frac{1 + H_k P_k}{P_k 2 R_k} - \frac{1}{P_k} \right) \right] = \bar{p}_k. \] (14)

We then have the following result.

**Theorem 1:** For any \( \nu > 0 \), let us define \( \bar{\alpha}_k = -\alpha(E) \ln \bar{p}_k, A_k = \bar{\alpha}_k \nu H_k, B_k = \nu (\bar{\alpha}_k + H_k) \) and \( C_k = \nu - H_k + \bar{\alpha}_k \). For a given set of outage probabilities \( \{\bar{p}_k\} \), if \( C_k < 0, \forall k \), the power allocation \( \{P_k^*\} \) that solves the maximization problem (3) with CPS, under constraints (2a), (2b) and (13), with secrecy outage probability as in (12), satisfies
\[ P_k = -B_k + \sqrt{B_k^2 - 4A_k C_k} \] (15)
where \( \nu > 0 \) is such that (2b) is satisfied.

The corresponding secrecy rate is
\[ \sum_{k=1}^{K} \log \frac{1 + H_k P_k}{\bar{\alpha}_k P_k + 1}. \] (16)

**Proof:** See Appendix C

Therefore, the maximum secrecy rate ensuring a secrecy outage probability not greater than \( \varepsilon \) is obtained by solving
\[ \max_{P, \nu} \sum_{k=1}^{K} \log \frac{1 + H_k P_k}{\bar{\alpha}_k P_k + 1}. \] (17)
subject to 

\[ 1 - \prod_{k=1}^{K} (1 - \bar{p}_k) \leq \varepsilon, \]  

(18)

(15), (25), and (13). The solution of these problems requires numerical methods. Note however that Theorem 1 has allowed a strong reduction of the unknowns, from \( 2K \) in the original problem formulation (3) to \( (K + 1) \) in the formulation (17).

IV. SECRECY PERFORMANCE METRICS WITH PRACTICAL CODES

The analysis in Section III relies on the assumption that codes achieve capacity and, in this sense, it provides an upper bound on the performance reachable by using practical codes. On the other hand, in order to measure the efficiency of practical schemes, further issues should be included in the analysis. In the following, we consider a system where Alice scrambles the message and encodes the result with a systematic code before transmission. Scrambling has been shown [10], [12], [13] to be a useful tool to implement security at the physical layer over the AWGN channel, and is practically feasible with standard equipment [14]. Moreover, we assume that Eve uses the best possible decoder, that is, the maximum likelihood (ML) decoder.

In the considered system, when a vector \( r \) is received, the code \( C \) may be able to correct all the errors induced by the channel, thus recovering the transmitted codeword \( c \). This is what occurs for Bob with a very high probability. Concerning Eve, she performs ML decoding on \( r \) and obtains a wrong codeword \( c' \neq c \) with probability \( p^{(E)}(\gamma^{(E)}) \approx 1 \). Despite this, ML decoding provides Eve with an a-posteriori probability about the transmitted codeword \( c \). In fact, even when Eve’s ML decoder fails to correct all errors, she still has some partial information, since likelihood-based decoding provides the a-posteriori probability of each codeword. Since in general these probabilities are different each other, it is clear that the system does not achieve perfect secrecy. On the other hand, Eve still has uncertainty on the transmitted codeword, as picking just the ML codeword yields a frame decoding error probability close to one. This means that, for a fraction of the received frames equal to \( p^{(E)}(\gamma^{(E)}) \approx 1 \), Eve must perform at least two attempts to obtain the correct transmitted codeword. This amount of uncertainty, though being small, defines a weak secrecy condition, similar to that considered in [15], which can be exploited to achieve security. For this purpose, we consider the hypothesis of perfect scrambling, which can be approached by using real scramblers and descramblers [10], [14], acting on \( L \)
consecutive frames. Under this hypothesis, each set of $L$ information vectors \( \{ u_1, u_2, u_3, \ldots, u_L \} \) is linearly combined into a set of $L$ scrambled information vectors \( \{ u'_1, u'_2, u'_3, \ldots, u'_L \} \), which are then encoded separately into $L$ codewords \( \{ c_1, c_2, c_3, \ldots, c_L \} \). Only if all of them are correctly decoded, \( \{ u'_1, u'_2, u'_3, \ldots, u'_L \} \) can be correctly descrambled into \( \{ u_1, u_2, u_3, \ldots, u_L \} \), otherwise the error probability on the bits of \( \{ u_1, u_2, u_3, \ldots, u_L \} \) is 0.5. Hence, this achieves an effect which is similar to an all-or-nothing transform [16]. Thanks to the use of concatenated scrambling, even if Eve only needs to perform two attempts for recovering each wrongly decoded codeword, the total number of attempts she needs, on average, prior to be able to correctly descramble the set of $L$ concatenated frames becomes \( 2^{p(E)(\gamma(E))} \cdot L \), which can be made arbitrarily large by increasing $L$. This is paid in terms of some increased latency, but allows to achieve any desired security level, though starting from a weak secrecy condition.

A very useful metric is the security gap, which is based on the evaluation of the error rate experienced by the authorized receiver and the eavesdropper. This metric has already been applied on the AWGN channel [9], [10], [12], [13] and is here extended to the case of block fading channels, for the first time to the best of the authors’ knowledge. It allows to consider specific transmission (and reception) techniques, as well as specific channel codes, in order to assess and compare their security performance. Another useful metric to assess the gap between theoretical limits and the performance of practical codes is the equivocation rate [17]. Through an outage-based approach, we also extend this metric to the present context.

Let
\[
\gamma^{(B)} = \left[ \gamma_1^{(B)}, \gamma_2^{(B)}, \ldots, \gamma_K^{(B)} \right] = [H_1 P_1, H_2 P_2, \ldots, H_K P_K],
\]
be the vector of random SNRs experienced by Bob for the message transmitted by Alice. Similarly, let
\[
\gamma^{(E)} = \left[ \gamma_1^{(E)}, \gamma_2^{(E)}, \ldots, \gamma_K^{(E)} \right] = [G_1 P_1, G_2 P_2, \ldots, G_K P_K]
\]
be the vector of random SNRs experienced by Eve for the same message. Let $p^{(B)}(\gamma^{(B)})$ and $p^{(E)}(\gamma^{(E)})$ be the frame error rates (FERs) experienced by Bob and by Eve, respectively, i.e., the probability that at least one message bit is in error.

