Wireless Information-Theoretic Security

Matthieu Bloch, *Student Member, IEEE*, João Barros, *Member, IEEE*, Miguel R. D. Rodrigues, *Member, IEEE*, and Steven W. McLaughlin, *Fellow, IEEE*

***Abstract*—This paper considers the transmission of confidential data over wireless channels. Based on an information-theoretic formulation of the problem, in which two legitimates partners communicate over a quasi-static fading channel and an eavesdropper observes their transmissions through a second independent quasi-static fading channel, the important role of fading is characterized in terms of average secure communication rates and outage probability. Based on the insights from this analysis, a practical secure communication protocol is developed, which uses a four-step procedure to ensure wireless information-theoretic security: (i) common randomness via opportunistic transmission, (ii) message reconciliation, (iii) common key generation via privacy amplification, and (iv) message protection with a secret key. A reconciliation procedure based on multilevel coding and optimized low-density parity-check (LDPC) codes is introduced, which allows to achieve communication rates close to the fundamental security limits in several relevant instances. Finally, a set of metrics for assessing average secure key generation rates is established, and it is shown that the protocol is effective in secure key renewal—even in the presence of imperfect channel state information.**

***Index Terms*—Information-theoretic security, low-density parity-check (LDPC) codes, secrecy capacity, secret key agreement, wireless channels.**

I. Introduction

A. Motivation

THE issues of privacy and security in wireless communication networks have taken on an increasingly important role as these networks continue to flourish worldwide. Traditionally, security is viewed as an independent feature addressed above the physical layer, and all widely used cryptographic protocols (e.g., RSA and AES) are designed and implemented assuming the physical layer has already been established and provides an error-free link. In contrast with this paradigm, there exist both theoretical and practical contributions that support the potential of physical layer security ideas to significantly strengthen the security of digital communication systems. The basic principle of *information-theoretic* security—widely accepted as the strictest notion of security—calls for the combination of cryptographic schemes with channel coding techniques that exploit the randomness of communication channels to guarantee that the messages sent cannot be decoded by a third party maliciously eavesdropping on the wireless medium (see Fig. 1).

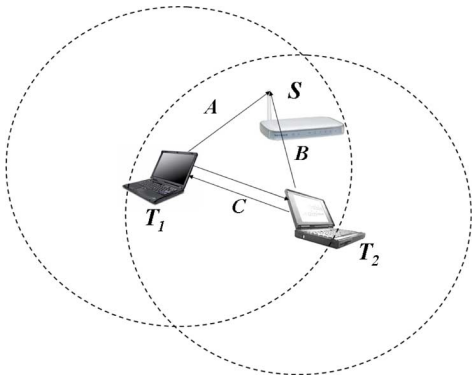

Fig. 1. Example of a wireless network with potential eavesdropping. Terminals T_1 and T_2 communicate with a base station S over a wireless medium (channels A and B). By listening to the transmissions of terminal T_1 (through channel C), terminal T_2 may acquire confidential information. If T_1 wants to exchange a secret key or guarantee the confidentiality of its transmitted data, it can exploit the *physical* properties of the wireless channel to secure the information by *coding* against terminal T_2.

The theoretical basis for this information-theoretic approach, which builds on Shannon's notion of *perfect* secrecy [1], was laid by Wyner [2] and later by Csiszár and Körner [3], who proved in seminal papers that there exist channel codes guaranteeing both robustness to transmission errors and a prescribed degree of data confidentiality. In the 1970s and 1980s, the impact of these works was limited, partly because practical wiretap codes were not available, but mostly because a strictly positive secrecy capacity in the classical wiretap channel setup requires the legitimate sender and receiver to have some advantage over the attacker in terms of channel quality. Moreover, almost at the same time, Diffie and Hellman [4] published the basic principles of public-key cryptography, which was to be adopted by nearly all contemporary security schemes.

More recently, there has been a renewed interest for information-theoretic security, arguably due to the work of Maurer [5], who proved that even when the legitimate users (say Alice and Bob) have a worse channel than the eavesdropper (say Eve), it is possible for them to generate a secret key through public communication over an insecure yet authenticated channel. The advent of wireless communications, which are particularly susceptible to eavesdropping because of the broadcast nature of the transmission medium, has also motivated a closer analysis of the secrecy potential of wireless networks. Hero [6] introduced space–time signal processing techniques for secure communication over wireless links, and Goel and Negi [7], [8] investigated achievable secret communication rates taking advantage

Manuscript received November 22, 2006; revised January 8, 2008. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Seattle, WA, July 2006, at the 44th Annual Allerton Conference on Communication Control and Computing, Monticello, IL, 2006, and at the IEEE Information Theory Workshop, Chengdu, China, October 2006.

M. Bloch and S. W. McLaughlin are with the GT-CNRS UMI 2958, Metz, France, and also with the School of electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332-0250 USA (e-mail: matthieu@gatech.edu; swm@ece.gatech.edu).

J. Barros and M. Rodrigues are with the Instituto de Telecomunicações and the Department of Computer Science, Faculdade de Ciências da Universidade do Porto, 4169-007 Porto, Portugal (e-mail: barros@dcc.fc.up.pt; mrodrigues@dcc.fc.up.pt).

Communicated by U. Maurer, Guest Editor for Special Issue on Information Theoretic Security.

Color versions of Figures 2–6 and 8–13 in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2008.921908

of multiple-input multiple-output communications. Parada and Blahut [9] established the secrecy capacity of various degraded fading channels. Barros and Rodrigues [10] provided a detailed characterization of the outage secrecy capacity of slow fading channels, and they showed that fading alone guarantees that information-theoretic security is achievable, even when the eavesdropper has a better average signal-to-noise ratio (SNR) than the legitimate receiver—without the need for public communication over a feedback channel or the introduction of artificial noise. The ergodic secrecy capacity of fading channels was derived independently by Liang *et al.* [11], Li *et al.* [12], and Gopala *et al.* in [13] and power and rate allocation schemes for secret communication over fading channels were presented.