Under the practical viewpoint we propose, the transmission is considered successful and secure if the following two conditions are satisfied:
\[
p^{(B)}(\gamma^{(B)}) \leq \delta,
\]

(21a)
\[ p^{(E)}(\gamma^{(E)}) \geq 1 - \eta, \]  

(21b)

where \( \delta \) and \( \eta \) represent two small threshold values.

We note that condition (21a) can be met through a suitable power allocation, since Bob’s channel is known. Condition (21b), instead, can only be met statistically, that is, by tolerating a small secrecy outage probability, since Eve’s channel state is not known. An approach for studying the case in which also Bob’s channel is fading and known only in statistical terms is reported in Appendix A.

We indicate by \( \gamma_{\delta} \) the minimum value of \( \gamma^{(B)} \) at which \( p^{(B)}([\gamma^{(B)}, \gamma^{(B)}, \ldots, \gamma^{(B)}]) = \delta \). On the other hand, since we assume that Alice does not know the channel with respect to Eve, we consider an outage approach for the definition of the security gap. In fact, \( p^{(E)}(\gamma^{(E)}) \) is a random variable, whose distribution depends on the average SNR of Eve’s channel. The mean SNR of the Alice to Eve channel is

\[ \bar{\gamma}^{(E)} = \frac{1}{K} \sum_k \alpha^{(E)} P_k. \]  

(22)

We are interested in finding the maximum value of \( \bar{\gamma}^{(E)} \), \( \bar{\gamma}^{(E)}_{\text{max}} \), for which the probability that \( p^{(E)}(\gamma^{(E)}) < 1 - \eta \) is not greater than \( \zeta \), i.e.,

\[ \bar{\gamma}^{(E)}_{\text{max}} = \frac{1}{K} \sum_k P_k \cdot \max\{\alpha^{(E)} : \mathbb{P}[p^{(E)}(\gamma^{(E)}) < 1 - \eta] \leq \zeta\}. \]  

(23)

Aiming to extend the original definition of security gap given for the AWGN channel in [8] to the fading scenario, we define the \( \zeta \)-outage security gap as

\[ S_g^{(\zeta)}(\delta, \eta) = \frac{\gamma_{\delta}}{\bar{\gamma}^{(E)}_{\text{max}}}. \]  

(24)

In the following we derive bounds on the \( \zeta \)-outage security gaps for the CPS and CAS cases and discuss their power optimization.

A. Computation of \( \bar{\gamma}^{(E)}_{\text{max}} \) and \( \gamma_{\delta} \)

Computation of \( \bar{\gamma}^{(E)}_{\text{max}} \) for CPS: When coding is applied separately on each sub-message, condition (21b) must hold on each block. In principle, full variable rate coding requires a different code on each block. In this section, however, we use a linear block code with fixed length and rate, properly chosen, for each sub-message and for the whole duration of the transmission.
With a slight abuse of notation, we will denote by $p^c(\cdot)$ the FER over a single message. Hence the eavesdropper outage probability becomes
\[
\mathbb{P} \left[ \bigcup_{k=1}^{K} \left\{ p^c(\gamma^E_k) < 1 - \eta \right\} \right] = 1 - \prod_{k=1}^{K} \left( 1 - \mathbb{P}[p^c(\gamma^E_k) < 1 - \eta] \right) \\
= 1 - \prod_{k=1}^{K} \left( 1 - \mathbb{P}[\gamma^E_k > \gamma_\eta] \right), \tag{25}
\]
where $\gamma_\eta$ is the SNR that ensures a FER $1 - \eta$ for Eve’s decoding. In Appendix D we derive a lower bound on the value of $\gamma_\eta$ for BPSK transmission with several decoders, which allows to estimate the best performance achievable by Eve.

Let $O_k$ be the event that $\gamma^E_k > \gamma_\eta$. From the Rayleigh fading assumption we have
\[
\mathbb{P}[O_k] = \exp \left( -\frac{\gamma_\eta}{\beta_k \alpha^E} \right) 
\]
and hence (25) becomes
\[
\mathbb{P} \left[ \bigcup_{k=1}^{K} \left\{ p^c(\gamma^E_k) < 1 - \eta \right\} \right] = 1 - \prod_{k=1}^{K} \left( 1 - \mathbb{P}[O_k] \right) = 1 - \prod_{k=1}^{K} \left[ 1 - \exp \left( -\frac{\gamma_\eta}{\beta_k \alpha^E} \right) \right]. \tag{27}
\]

By exploiting these results, and the knowledge of the transmission (and reception) technique, we can compute $\bar{\gamma}^{(E)}_{\text{max}}$ for which condition (21b) is satisfied for a given power allocation.

**Computation of $\bar{\gamma}^{(E)}_{\text{max}}$ for CAS:** When CAS is considered, we are interested in finding a worst-case estimation of the error probability for Eve. As a closed form expression is not available, we resort to a lower bound, by defining $\gamma_M = \max_k \{ \gamma^E_k \}$, and by letting $p^c(\gamma^E)$ be the error probability achieved by Eve for a given channel realization $\gamma^E$. We consider the lower bound
\[
p^c(\gamma^E) \geq p^c([\gamma_M, \gamma_M, \ldots, \gamma_M]), \tag{28}
\]

hence (23) becomes
\[
\bar{\gamma}^{(E)}_{\text{max}} = \frac{1}{K} \sum_{k} P_k \cdot \max \{ \alpha^E : \mathbb{P}[\gamma_M \geq \gamma_\eta] \leq \zeta \} \tag{29}
\]
and we aim at computing $\mathbb{P}[\gamma_M \geq \gamma_\eta]$.

We have
\[
\mathbb{P}[\gamma_M \geq \gamma_\eta] = \mathbb{P} \left[ \bigcup_{k=1}^{K} O_k \right] = 1 - \prod_{k=1}^{K} \left( 1 - \mathbb{P}[O_k] \right). \tag{30}
\]
Therefore, we obtain again (27), though in this case it results from the use of a lower bound based on $\gamma_M$, while in the case of CPS it is given by an exact derivation. So, with such specification, (27) can be used to model both CPS and CAS scenarios, and we will not distinguish between the two cases for the subsequent analysis.

**Computation of $\gamma_\delta$:** For modeling Bob’s channel, which is supposed to be known, we only need to compute $\gamma_\delta$, that is, the threshold channel gain which allows to satisfy the constraint (21b). The case in which Bob’s channel is known only in statistical terms is more involved, and addressed in Appendix A.