In spite of the numerous theoretical contributions, the general problem of physical-layer coding and modulation schemes for both reliable and secure communication over Gaussian and fading wiretap channels has not received much attention. There is still no general framework to draw on, even as we witness sustained advances in the area of capacity-achieving coding and modulation for Gaussian and fading channels [14], [15]. Much of previous work for the wiretap channel stems from the early work in [2] and [16] and is studied more extensively by Wei [17], who shows how to encode secret information using cosets of certain linear block codes. More recently, this general notion has been extended by Thangaraj *et al.* [18], and later by Liu *et al.* [19], where it was shown how low-density parity-check (LDPC) codes can achieve the secrecy capacity of the erasure wiretap channel asymptotically, and how this class of codes can be used to provide perfectly secret communications at rates below the secrecy capacity for other channels. Thangaraj *et al.* [18] also showed how the joint problems of reliability and security interact in a code and how capacity approaching codes for the reliability problem can be used to meet the reliability and security requirements of the wiretap channel. Several authors recently proved the existence of coding schemes for various generalized wiretap channel scenarios [20], [21]. In particular, the possibility of coding methods based on LDPC codes was shown in [22].

Since designing wiretap codes for Gaussian and fading channels appears to be beyond the capabilities of current coding techniques, we focus on the somewhat less difficult problem of generating secret keys for secure communication over Gaussian and wireless channels. The key generation/distribution problem in wiretap channels falls under the general problem of key generation from correlated source outputs, which has been extensively studied in an information-theoretic context [5], [23], [24]. The objective of secure key distribution is for Alice and Bob to agree on a common k-bit key about which Eve's entropy is maximal. In key distribution, the k bits can be unknown to Alice before transmission, which is in sharp contrast to secure message communication where Alice has a k-bit message that she wants to communicate to Bob. Powerful tools, such as common randomness, advantage distillation, and privacy amplification, were developed in the context of secret key agreement over wiretap channels [23], [25] and will be discussed, as they form the basis for much of the practical secret key agreement protocol proposed in this paper. Most key agreement protocols require some level of interactive communication between Alice and Bob to arrive at a common yet secret key [5], where the exchange of information is by way of a parallel, error-free public channel between Alice and Bob used during the key agreement phase [26]. One key advance in this paper is that we focus exclusively on protocols that require only one-way feedforward communication from Alice to Bob across the noisy wireless channel, thus obviating the need for a noiseless, authenticated public channel.

B. Main Contributions and Organization of the Paper

In the following, we summarize the main contributions of this work.

- *Role of fading;* we analyze the impact of quasi-static fading on wireless channels in terms of information-theoretically secure communication rates, and we highlight the benefit of fading towards achieving nonzero secure communication rates.
- *Opportunistic secret key agreement;* based on the insight provided by the aforementioned analysis, we propose an *opportunistic* secret key agreement protocol, which exploits the fluctuations of the fading coefficients to generate information theoretically secure keys.
- *Coding algorithm;* we present a practical algorithm for the secret key agreement protocol based on multilevel coding and LDPC codes.
- *Performance evaluation;* we introduce a set of reasonable metrics to assess the performance of the protocol, and we analyze the secure communication rates achievable by the protocol in asymptotic regimes.
- *Impact of channel state information;* we extend the secret key agreement protocol to allow for imperfect channel state information (CSI), and we show its effectiveness in secure key renewal.

The rest of this paper is organized as follows. In Section II, we study the impact of fading on the secure communication rates that are achievable over quasi-static wireless channels, thus shedding light on how to design opportunistic secret key agreement protocols. Section III describes one such opportunistic secret key agreement protocol in detail and presents a reconciliation procedure based on multilevel coding and LDPC codes. In Section IV, we analyze the performance of the protocol, both analytically in asymptotic regimes and through simulation, and we discuss the impact of imperfect CSI. Concluding remarks are provided in Section V.

II. Information-Theoretic Security Over Wireless Channels

A. Wireless System Setup

We consider the wireless system setup depicted in Fig. 2, where a legitimate user (Alice) wants to send messages to another user (Bob). Alice encodes a message block, represented by the random variable (RV) W^k, into a codeword, represented by the RV X^n, for transmission over the channel. Bob observes the output of a discrete-time Rayleigh-fading channel (the *main* channel) given by

$$Y_m(i) = H_m(i)X(i) + Z_m(i)$$

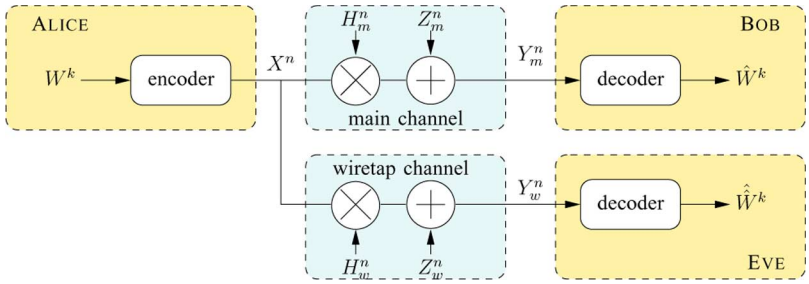

Fig. 2. Wireless wiretap channel setup.

where $H_m(i)$ is a circularly symmetric complex Gaussian RV with zero-mean and unit-variance representing the main channel fading coefficient and $Z_m(i)$ is a zero-mean circularly symmetric complex Gaussian noise RV.

A third party (Eve) is also capable of eavesdropping on Alice's transmissions. Eve observes the output of an independent discrete-time Rayleigh-fading channel (the *eavesdropper*'s channel) given by

$$Y_w(i) = H_w(i)X(i) + Z_w(i)$$

where $H_w(i)$ denotes a circularly symmetric complex Gaussian RV with zero-mean and unit-variance representing the eavesdropper's channel fading coefficient and $Z_w(i)$ denotes a zero-mean circularly symmetric complex Gaussian noise RV.