We now refer to ML decoding also for Bob, and resort to an upper bound on the probability $p^{(B)}(\gamma)$ for a given SNR $\gamma$ from Alice to Bob, obtained by the union bound. In fact, in the high SNR region, the union bound is known to provide a tight bound on the performance of ML and ML-like decoders.

Consider a linear block code with codeword length $N$, and let $d_{\text{min}}$ denote the code minimum distance and $A_w$ the number of codewords with weight $w \leq N$. The union bound approximation yields

$$p^{(B)}(\gamma) \leq \sum_{w=d_{\text{min}}}^{N} A_w Q\left(\sqrt{2\gamma w}\right),$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt$ is the complementary CDF of the zero-mean, unit-variance Gaussian distribution. By only considering a subset of the weight spectrum of the code, we get a truncated union bound approximation. In particular, by only considering the minimum weight codewords we get

$$p^{(B)}(\gamma) \lesssim A_{d_{\text{min}}} Q\left(\sqrt{2\gamma d_{\text{min}}}\right).$$

By imposing that the right-hand side of (31) or (32) equals $\delta$, and solving for $\gamma$, we obtain $\gamma_\delta$. It must be noted that (31) provides a tight bound only for large values of $\gamma$, that is, small values of $p^{(B)}(\gamma)$, which, however, occur for Bob.

**B. Power allocation and security gap**

In this section we consider fixed secrecy rate transmissions, regardless of the channel state. On the other hand, by varying the power allocation we can alter the reliability of reception at Bob and Eve. Hence, in a parallel to the security rate regions, we see that conditions (21) define regions for power allocation strategies that ensure reliable and secure communications.
In order to satisfy Bob’s reliability condition (21a), Alice transmits at minimum power levels

\[ P_k = \frac{\gamma \delta}{H_k}. \quad (33) \]

Based on (33), Alice finds the optimal power allocation, and checks whether the power constraint (2b) is satisfied. In the latter case, transmission occurs, and the security gap results from the need to meet the security condition (21b). Instead, if the power constraint is not satisfied, Alice skips the transmission, since the reliability target cannot be achieved.

C. Outage equivocation rate

In [17] the level of confidentiality obtained in a coded transmission over an AWGN channel is evaluated through its equivocation rate, that is, the difference between the code rate and the information rate at the eavesdropper. In this section we extend the notion of equivocation rate to the fading channel scenario through an outage formulation, and derive lower bounds for both considered coding schemes.

We consider a coded transmission with constant rate \( R_c \), and allocated powers \( \{P_k\} \) that are assumed to satisfy condition (21a) for reliable decoding. Since all information bits are intended for confidential transmission, we define the \( \xi \)-outage equivocation rate as follows

\[ R^{(\xi)}_E = R_c - I^{(\xi)}_E, \quad (34) \]

where the outage information rate at the eavesdropper for the CPS scheme is given by

\[ I^{(\xi)}_E = \min \left\{ \beta : \mathbb{P} \left[ \bigcup_k \{I_{E,k} \geq \beta\} \right] \leq \xi \right\} \quad (35) \]

while for the CAS scheme is

\[ I^{(\xi)}_E = \min \left\{ \beta : \mathbb{P} \left[ \frac{1}{K} \sum_k I_{E,k} \geq \beta \right] \leq \xi \right\} \quad (36) \]

and \( I_{E,k} \) is the eavesdropper information rate for sub-message \( k \). By choosing the symbol constellation independently of the channel state, an upper bound on \( I_{E,k} \) can be written as \( I_{E,k} \leq C(\gamma^{(E)}_k) \) where \( C(\gamma) \) yields the maximum information rate through a Gaussian channel as a (monotonically increasing) function of the SNR \( \gamma \), and its expression depends on the adopted input constellation.
Thus, for the CPS scheme, the probability in (35) is bounded as
\[
\mathbb{P} \left[ \bigcup_k \{ I_{E,k} \geq \beta \} \right] \leq \mathbb{P} \left[ \bigcup_k \{ C(\gamma_k) \geq \beta \} \right] \\
= \mathbb{P} \left[ \gamma_M \geq C^{-1}(\beta) \right] \\
= 1 - \prod_{k=1}^{K} \left( 1 - \exp \left( -\frac{C^{-1}(\beta)}{P_k \alpha_k} \right) \right),
\]
(37)
where the last steps are analogous to (26)–(27).

Similarly, for the CAS scheme we have
\[
\mathbb{P} \left[ \frac{1}{K} \sum_k I_{E,k} \geq \beta \right] \leq \mathbb{P} \left[ \frac{1}{K} \sum_k C(\gamma_k) \geq \beta \right] \\
\leq \mathbb{P} \left[ \gamma_M \geq C^{-1}(\beta) \right] \\
= 1 - \prod_{k=1}^{K} \left( 1 - \exp \left( -\frac{C^{-1}(\beta)}{P_k \alpha_k} \right) \right).
\]
(38)
Hence, in the CAS case, the bound is looser than in the CPS case.

By using (37) and (38) in (35) and (36), respectively, we then obtain a lower bound on the \( \xi \)-outage equivocation rate as follows
\[
R_{e}(\xi) \geq R_c - \min \left\{ \beta : \prod_{k=1}^{K} \left( 1 - \exp \left[ -\frac{C^{-1}(\beta)}{P_k \alpha_k} \right] \right) \geq 1 - \xi \right\}.
\]
(39)