It is assumed that the channel input, the channel fading coefficients, and the channel noises are all independent. It is also assumed that both the main channel and the eavesdropper's channel are quasi-static fading channels, that is, the fading coefficients, albeit random, are constant during the transmission of an entire codeword ($\forall\ i = 1, \ldots, n\ H_m(i) = H_m$ and $H_w(i) = H_w$) and, moreover, independent from codeword to codeword. This corresponds to a situation where the coherence time of the channel is large.

The codewords transmitted by Alice are subject to the average power constraint

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\{|X(i)|^2\} \leq P$$

and the average noise powers in the main channel and the eavesdropper's channel are denoted by N_m and N_w, respectively. Consequently, the instantaneous SNR at Bob's receiver is given by

$$\Gamma_m(i) = P|H_m(i)|^2/N_m = P|H_m|^2/N_m = \Gamma_m$$

and its average value corresponds to

$$\overline{\gamma}_m(i) = P\mathbb{E}\{|H_m(i)|^2\}/N_m = P\mathbb{E}\{|H_m|^2\}/N_m = \overline{\gamma}_m.$$

Likewise, the instantaneous SNR at Eve's receiver is given by

$$\Gamma_w(i) = P|H_w(i)|^2/N_w = P|H_w|^2/N_w = \Gamma_w$$

and its average value can be written as

$$\overline{\gamma}_w(i) = P\mathbb{E}\{|H_w(i)|^2\}/N_w = P\mathbb{E}\{|H_w^2\}/N_w = \overline{\gamma}_w.$$

Since the channel fading coefficients H are zero-mean complex Gaussian RVs and the instantaneous SNR $\Gamma \propto |H|^2$, it follows that Γ is exponentially distributed, specifically

$$p(\gamma_m) = \frac{1}{\overline{\gamma}_m}\exp\left(-\frac{\gamma_m}{\overline{\gamma}_m}\right), \qquad \gamma_m > 0 \tag{1}$$

and

$$p(\gamma_w) = \frac{1}{\overline{\gamma}_w}\exp\left(-\frac{\gamma_w}{\overline{\gamma}_w}\right), \qquad \gamma_w > 0. \tag{2}$$

Let the transmission rate between Alice and Bob be $R = H(W^k)/n$, the equivocation rate of Eve be $R_e = H\left(W^k|Y_w^n\right)/n$, and the error probability $\mathcal{P}_\epsilon = \mathcal{P}(W^k \neq \hat{W}^k)$, where W^k denotes the sent messages and $\hat{W}^k$ denotes Bob's estimate of the sent messages. Notice that the secrecy condition used here (and in [2], [3]) is weaker than the one proposed by Maurer and Wolf in [27] or Narayan and Csiszár in [28], where the information obtained by the eavesdropper is negligibly small not just in terms of rate but in absolute terms. Maurer and Wolf showed that the notions could be used interchangeably for discrete memoryless channels, and this result was very recently extended to the Gaussian case [29].

In general, one is interested in characterizing the rate-equivocation region, defined as the set of pairs (R', R'_e) such that for all $\epsilon > 0$ there exists an encoder–decoder pair satisfying $R \geq R' - \epsilon$, $R_e \geq R'_e - \epsilon$, and $\mathcal{P}_\epsilon \leq \epsilon$. Here, however, we focus on the secrecy capacity C_s of the channel, which corresponds to the maximum transmission rate R such that $R_e = R$.

B. Impact of Fading on Secure Communications

In this subsection, we study the impact of fading on the secrecy capacity of this wireless system by considering two metrics: average secrecy capacity and probability of outage of secrecy capacity. We assume that Alice and Bob have perfect knowledge of the main channel fading coefficient and that Eve also has perfect knowledge of the eavesdropper's channel fading coefficient. These assumptions are realistic for the slow-fading wireless environment under consideration: both receivers can always obtain close to perfect channel estimates and, additionally, the legitimate receiver can also feed back the channel estimates to the legitimate transmitter. Moreover, we assume that Alice and Bob also have partial knowledge of the eavesdropper's channel fading coefficient. This corresponds, for instance, to the situation where Eve is another active user in the wireless network (e.g., in a time-division multiple-access

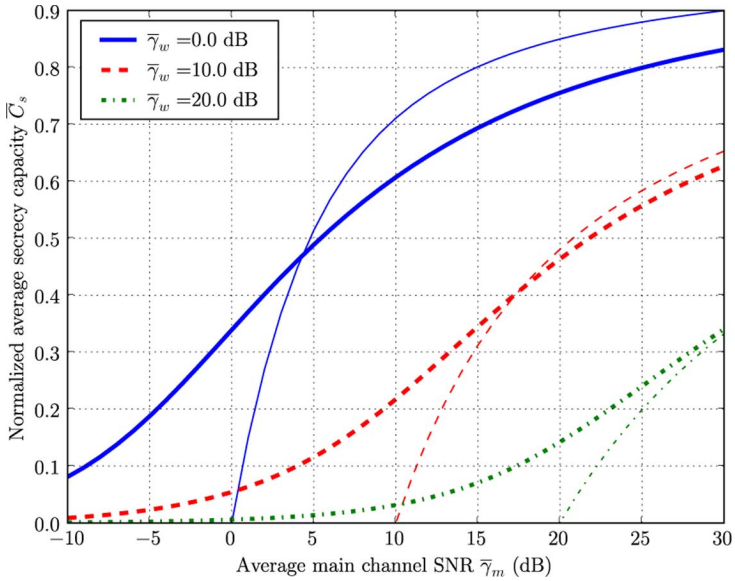

Fig. 3. Normalized average secrecy capacity versus $\overline{\gamma}_m$, for selected values of $\overline{\gamma}_w$. Thinner lines correspond to the normalized average secrecy rate capacity of a Rayleigh-fading channel while thicker lines correspond to the secrecy capacity of a Gaussian wiretap channel. Normalization is performed with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_m$.

(TDMA) environment), so that Alice can estimate the eavesdropper's channel during Eve's transmissions.

Nevertheless, we shall see that the probability of outage of secrecy capacity allows, in principle, to consider also situations where no CSI about the eavesdropper's channel is available to Alice and Bob. This case corresponds to the situation where Eve is a purely passive and malicious eavesdropper in the wireless network.

We start by deriving the secrecy capacity for one realization of a pair of quasi-static fading channels with complex noise and complex fading coefficients. For this purpose, we recall the results of [30] for the real-valued Gaussian wiretap channel, where it is assumed that Alice and Bob communicate over a standard real additive white Gaussian noise (AWGN) channel with noise power N_m and Eve's observation is also corrupted by Gaussian noise with power $N_w > N_m$, i.e., Eve's receiver has a lower SNR than Bob's receiver. The input power is constrained according to $\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\{X(i)^2\} \leq P$. For this instance, the secrecy capacity is given by

$$C_s = C_m - C_w \tag{3}$$

where

$$C_m = \frac{1}{2}\log\left(1+\frac{P}{N_m}\right) \quad \text{and} \quad C_w = \frac{1}{2}\log\left(1+\frac{P}{N_w}\right)$$

denote the capacity of the main channel and of the eavesdropper's channel, respectively. From this result, we can derive the instantaneous secrecy capacity for the wireless fading scenario defined in Section II-A.

Lemma 1: The secrecy capacity for one realization (γ_m, γ_w) of the quasi-static complex fading wiretap-channel is given by

$$C_s(\gamma_m,\gamma_w) = \begin{cases} \log(1+\gamma_m) - \log(1+\gamma_w), & \text{if } \gamma_m > \gamma_w \\ 0, & \text{if } \gamma_m \leq \gamma_w. \end{cases} \tag{4}$$

Proof: See Appendix A. □

1) Average Secrecy Capacity: If perfect CSI of the eavesdropper's channel is available to Alice, the coding scheme can be adapted to every realization of the fading coefficients. Therefore, in principle, any average secure communication rate below the average secrecy capacity of the channel

$$\overline{C}_s = \int_0^\infty \int_0^\infty C_s(\gamma_m,\gamma_w)\, p(\gamma_m)p(\gamma_w)d\gamma_m d\gamma_w$$

is achievable.

Remark 1: The average secrecy capacity is easily computable numerically. It can be shown (see the proof of Lemma 2 in Appendix C) that

$$\overline{C}_s = F(\overline{\gamma}_m) - F\left(\frac{\overline{\gamma}_m\overline{\gamma}_w}{\overline{\gamma}_w+\overline{\gamma}_m}\right) \tag{5}$$

where

$$F(x) = \int_0^\infty \log_2(1+u)\frac{1}{x}e^{-\frac{u}{x}}du = e^{\frac{1}{x}}\mathrm{E}_1(x^{-1})\frac{1}{\log 2} \tag{6}$$

and E_1 is the exponential-integral function.

Fig. 3 compares the average secrecy capacity of a quasi-static fading channel to the secrecy capacity of a classic wiretap Gaussian channel. Strikingly, one observes that the average secrecy rate of the fading channel is indeed higher than or close to the secrecy capacity of the Gaussian channel. One also observes that, in contrast to the situation of the Gaussian channel, the average secrecy rate of the fading channel is nonzero even when the average SNR of the main channel is lower than the average SNR of the eavesdropper's channel. These observations underline once again the potential of fading channels to secure the transmission of information between two legitimate parties against a possible eavesdropper.

2) Outage Probability of Secrecy Capacity: The secrecy capacity of a quasi-static Rayleigh-fading channel can also be characterized in terms of outage probability.

Proposition 1:

$$\mathrm{P}\left[C_s > \tau\right] = P_0(\tau) = \frac{\bar{\gamma}_m}{\bar{\gamma}_m + \bar{\gamma}_w 2^{\tau}} \exp\left(-\frac{2^{\tau}-1}{\bar{\gamma}_m}\right).$$

Proof:

$$\begin{aligned}\mathrm{P}\left[C_s > \tau\right] &= \mathrm{P}\left[\log\frac{1+\Gamma_m}{1+\Gamma_w} > \tau\right] \\ &= \mathrm{P}\left[\Gamma_m > 2^{\tau}(1+\Gamma_w) - 1\right], \\ &= \int_0^{\infty} p(\gamma_w)\left(\int_{2^{\tau}(1+\gamma_w)-1}^{\infty} p(\gamma_m)d\gamma_m\right)d\gamma_w\end{aligned}$$

where the last equality exploits the fact that $p(\gamma_m, \gamma_w) = p(\gamma_m)p(\gamma_w)$. The expressions of $p(\gamma_m)$ and $p(\gamma_w)$ are given by (2), and the result follows from simple algebra. □

Based on this result, it becomes immediately clear that for average SNRs $\overline{\gamma}_m$ and $\overline{\gamma}_w$ on the main channel and the eavesdropper's channel, respectively, the probability of strictly positive secrecy capacity is

$$\mathrm{P}\left[C_s > 0\right] = \frac{\overline{\gamma}_m}{\overline{\gamma}_m + \overline{\gamma}_w}. \tag{7}$$

It is also useful to express this probability in terms of parameters related to user location. Using the fact that $\overline{\gamma}_m \propto 1/d_m^{\alpha}$ and $\overline{\gamma}_w \propto 1/d_w^{\alpha}$ [31], we have that for distance d_m between Alice and Bob, distance d_w between Alice and Eve, and path-loss exponent α, the probability of strictly positive secrecy capacity is

$$P\left[C_s > 0\right] = \frac{1}{1 + (d_m/d_w)^{\alpha}}. \tag{8}$$

Remark 2: When $\gamma_m \gg \gamma_w$ (or $d_m \ll d_w$) then $P\left[C_s > 0\right] \approx 1$ (or $P\left[C_s = 0\right] \approx 0$). Conversely, when $\gamma_w \gg \gamma_m$ (or $d_w \ll d_m$) then $P\left[C_s > 0\right] \approx 0$ (or $P\left[C_s = 0\right] \approx 1$). This confirms the intuition that greater security is achieved when Eve is further away from Alice than Bob. It is also interesting to observe that to guarantee the existence of a nonzero secrecy capacity with probability greater than p_0 then it follows from (7) and (8) that

$$\frac{\overline{\gamma}_m}{\overline{\gamma}_w} > \frac{p_0}{1-p_0} \text{ or } \frac{d_m}{d_w} < \sqrt[\alpha]{\frac{1-p_0}{p_0}}.$$

In particular, a nonzero secrecy capacity exists even when $\overline{\gamma}_m < \overline{\gamma}_w$ or $d_m > d_w$, albeit with probability less than $1/2$.