The outage equivocation rate, or its lower bound, can be compared to the code rate \( R_c \), as well as to the achievable outage secrecy rates derived in Section III, with the latter representing an upper bound when reliable decoding by Bob is achieved. However, here we prefer to give a tighter upper bound
\[
R_{e}(\xi) \leq C_{s}(\xi)
\]
(40)
where \( C_{s}(\xi) \) is the outage secrecy capacity of the fading wiretap channel with a constellation constrained input. This can be derived analogously to the AWGN wiretap channel case [18], [19], with \( H \) and \( G \) being, respectively, the main and eavesdropper channels gains, i.e.,
\[
C_{s}^{\text{AWGN}} = \max_{0 \leq P \leq P_{\text{max}}} \{ C(PH) - C(PG) \}.
\]
(41)
We then obtain
\[
C_{s}(\xi) = \max_{\left( P_k : \frac{1}{K} \sum_k P_k \leq P_{\text{max}} \right)} \max \left\{ \beta : \mathbb{P} \left[ \frac{1}{K} \sum_k C(P_k H_k) - C(P_k G_k) \leq \beta \right] \leq \xi \right\}.
\]
(42)
which can be upper bounded as
\[
C_s^{(\xi)} \leq \max_{\{P_k\} : \frac{1}{K} \sum_k P_k \leq P_{\text{max}}} \max \left\{ \beta : \mathbb{P} \left[ \bigcap_k \left\{ C(\gamma_k^{(B)}) \geq \frac{1}{K} \sum_k C(\gamma_k^{(B)}) - \beta \right\} \right] \leq \xi \right\}
\]
\[
= \max_{\{P_k\} : \frac{1}{K} \sum_k P_k \leq P_{\text{max}}} \max \left\{ \beta : \exp \left[ - \sum_k \frac{C^{-1} \left( \frac{1}{K} \sum_k C(\gamma_k^{(B)}) - \beta \right)}{P_k \alpha^{(E)}} \right] \leq \xi \right\}
\]
\[
= \max_{\{P_k\} : \frac{1}{K} \sum_k P_k \leq P_{\text{max}}} \left[ \frac{1}{K} \sum_k C(\gamma_k^{(B)}) - C \left( - \frac{\ln \xi}{\sum_k \frac{1}{P_k \alpha^{(B)}}} \right) \right].
\]

V. Numerical Results

On the basis of the theoretical analysis developed in the previous sections, we provide here some examples, under different kinds of fading channel conditions.

A. Security gap and equivocation rate

Let us consider the case of \( N = 128 \), and a channel code rate \( 1/2 \), that is, 64 information bits per block. More precisely, we focus on a \((128, 64)\) extended BCH (eBCH) code with minimum distance \( d_{\text{min}} = 22 \). The performance achievable by using this code can be evaluated by comparing it with the sphere packing bound (SPB).

Considering modern coding schemes, like LDPC codes, could seem a better choice. However, it must be taken into account that, for short code lengths, soft-decision decoding algorithms able to approach ML decoding performance have reasonable complexity. In these conditions, Bob’s error correcting performance is excellent, and is not outperformed by iteratively decoded LDPC codes with the same length and rate. Additionally, Bob uses an ML-like decoder, which is the best one and the same as that of Eve. This way, the security gap is kept small. On the other hand, ML-like decoding becomes intractable for longer codes, while LDPC codes with soft-decision iterative decoding achieve good performance with limited complexity. This allows Bob to work at a lower SNR, but the gap to the SPB increases. Hence, since we assume that Eve is always able to use the best decoder, the security gap becomes larger than for the case of short codes.

For these reasons, we consider the \((128, 64)\) eBCH code, and compute its corresponding union bound through (31). Shannon’s SPB is computed as described in Appendix D, and it is referred to any \((128, 64)\) linear block code under ML decoding. Fig. 2 reports the achievable performance, and the corresponding bounds, in terms of FER over the AWGN static channel, as a function
of the channel gain $\gamma$. The performance of the eBCH code under ML decoding is obtained as in [20]. From the figure we observe that the ML decoding performance is tightly upper bounded by the union bound in the high SNR region, and tightly lower bounded by Shannon’s SPB in the low SNR region. This confirms that the two bounds are well suited to model the performance achievable by Bob and Eve, respectively. We also report, for the sake of comparison, the performance achieved by using other decoders. Soft-decision decoding of the eBCH code has been implemented by following the approach proposed in [21], while hard-decision decoding of the same code has been simply estimated by using the closed form expression for bounded distance decoders [22]. We have also included the performance of an LDPC code, with the same length and dimension, designed through the Progressive Edge Growth algorithm [23], and decoded through the logarithmic version of the Sum-Product Algorithm [24]. Shannon’s SPB provides a lower bound for all the considered schemes, so it actually represents a reliable and conservative tool for modeling Eve’s performance. Instead, when Bob uses other decoders than ML, his performance can be rather far from the union bound. In this case, the security gap must be increased by a suitable margin, which depends on the specific decoding algorithm. By focusing on ML decoding and using the upper and lower bounds, we can estimate $\gamma_\delta$ and $\gamma_\eta$. 

Fig. 2. Performance and bounds for codes with $N = 128, K = 64$ over a non-fading channel with SNR $\gamma$. 

June 11, 2013 DRAFT
For example, if $\delta = 10^{-6}$ and $\eta = 0.1$, we have $\gamma_\delta = 0.8$ dB and $\gamma_\eta = -4.8$ dB.

If we consider that Bob’s channel is fading but its state is known, we can use the derivations reported in Section IV-B and suppose that Alice chooses the optimal power allocation strategy with respect to Bob’s channel. So, by knowing Bob’s channel gain, she exploits (33) and checks that power constraint (2b) is verified. For both CAS and CPS, by (27) we impose $\zeta = 10^{-2}$ and find the maximum value of $\alpha^{(E)}$ from which $\bar{\gamma}^{(E)}_{\text{max}}$ is obtained, according to (29). We have simulated 10,000 realizations of Bob’s fading channel, with $K = 4, 8, 16, 32$, and we have assumed the same value of $K$ also for Eve’s channel. The maximum total power transmitted by Alice is the same as for the case without fading on Bob’s channel. The resulting CDF of the security gap is shown in Fig. 3. The average security gap, in these three cases, is $14.68$ dB, $15.84$ dB, $16.94$ dB and $17.93$ dB for $K = 4, 8, 16$ and $32$, respectively.

We can compare this scenario with that in which only Eve’s channel is fading, while Bob’s channel is deterministic (i.e., a known constant coefficient). The latter case is considered in Table I where we report the values of $\bar{\gamma}^{(E)}_{\text{max}}$ and $S_g^{(C)}$ for several fading conditions (i.e., different values of $K$) on Eve’s channel. As expected, we observe that the security gap is lower than the average security gap for the case with fading on Bob’s channel. The other columns of Table I will be
explained in Appendix A, where also Bob’s channel will be considered fading and known only in statistical terms.