We are now ready to characterize the outage probability

$$\mathcal{P}_{\mathrm{out}}(R_s) = P\left[C_s < R_s\right]$$

i.e., the probability that the instantaneous secrecy capacity is less than a target secrecy rate $R_s > 0$. The operational significance of this definition of outage probability is twofold. First, it provides the fraction of fading realizations for which the wireless channel can support a secure rate of R_s bits/channel use. Second, it provides a security metric for the situation where Alice and Bob have no CSI about the eavesdropper. In this case, Alice has no choice but to set her secrecy rate to a constant R_s. By doing so, Alice is assuming that the capacity of the wiretap channel is given by $C'_w = C_m - R_s$. As long as $R_s < C_s$, Eve's channel is worse than Alice's estimate, i.e., $C_w < C'_w$, and the wiretap codes used by Alice ensure perfect secrecy. Otherwise, if $R_s > C_s$ then $C_w > C'_w$ and information-theoretic security is compromised.

Proposition 2: From Proposition 1, the outage probability for a target secrecy rate R_s is given by

$$\begin{aligned}\mathcal{P}_{\mathrm{out}}(R_s) &= \mathrm{P}\left[C_s \le R_s\right] \\ &= 1 - \frac{\overline{\gamma}_m}{\overline{\gamma}_m + 2^{R_s}\overline{\gamma}_w} \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_m}\right).\end{aligned} \tag{9}$$

It is illustrative to examine the asymptotic behavior of the outage probability for extreme values of the target secrecy rate R_s. From (9) it follows that when $R_s \to 0$

$$\mathcal{P}_{\mathrm{out}} \to \frac{\overline{\gamma}_w}{\overline{\gamma}_m + \overline{\gamma}_w}$$

and when $R_s \to \infty$, we have that $\mathcal{P}_{\mathrm{out}} \to 1$, such that it becomes impossible for Alice and Bob to transmit secret information (at very high rates).

Also of interest is the asymptotic behavior of the outage probability for extreme values of the average SNRs of the main channel and the eavesdropper's channel. When $\overline{\gamma}_m \gg \overline{\gamma}_w$, (9) yields

$$\mathcal{P}_{\mathrm{out}}(R_s) \approx 1 - \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_m}\right)$$

and in a high-SNR regime $\mathcal{P}_{\mathrm{out}} \approx (2^{R_s}-1)/\overline{\gamma}_m$, i.e., the outage probability decays as $1/\overline{\gamma}_m$. Conversely, when $\overline{\gamma}_w \gg \overline{\gamma}_m$

$$\mathcal{P}_{\mathrm{out}}(R_s) \approx 1$$

and confidential communication becomes impossible.

Fig. 4 depicts the outage probability versus $\overline{\gamma}_m$, for selected values of $\overline{\gamma}_w$ and for a normalized target secrecy rate equal to 0.1. Observe that the higher $\overline{\gamma}_m$ the lower the outage probability, and the higher $\overline{\gamma}_w$ the higher the probability of an outage. Moreover, if $\overline{\gamma}_m \gg \overline{\gamma}_w$, the outage probability decays as $1/\overline{\gamma}_m$. Conversely, if $\overline{\gamma}_w \gg \overline{\gamma}_m$ the outage probability approaches one. The relationship between outage and distance is highlighted in Fig. 5.

The outage probability is also convenient to analyze the situation where Alice might only have imperfect estimates $\hat{H}_m$ and $\hat{H}_w$ of the gains of the main and eavesdropper's channels, respectively. We can reasonably assume that Bob cooperates with Alice, which allows her to obtain a perfect estimate of the main channel fading coefficient. Hence, $\hat{H}_m = H_m$, where H_m is the true fading coefficient of the main channel. Unfortunately, Eve may not be as helpful and Alice's knowledge of the eavesdropper's channel fading is more likely to be noisy. In order to assess the performance of our protocol under more realistic conditions, we model Alice's estimate of Eve's fading coefficient by

$$\hat{H}_w = H_w + Z'_w$$

where H_w is the true fading coefficient and Z'_w is a zero-mean complex Gaussian noise with known variance σ_e^2 per dimension.

In the absence of additional information allowing Alice to refine her estimation, we have to resort once again to outage

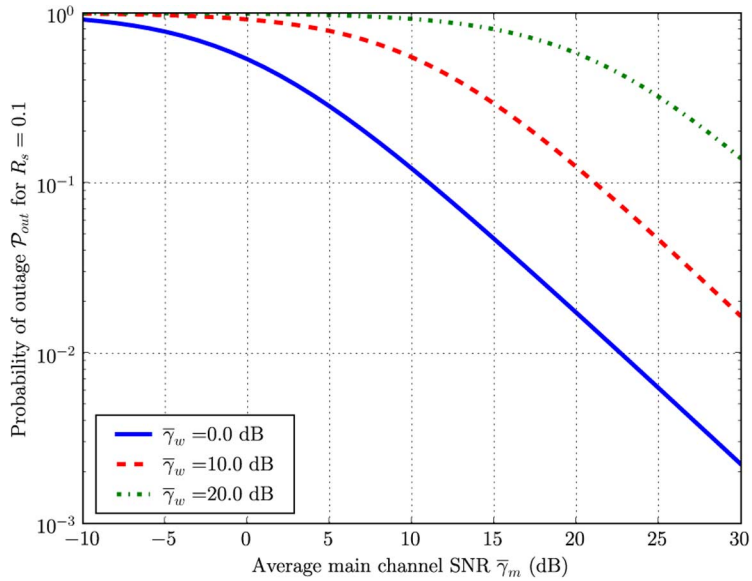

Fig. 4. Outage probability versus $\overline{\gamma}_m$, for selected values of $\overline{\gamma}_w$ and for a normalized target secrecy rate $R_s = 0.1$. Normalization is performed with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_m$.