As a further benchmark, we compute the equivocation rate by following the derivation reported in Section IV-C. For the sake of simplicity, we consider uniform power allocation, hence \( \gamma_k(B) = \gamma(B) \), \( P_k = \alpha(E) = \bar{\gamma}(E) = \gamma(B)/S_g \). Under these hypotheses, the two bounds (39) and (43) respectively become

\[
R_e(\xi) \geq R_c - C \left( -\bar{\gamma}(E) \ln \left( 1 - (1 - \xi)^{1/K} \right) \right), \tag{44}
\]

\[
C_s(\xi) \leq \max_{\gamma \leq \bar{\gamma}(B)} \left[ C(\gamma) - C \left( -\gamma \ln \frac{\xi}{KS_g} \right) \right]. \tag{45}
\]

For BPSK input, the expression of \( C(\gamma) \) in Eqs. (37) and following is given by

\[
C(\gamma) = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{-\frac{(y-\sqrt{\gamma})^2}{2}} \log(1 + e^{-2y\sqrt{\gamma}}) dy. \tag{46}
\]

By using these expressions, and considering \( \gamma(B) = \gamma_0 = 0.8 \) dB, we have computed \( R_e(\xi) \) and \( C_s(\xi) \), as functions of \( \tilde{\gamma}(E) \), for \( \xi = 0.01, R_e = 1/2 \) and several values of \( K \). Results are reported in Fig. 4. As expected, we observe that, for decreasing values of \( \tilde{\gamma}(E) \), the \( \xi \)-outage equivocation rate approaches the BPSK-input-constrained \( \xi \)-outage secrecy capacity, and the influence of \( K \) tends to vanish.
Fig. 4. $\xi$-outage equivocation rate and BPSK-input-constrained $\xi$-outage secrecy capacity for $\gamma^{(B)} = \gamma^d = 0.8$ dB, $R_c = 1/2$ and $\xi = 0.01$.

B. Secrecy rate: coding per sub-message

In this section, we show numerical examples of the secrecy rates that can be achieved over block fading channels with CPS. We consider a simple case in which the secret message is transmitted over only two sub-messages (i.e., $K = 2$) with independent coding over each sub-message, as described in Section III-B. The secrecy outage probability is guaranteed to be less than the threshold $\varepsilon = 0.01$ and the average power per block is $P_{\text{max}}$.

The optimal values of the transmission secrecy rates for each of the two sub-messages are determined as from Theorem 1 and for three different power allocation strategies: a) equal power distribution among sub-messages, b) water-filling [25] power distribution with respect to Bob’s channel, and c) optimal power allocation, as from (15) and (17).

Fig. 5 shows the contour lines of the secrecy rates obtained with the different power allocations described above, as a function of the power gains of Bob’s channel. The eavesdropper average power gain is such that $\alpha^{(E)} P_{\text{max}} = 0.05$ for each block. As expected from the symmetry of the problem, the three strategies provide similar performance when the two blocks have similar gains, as all the three methods equally split the power between the two blocks. On the other hand,
Fig. 5. Achievable secrecy rates with CPS and (a) equal power (solid lines) and waterfilling (dashed lines), (b) optimal power allocation, for different values of Bob’s channel gains. In all plots, $\varepsilon = 0.01$, and $\alpha^{(E)} P_{\text{max}} = 0.05$.

Fig. 6. (a) Achievable secrecy rates with CPS and (b) fraction $P_1/(2P_{\text{max}})$ of the available power that is allocated to $k = 1$. In all plots, $\varepsilon = 0.01$, $\alpha^{(E)} P_{\text{max}} = 0.05$ and $H(2)P_{\text{max}} = 2$ dB.

when the channel gains at Bob are highly unbalanced, equal power allocation yields a secrecy rate that is much lower than that obtained with the optimal solution, whereas water-filling still provides secrecy rates close to optimal. Water-filling loses against the optimal solution in the intermediate region, as it is possible to observe from Fig. 5(a), in which the secret rates are shown for a specific value of Bob’s gain in the second block, i.e., $H(2)P_{\text{max}} = 2$ dB. The loss can also be seen (although it is not shown here) to be increasing with the values of $\alpha^{(E)}$, since, as $\alpha^{(E)}$
decreases, the secrecy constraint becomes less stringent than reliability, and water-filling becomes more effective. This effect is explained by observing that water-filling allocates power to a block when its gain is sufficiently high to guarantee a benefit in terms of transmission rate without secrecy constraints. However, when a constraint is imposed on the secrecy outage probability, a further advantage for the main channel with respect to Eve’s channel is to be guaranteed in order to allocate power to a particular block. This mechanism is observed also in Fig. 6(b), in which the fraction of power allocated to the first block by the three methods is reported. The channel power gain for the second block is such that $H(2)P_{\text{max}} = 2$ dB. From Fig. 6(b), we see that, for allocating power to the first block, the optimal joint/rate power allocation method requires a significantly lower average received power than that required by the water-filling solution.

C. Secrecy rate: coding across sub-messages

In order to evaluate the secrecy rate of the CAS scheme, we first compare it with the corresponding secrecy rate achieved by CPS. Fig. 7 shows the contour lines of the secrecy rates obtained within the simplified two-blocks scenario considered in Section V-B. Secrecy rates are computed as in (8) for the three power allocation strategies considered in the previous subsection: a) equal power distribution among sub-messages, b) water-filling power distribution with respect to Bob’s channel, and c) optimal power allocation, as from (9). Perhaps surprisingly, and in
contrast with the results obtained for different block fading channel scenarios in the literature, we observe that CAS yields slightly higher secrecy rates than CPS. Moreover, CAS seems more robust against imperfect power allocation, as we note that the loss incurred by equal power allocation and water-filling with respect to the optimal solution of (9) is almost negligible for a wide range of channel gains (as it can be observed also from Fig. 8(a)). On the other hand, Fig. 8(b) shows that, opposite to what happens for CPS, when \( H(1) \) is small, the optimal power allocation for CAS provides the first block with a higher fraction of power compared to water-filling.

As a more practical example of the use of CAS, we have also considered the case of messages comprising \( K = 48 \) sub-messages. Since the computation of the optimal power allocation in this case is infeasible, we have considered a suboptimal approach, in which only a subset of \( K' \leq K \) sub-messages (those with the highest \( H_k \)) are selected and the available power is allocated uniformly among them. Thus, no power is allocated to a sub-message when its channel gain to Bob is smaller than a prefixed threshold; on the other hand, for all sub-messages for which the channel gain to Bob is larger than the threshold, the same power is used. By imposing the outage probability \( \varepsilon = 0.01 \), and considering \( P_{\text{max}} = 3.8 \) dB and \( \alpha^{(B)} = 1 \), Fig. 9(a) shows the maximum (over all values of \( K' \leq K \)) mean outage secrecy rate \( R_S = \frac{1}{K} \sum_k R_k \) as a function of \( \alpha^{(E)} \). As expected, from the figure we observe that, as \( \alpha^{(E)} \) increases, the secrecy
rate decreases. This behavior is confirmed in Fig. 9(b), that shows CDFs of the outage secrecy rates due to the statistics of Bob’s channel, for different values of $\alpha^{(E)}$.

VI. CONCLUSIONS

In this paper we have characterized the performance of secret transmissions over block fading channels, under the assumption of knowing the Alice-Bob channel and only a statistical description of the Alice-Eve channel. We have used a set of metrics that allow to study the problem both from the theoretical standpoint and by considering practical coded transmission schemes. We have derived bounds on the achievable outage secrecy rates (under the assumption of a capacity-achieving system), and studied the effect of power allocation on the secrecy performance. The definitions of security gap and equivocation rate have been extended to this scenario, and we have used them to assess the requirements for achieving security when practical codes are adopted.

APPENDIX A

SECURITY GAP FOR BOB’S CHANNEL KNOWN ONLY IN STATISTICAL TERMS

When Bob’s channel is fading and known only in statistical terms, we consider an outage approach also for Bob in order to define the security gap. In fact, $p^{(B)}(\gamma^{(B)})$ is a random
variable, whose distribution depends on the average SNR of Bob’s channel. The mean SNR of the channel between Alice and Bob is

\[ \bar{\gamma}^{(B)} = \frac{1}{K} \sum_k \alpha^{(B)} P_k. \]  

(47)

We are interested in finding the minimum value of \( \bar{\gamma}^{(B)} \), denoted as \( \bar{\gamma}^{(B)}_{\text{min}} \), for which the probability that \( p^{(B)} > \delta \) is not greater than \( \omega \), i.e.,

\[ \bar{\gamma}^{(B)}_{\text{min}} = \frac{1}{K} \sum_k P_k \cdot \min\{ \alpha^{(B)} : \mathbb{P}[p^{(B)}(\gamma^{(B)}) > \delta] \leq \omega \}. \]  

(48)

Then the \( \omega - \zeta \) security gap in this case is defined as

\[ S_g^{(\omega, \zeta)} = \frac{\bar{\gamma}^{(B)}_{\text{min}}}{\bar{\gamma}^{(E)}_{\text{max}}}, \]  

(49)

where \( \bar{\gamma}^{(E)}_{\text{max}} \) is given by (23). The value of \( \bar{\gamma}^{(B)}_{\text{min}} \) can be computed for the two cases of CAS and CPS.

**Computation of \( \bar{\gamma}^{(B)}_{\text{min}} \) for CAS:** Similarly to what has been done for Eve in Section IV-A, when CAS is considered, we are interested in finding a worst-case estimate of Bob’s error probability. As a closed form expression is not available, we resort to an upper bound, by defining \( \gamma_m = \min_k \{ \gamma_k^{(B)} \} \). Let \( p^{(B)}(\gamma^{(B)}) \) be the error probability achieved by Bob for a given channel realization \( \gamma^{(B)} \). We consider the upper bound

\[ p^{(B)}(\gamma^{(B)}) \leq p^{(B)}([\gamma_m, \gamma_m, \ldots, \gamma_m]); \]  

(50)

hence (48) becomes \( \bar{\gamma}^{(B)}_{\text{min}} = \frac{1}{K} \sum_k P_k \cdot \min\{ \alpha^{(B)} : \mathbb{P}[\gamma_m \leq \gamma] \leq \omega \}. \)

For the computation of \( \mathbb{P}[\gamma_m \leq \gamma] \), let us denote by \( L_k \) the event that \( \gamma_k^{(B)} \leq \gamma_\delta \). From the Rayleigh fading assumption we have \( \mathbb{P}[L_k] = 1 - \exp \left(-\frac{\gamma_\delta^2}{P \alpha^2} \right) \). Moreover, we have

\[ \mathbb{P}[\gamma_m \leq \gamma] = \mathbb{P} \left[ \bigcup_{k=1}^K L_k \right] = 1 - \prod_{k=1}^K (1 - \mathbb{P}[L_k]). \]  

(51)

Through this derivation, we can compute \( \bar{\gamma}^{(B)}_{\text{min}} \) for which condition (21a) is satisfied, from which \( S_g^{(\omega, \zeta)} \) is easily obtained, as in (49).
Computation of $\bar{\gamma}_{\min}^{(B)}$ for CPS: When CPS is considered, we must impose that the error probability for Bob is less than $\delta$ on each block, therefore Bob’s outage probability is

$$\mathbb{P}[p^{(B)}(\gamma^{(B)}) > \delta] = 1 - \prod_{k=1}^{K} \left(1 - \mathbb{P}[p^{(B)}(\gamma_k^{(B)}) > \delta]\right) = 1 - \prod_{k=1}^{K} (1 - \mathbb{P}[\mathcal{L}_k]). \quad (52)$$

So, also in this case, (51) can be used to model both the CPS and the CAS scenario, though in the former case it results from an exact derivation, while in the latter it is due to the use of the upper bound based on $\gamma_m$.

By using the derivation here described, we can compute $\bar{\gamma}_{\min}^{(B)}$ and $S_y^{(\omega,\zeta)}$ for the same cases already considered in Table I, where the results of this analysis are also reported. As expected, when Bob’s channel is fading and known only in statistical terms, the values of the security gap needed to ensure conditions (21) are significantly higher than those of the case in which Bob’s channel is known.