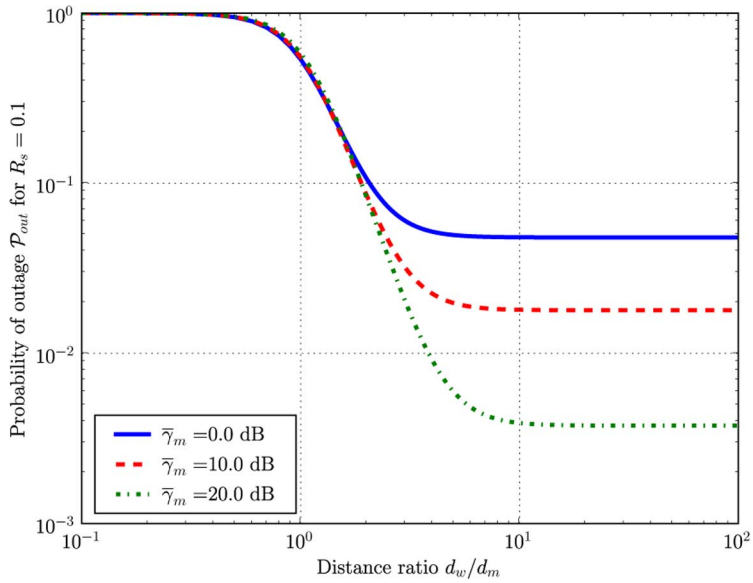

Fig. 5. Outage probability versus d_w/d_m for selected values of $\overline{\gamma}_m$ and for a normalized target secrecy rate $R_s = 0.1$. The path-loss exponent is $\alpha = 0.4$ and normalization is performed with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_m$.

analysis. If Alice communicates by blindly assuming that her estimation is accurate, an outage occurs whenever Alice underestimates the gain of the eavesdropper's channel and attempts to achieve a secure communication rate not supported by the channel.

Proposition 3: The probability of outage is upper-bounded by

$$\mathcal{P}_{\text{out}} \leq \frac{1}{2} - \frac{1}{2}\frac{1}{\sqrt{1+2/\sigma_e^2}}. \tag{10}$$

Proof: See Appendix B. □

This upper bound on the outage probability is a decreasing function of the variance of the channel estimation error σ_e^2, so that the higher σ_e^2 the lower the outage probability. This counterintuitive result stems from the fact that, at moderate values of the variance of the channel estimation error, Alice tends to consistently underestimate the true wiretap fading coefficient. Consequently, she consistently attempts to communicate at secure rates lower than what the true instantaneous secrecy capacity of the channel would allow.

C. Opportunistic Secret Key Agreement

In principle, secure communications over wireless quasi-static fading channels can be achieved with codes designed for the Gaussian wiretap channel; however, although the secrecy capacity of the Gaussian wiretap channel has been fully characterized [30], the design of *practical* coding schemes is still an open problem. In contrast, previous results on secret key agreement by public discussion [5] and privacy

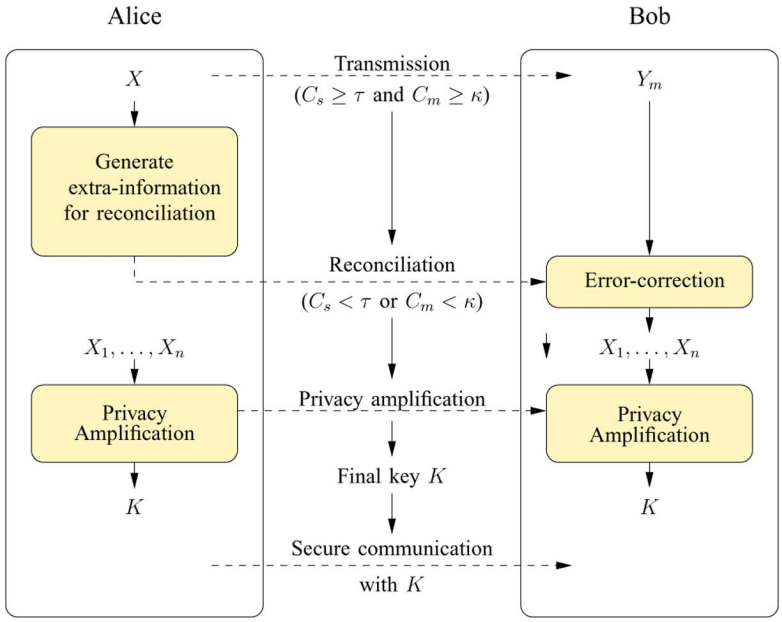

Fig. 6. Flowchart of the opportunistic protocol.

amplification [25] support the idea that the generation of information-theoretically secure keys from common randomness is a somewhat less difficult problem, suggesting a four-step approach to secure communications: *randomness sharing*, *information reconciliation*, *privacy amplification*, and *secure communication*.

- **Opportunistic randomness sharing.** To share randomness, Alice transmits discrete random symbols, represented by the RV X, over the wireless channel. Bob and Eve observe correlated symbols, represented by the RVs Y_m and Y_w, respectively. In theory, as long as Eve and Bob do not share the same information, the amount of secrecy that Alice and Bob can distill from their common randomness is nonzero [5]; however, we are interested in designing a one-way secret key agreement protocol requiring communications from Alice to Bob only. Therefore, the common randomness must be such that $I(X;Y_m) > I(X;Y_w)$. Clearly, this is the case if randomness is shared when the secrecy capacity of the wireless channel is strictly positive. Therefore, provided perfect CSI of the eavesdropper's channel is available, Alice and Bob should *opportunistically* exploit the fluctuations of the instantaneous secrecy capacity C_s with time, and they should attempt to share randomness only when C_s is sufficiently large. Specifically, in the remainder of the paper, we take the set of fading realization (γ_m, γ_w) for which an opportunistic transmission of randomness is performed to be

$$\mathcal{D}(\tau,\kappa) = \{(\gamma_m,\gamma_m) : C_s \geq \tau, C_m > \kappa\}. \qquad (11)$$

  The threshold τ ensures that a minimum amount of secrecy can be distilled from the randomness while the threshold κ ensures that the correlation between Alice and Bob's data is high enough. We shall see in Section III-B that the latter condition is required for practical algorithms. Finally, let us emphasize that, the behavior of the protocol is governed by the fading realizations in the set $\mathcal{D}(\tau,\kappa)$ and, therefore, by a probability of outage, although we assume perfect CSI of the eavesdropper's channel. This connection will be established explicitly in Section IV.
- **Key generation: reconciliation and privacy amplification.** When the estimated fading realizations are such that the secrecy capacity or main channel capacity are too small (i.e., $(\gamma_m,\gamma_w) \notin \mathcal{D}(\tau,\kappa)$), Alice and Bob communicate to generate a secure key from the shared randomness previously obtained. Key generation is performed in two steps. First, Alice and Bob "reconcile" their randomness, that is, they correct the discrepancies in their random values by exchanging additional error-correction information. Second, Alice and Bob distill secret bits from the corrected data using a technique called privacy amplification. Both procedures are detailed in Section III.
- **Secure communication.** Alice and Bob can finally use their secret key to transmit messages, using either a one-time pad to ensure perfect secrecy or any symmetric cypher.

The flowchart of the opportunistic protocol is shown in Fig. 6. Note that the randomness sharing and privacy amplification steps rely on a perfect estimation of the fading coefficients to calculate the instantaneous secrecy capacity and correctly estimate the amount of secrecy to distill. We shall see in Section IV that this assumption can be somewhat alleviated to consider a more realistic situation where only imperfect CSI (or a conservative estimate) is available for the eavesdropper's channel.

III. Practical Algorithms for Secret-Key Agreement

In this section, we describe in detail the various steps of the protocol presented in the previous section. To ease the presentation, we present the protocol for a real Gaussian wiretap channel, which corresponds to a single realization of the fading coefficients (γ_m,γ_w) and coding over one dimension only

in the wireless setup of Section II. Its performance in the quasi-static fading case is then evaluated in Section IV.

A. Secure Communication Protocol

The existence of common information between Alice and Bob is the essential ingredient for secret key agreement. In a wiretap scenario, Alice can generate this shared randomness by transmitting a sequence $X^n = (X_1, \ldots, X_n)$ of n independent and identically distributed (i.i.d.) realizations of a discrete RV X over the main channel, which provides Bob and Eve with sequences of correlated continuous RVs $Y_m^n = (Y_{m,1}, \ldots, Y_{m,n})$ and $Y_w^n = (Y_{w,1}, \ldots, Y_{w,n})$, respectively.

The channel noise introduces discrepancies between Bob's received symbols Y_m^n and Alice's symbols X^n, and Bob's estimate $\hat{X}^n = \left(\hat{X}_1, \ldots, \hat{X}_n\right)$ of Alice's symbols is erroneous. Therefore, the first step is for Alice and Bob to correct the errors before any further processing. In the context of secret key generation, this operation is called "reconciliation" and it requires an additional exchange of information between Alice and Bob. Little can be said in general about Eve's knowledge of the reconciliation messages, and we have to make the worse case assumption that this information is fully available to Eve. Note that reconciliation can be viewed as a special case of source coding with side information, where Alice compresses her source symbols X^n and Bob decodes them with the help of correlated side information Y_m^n. The Slepian–Wolf theorem [32] yields a lower bound on the total number of bits M_{rec} which have to be exchanged

$$M_{\text{rec}} \geq H\left(X^n | Y_m^n\right) = nH(X|Y_m). \tag{12}$$

Practical reconciliation algorithms introduce an overhead $\epsilon_{\text{rec}} > 0$ and require the transmission of $M_{\text{rec}} = nH(X|Y_m)(1+\epsilon_{\text{rec}})$ additional bits. Alternatively, the reconciliation can also be characterized by its efficiency β which is defined as

$$\beta = 1 - \epsilon_{\text{rec}} \frac{H(X|Y_m)}{I(X;Y_m)} \leq 1 \tag{13}$$

and the number of bits required for reconciliation is therefore

$$M_{\text{rec}} = n(H(X) - \beta I(X;Y_m)). \tag{14}$$

At the end of the reconciliation step, Alice an Bob share with high probability the common sequence X^n with entropy $n_{\text{rec}} = nH(X)$. The sequence X^n is then compressed into a binary sequence S of length n_{rec}. As discussed in Section III-B, for our application to the Gaussian wiretap channel, we use Multilevel Coding (MLC) and Multistage Decoding (MSD) to reconcile and correct the differences between $\hat{X}$ and X. Our algorithm is a more efficient version of the information reconciliation method of [26].

Privacy amplification allows Alice and Bob to extract a secret key from the binary sequence S. Its principle is to apply a well-chosen compression function $g : \{0,1\}^{n_{\text{rec}}} \rightarrow \{0,1\}^k$ ($k < n_{\text{rec}}$) to the bit sequence S, such that the eavesdropper obtains negligible information about the final k-bit sequence $g(S)$. In practice, this can be achieved by choosing g at random within a family of universal hash functions [33], as stated in the following theorem.