APPENDIX B

PROOF OF (6)

We can rewrite $p_s(P, R_1)$ as

$$p_s(P, R_1) = \mathbb{P}\left\{ \sum_{k=1}^{K} \log(1 + G_k P_k) \geq \sum_{k=1}^{K} \log(1 + H_k P_k) - KR_1 \right\}$$

$$= \mathbb{P}\left\{ \prod_{k=1}^{K} (1 + G_k P_k) \geq \Phi(P, R_1) \right\}. \quad (53)$$

Defining $\beta = \prod_{k=1}^{K} (1 + G_k P_k)$ we have

$$p_s(P, R_1) = 1 - \int_{1}^{\Phi(P, R_1)} p_\beta(a) da \quad (54)$$

with $p_\beta(a)$ the PDF of $\beta$, which has been computed in [26]. We recall the definition of the generalized Fox H-function [26]

$$\mathcal{H}_{p, q}^{m, n} \left[ r \left| \begin{array}{c} \{a_i, c_i, A_i\} \\ \{b_j, d_j, B_j\} \end{array} \right. \right] = \frac{1}{2\pi i} \oint_{\mathcal{C}} M_{p,q}^{m,n} \left[ s \left| \begin{array}{c} \{a_i, c_i, A_i\} \\ \{b_j, d_j, B_j\} \end{array} \right. \right] r^{-s} ds, \quad (55)$$

where $\mathcal{C}$ is a contour in the complex plane from $\omega - i\infty$ to $\omega + i\infty$ (where $i$ is the imaginary unit) such that $(b_i + k)/d_i$ and $(a_i - 1 - k)/c_i$ (with $k$ non-negative integer) lie to the right and
left of $C$, respectively, and

$$
M_{p,q}^{m,n} \left[ \begin{array}{c}
\{a_i, c_i, A_i\} \\
\{b_j, d_j, B_j\}
\end{array} \right] = \frac{\prod_{j=1}^{m} \hat{\Gamma}(b_j + d_j s, B_j) \prod_{i=1}^{n} \hat{\Gamma}(1 - a_i - c_i s, A_i)}{\prod_{j=m+1}^{p} \Gamma(a_i + c_i s, A_i) \prod_{i=n+1}^{q} \Gamma(1 - b_j - d_j s, B_j)}
$$

(56)

is the Mellin transform of the generalized Fox H-function, where $\hat{\Gamma}(\cdot, \cdot)$ is the upper incomplete Gamma function

$$
\hat{\Gamma}(s, a) = \int_{a}^{\infty} t^{s-1} e^{-t} dt,
$$

(57)

and an empty product is taken to be one. We have [26]

$$
p_{\beta}(a) = \frac{\zeta(P)}{\varphi(P)} H_{0,K}^{K,0} \left[ \frac{a}{\varphi(P)} \right] \{a, c \} \{0, 1, (P_k \alpha(E))^{-1}\} _{k=1,...,K},
$$

(58)

for $a \geq 1$ and $p_{\beta}(a) = 0$ otherwise. Now, by observing that

$$
\int_{1}^{q} t^{-s} dt = \frac{qq^{-s} - 1}{1 - s} = (qq^{-s} - 1) \frac{\hat{\Gamma}(1 - s, 0)}{\hat{\Gamma}(2 - s, 0)},
$$

(59)

and inserting the integral of (54) into (55) and using (59) together with (56) we obtain (6).

**APPENDIX C**

**PROOF OF THEOREM 1**

From (14) we have

$$
\frac{1 + H_k P_k}{P_k 2^{R_k}} - 1 = -\alpha^{(E)} \ln \bar{p}_k
$$

(60)

which can be rewritten as

$$
2^{R_k} = \frac{1 + H_k P_k}{\bar{u}_k P_k + 1}.
$$

(61)

From (61) we immediately the second result of the theorem (16).

By the KKT conditions, we have that maximizing that problem (3) subject to power constraint (2b) can be written as

$$
\max_{P, \nu} \sum_{k=1}^{K} \left\{ \log \frac{1 + H_k P_k}{\bar{u}_k P_k + 1} - \nu [P_k - P_{\max}] \right\}.
$$

(62)

Setting to zero the derivative with respect to $P_k$ we obtain

$$
\frac{\bar{u}_k P_k + 1}{1 + H_k P_k} \left[ \frac{H_k}{\bar{u}_k P_k + 1} - \frac{\bar{u}_k (1 + H_k P_k)}{(\bar{u}_k P_k + 1)^2} \right] - \nu = 0
$$

(63)

which can be rewritten as

$$
A_k P_k^2 + B_k P_k + C_k = 0.
$$

(64)

Now from (64) if $C_k < 0$ we obtain (15).
APPENDIX D
ON THE COMPUTATION OF $\gamma_{\eta}$

We assume that Eve uses ML decoding, which represents the most dangerous condition for the legitimate receiver. For assessing Eve’s error rate, we use Shannon’s SPB on the error probability of a coded transmission with ML decoding [27], which is still the tightest bound for high error rate values, at which Eve is supposed to operate.

By Shannon’s SPB on the block error probability under ML decoding, the error probability at Eve with SNR $\gamma$ is [28]:

$$p^{(E)}(\gamma) > P_{\text{SPB}}(N, \vartheta, A),$$

(65)

where $P_{\text{SPB}}(N, \vartheta, A)$ is the probability that the received vector falls outside the $N$-dimensional circular cone of half angle $\vartheta$ whose main axis passes through the origin and the signal point which represents the transmitted signal [28]. The quantity $A$ is defined as $A = \sqrt{2R_c\gamma}$, where $R_c$ is the code rate.

The tightest lower bound on the decoding error probability is achieved for $\vartheta_1(N, R_{en})$ satisfying

$$\frac{\Omega_N(\vartheta_1(N, R_{en}))}{\Omega_N(\pi)} = \exp(-NR_{en}),$$

(66)

where $R_{en}$ is the code rate in nats per channel use, $\Omega_N(\vartheta) = \frac{2\pi^{N/2}}{\Gamma(N/2)} \int_{0}^{\vartheta} (\sin \varphi)^{N-2} d\varphi$, $\Omega_N(\pi) = \frac{2\pi^{N/2}}{\Gamma(N/2)}$, and $\Gamma$ denotes the Gamma function.

The value of $P_{\text{SPB}}(N, \vartheta, A)$ in (65) can be obtained as [28]:

$$P_{\text{SPB}}(N, \vartheta, A) = \frac{(N-1) \exp \left(-\frac{NA^2}{2}\right)}{\sqrt{2\pi}} \cdot \int_{\vartheta}^{\pi} (\sin \varphi)^{N-2} f_N \left(\sqrt{NA} \cos \varphi\right) d\varphi + Q \left(\sqrt{NA}\right),$$

(67)

where $f_N(x) = \sum_{j=0}^{N-1} \exp \left(d(N, j, x)\right)$ and the function $d(N, j, x)$ is defined as

$$d(N, j, x) = \frac{x^2}{2} + \ln \Gamma \left(\frac{N}{2}\right) - \ln \Gamma \left(\frac{j}{2} + 1\right) - \ln \Gamma (N - j) + (N - 1 - j) \ln \left(\sqrt{2x}\right) - \frac{\ln 2}{2} +$$

$$+ \ln \left[1 + (-1)^j \tilde{\Gamma} \left(\frac{x^2}{2}, \frac{j + 1}{2}\right)\right],$$

(68)

in which $\tilde{\Gamma}(\cdot, \cdot)$ denotes the lower incomplete Gamma function

$$\tilde{\Gamma}(x, a) = \frac{1}{\Gamma(a)} \int_{0}^{x} t^{a-1} e^{-t} dt.$$

(69)
This way of computing Shannon’s SPB corresponds to the logarithmic domain approach proposed in [28], which avoids the numerical over- and under-flows affecting the calculation of the bound for large block lengths. Concerning the logarithmic domain version of the function \( f_N(x) \), an alternative, recursive implementation is also presented in [28].

By solving \( P_{\text{SPB}}(N, \vartheta, A) = 1 - \eta \) with respect to \( \gamma \) we can compute \( \gamma_{\eta} \) such that an error probability \( 1 - \eta \) is achieved.

REFERENCES

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

[2] T. Liu, V. Prabhakaran, and S. Vishwanath, “The secrecy capacity of a class of parallel gaussian compound wiretap channels,” in *IEEE International Symposium on Information Theory (ISIT 2008)*, Toronto, Canada, Jul. 2008, pp. 116–120.

[3] X. Tang, R. Liu, and P. Spasojevic, “On the achievable secrecy throughput of block fading channels with no channel state information at transmitter,” in *41st Annual Conference on Information Sciences and Systems, (CISS 2007)*, Baltimore, MD, Mar. 2007, pp. 917–922.

[4] F. Renna, N. Laurenti, and H. V. Poor, “Physical-layer secrecy for OFDM transmissions over fading channels,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1354 –1367, Aug. 2012.

[5] ———, “High SNR secrecy rates with OFDM signaling over fading channels,” in *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, Istanbul, Turkey, Sep. 2010, pp. 2692–2697.

[6] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, “On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels,” *ArXiv*, Feb. 2012. [Online]. Available: http://arxiv.org/abs/1202.5830

[7] S.-C. Lin and P.-H. Lin, “On ergodic secrecy capacity of multiple input wiretap channel with statistical CSIT,” *ArXiv*, Jan. 2012. [Online]. Available: http://arxiv.org/abs/1201.2868

[8] D. Kline, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, “LDPC codes for physical layer security,” in *Proc. IEEE Global Telecommunications Conference (GLOBECOM 2009)*, Honolulu, HI, Nov. 2009, pp. 1–6.

[9] ———, “LDPC codes for the gaussian wiretap channel,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, Sep. 2011.

[10] M. Baldi, M. Bianchi, and F. Chiariulce, “Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.

[11] W. K. Harrison, J. Almeida, S. McLaughlin, and J. Barros, “Coding for cryptographic security enhancement using stopping sets,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 575–584, Sep. 2011.

[12] M. Baldi, M. Bianchi, and F. Chiariulce, “Non-systematic codes for physical layer security,” in *Proc. IEEE Information Theory Workshop (ITW 2010)*, Dublin, Ireland, Aug. 2010.

[13] ———, “Increasing physical layer security through scrambled codes and ARQ,” in *Proc. IEEE International Conference on Communications (ICC 2011)*, Kyoto, Japan, Jun. 2011.

[14] M. Baldi, M. Bianchi, N. Maturo, and F. Chiariulce, “A physical layer secured key distribution technique for IEEE 802.11g wireless networks,” *IEEE Wireless Commun. Lett.*, 2013, in press. [Online]. Available: http://arxiv.org/abs/1212.4991.
[15] K. Bhattad and K. R. Narayanan, “Weakly secure network coding,” in Proc. NetCod 2005, Riva del Garda, Italy, Apr. 2005.
[16] R. L. Rivest, “All-or-nothing encryption and the package transform,” in Fast Software Encryption, ser. Lecture Notes in Computer Science. Springer, 1997, vol. 1267, pp. 210–218.
[17] C. W. Wong, T. Wong, and J. Shea, “Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 551–564, Sep. 2011.
[18] M. R. D. Rodrigues, A. Somekh-Baruch, and M. Bloch, “On Gaussian wiretap channels with M-PAM inputs,” in European Wireless Conference, Lucca, Italy, Apr. 2010, pp. 1–8.
[19] G. D. Raghava and B. S. Rajan. (2010) Secrecy capacity of the Gaussian wire-tap channel with finite complex constellation input. [Online]. Available: http://arxiv.org/abs/1010.1163
[20] A. Valenbois and M. P. C. Fossorier, “Sphere-packing bounds revisited for moderate block lengths,” IEEE Trans. Inform. Theory, vol. 50, no. 12, pp. 2998–3014, Dec. 2004.
[21] J. Jiang and K. R. Narayanan, “Iterative soft-input soft-output decoding of Reed-Solomon codes by adapting the parity-check matrix,” IEEE Trans. Inform. Theory, vol. 52, no. 8, pp. 3746–3756, Aug. 2006.
[22] S. B. Wicker, Error Control Systems for Digital Communication and Storage. Upper Saddle River, NJ: Prentice Hal, Inc, 1995.
[23] X. Y. Hu and E. Eleftheriou, “Progressive edge-growth Tanner graphs,” in Proc. IEEE Global Telecommunications Conference (GLOBECOM’01), San Antonio, Texas, Nov. 2001, pp. 995–1001.
[24] J. Hagenauer, E. Offer, and L. Papke, “Iterative decoding of binary block and convolutional codes,” IEEE Trans. Inform. Theory, vol. 42, no. 2, pp. 429–445, Mar. 1996.
[25] T. Cover and J. Thomas, Elements of Information Theory, 2nd ed. New York, NY, USA: Wiley-Interscience, 2006.
[26] F. Yilmaz and M.-S. Alouini, “Product of shifted exponential variates and outage capacity of multicarrier systems,” in European Wireless Conference, Aalborg, Denmark, May 2009.
[27] C. E. Shannon, “Probability of error for optimal codes in a Gaussian channel,” Bell Syst. Tech. J., vol. 38, no. 3, pp. 611–656, May 1959.
[28] G. Wiechman and I. Sason, “An improved sphere-packing bound for finite-length codes over symmetric memoryless channels,” IEEE Trans. Inform. Theory, vol. 54, no. 5, pp. 1962–1990, May 2008.