Theorem 1: [25, Corollary 4] Let $S \in \{0,1\}^{n_{\text{rec}}}$ be the random variable representing the bit sequence shared by Alice and Bob, let E be the random variable representing the total information about S available to the eavesdropper, and let e be a particular realization of E. If the Rényi entropy (of order 2) $R(S|E=e)$ is known to be at least c and Alice and Bob choose $K = G(S)$ as their secret key, where G is a hash function chosen at random from a family of universal hash functions $\mathcal{G} : \{0,1\}^{n_{\text{rec}}} \rightarrow \{0,1\}^k$, then

$$H(K|G, E=e) \geq k - \frac{2^{k-c}}{\ln 2}. \tag{15}$$

The total information available to Eve E consists of the sequence Y_w^n received during the first stage of the protocol, as well as the additional bits exchanged during reconciliation, represented by the random variable M. As shown in [34, Theorem 5.2], for any $s > 0$ we have

$$\begin{aligned} &R\left(S|Y_w^n = y_w^n, M = m\right) \\ &\qquad \geq R\left(S|Y_w^n = y_w^n\right) - \log_2|M| - 2s - 2 \\ &\qquad\qquad \text{with probability } 1 - 2^{-s}. \end{aligned} \tag{16}$$

The quantity $\log_2|M|$ represents the number of bits intercepted by Eve during reconciliation, which is at most $nH(X|Y_m)(1+\epsilon_{\text{rec}})$. Evaluating $R\left(S|Y_w^n = y_w^n\right)$ is in general still difficult; however, conditioned on the typicality of the bit sequence, $R\left(S|Y_w^n = y_W^n\right)$ and $H\left(S|Y_w^n = y_w^n\right)$ are equal [27]. Hence, if n is large

$$nH(X|Y_w) - nH(X|Y_m)(1+\epsilon_{\text{rec}}) - 2s - 2$$

is a good lower bound of $R(S|E=e)$, and choosing

$$k = n(\beta I(X;Y_m) - I(X;Y_w)) - 2s - 2 - r_0 \tag{17}$$

with $r_0 > 0$ guarantees that Eve's uncertainty on the key is such that

$$H\left(K|G,E\right) \geq k - \frac{2^{-r_0}}{\ln 2} \quad \text{with probability } 1 - 2^{-s}.$$

For our protocol, we use standard families of hash functions [33], [35].

Finally, the secret key generated $K = G(S)$ can be used to secure Alice's message, using either a one-time pad for perfect secrecy or a standard secret key encryption algorithm. As shown by (15), Eve's uncertainty $H(K|G, E=e)$ about the key can be made as close to k as desired.

Since the amount size of the key generated from common randomness is proportional to $\beta I(X;Y_m) - I(X;Y_w)$ bits per symbol, we choose the random variable X such that the mutual information $I(X;Y_m)$ is maximized. Ideally, Alice should choose X achieving the capacity $0.5\log_2(1+\gamma_m)$ of the main channel, which is possible only with continuous Gaussian random variables; however, the discrete support $\mathcal{X}$ and the probability mass function of X can always be optimized so that $I(X;Y_m)$ approaches the channel capacity $0.5\log_2(1+\gamma_m)$ with arbitrary precision. For instance, for a fixed size $N_c = |\mathcal{X}|$

of the support, this optimization can be performed with the algorithm proposed in [36]. Alternatively, a good approximation of the optimum can be obtained by expanding a uniformly spaced support $\{x_i\}_{i=1\ldots N_c} = \left\{\pm 1, \pm 3, \ldots, \pm\frac{N_c-1}{2}\right\}$ by a factor $\alpha \in \mathbb{R}^+$, and using a Maxwell–Boltzmann probability distribution

$$P(X = x_i) = \frac{\exp\left(-\lambda\alpha^2|x_i|^2\right)}{\sum_j \exp\left(-\lambda\alpha^2|x_i|^2\right)}. \tag{18}$$

Remark 3: Even though $I(X;Y_m)$ is not a convex function of α and λ, the optimization seems to be relatively insensitive to the initialization of the optimization. N_c should be large enough not only to ensure that $I(X;Y_m)$ approaches $0.5\log_2(1+\gamma_m)$ within the required precision, but also to be compatible with the reconciliation algorithm, as discussed in Section III-B.

Remark 4: In the above, we apply the results of [25], [32], [34], which were only proven for discrete RVs, whereas Y_m and Y_w are continuous RVs; however, it should be noted that these continuous RVs only appear as conditioning RVs in expressions such as $H(X|Y_w)$ or $R(X|Y_w)$ where X is discrete, and therefore, the various results still hold. For instance, Y_m can be quantized into a discrete RV Y_Δ such that $H(X|Y_\Delta)$ approaches $H(X|Y_m)$ with arbitrary precision as $\Delta \to 0$, and the Slepian–Wolf theorem still holds.

B. LDPC Code Construction for Gaussian Reconciliation

In this subsection, we develop an efficient reconciliation approach for the second step of the key agreement protocol. The reconciliation of binary random variables has been extensively studied and several efficient methods have been proposed [37], however, little attention has been devoted to the practical reconciliation of nonbinary random variables [26]. As stated previously, given a nonbinary RV X with distribution given by (18) and an RV Y_m obtained by sending X through an additive Gaussian channel with noise variance N_m, gain H_m, and power constraint P, the goal is to generate a minimum amount of (parity) information that Alice needs to send to Bob so that X can be recovered from Y_m.

1) Multilevel LDPC Codes for Slepian–Wolf Compression: We assume here that Alice and Bob have access to the outcomes $x^n = \{x_i\}_{i=0\ldots n-1} \in \mathcal{X}^n$ and $y_m^n = \{y_{m,i}\}_{i=0\ldots n-1} \in \mathbb{R}^n$ of instances of the random variables X^n and Y_m^n, respectively. Next, Alice sends Bob additional information to help him recover x^n based on y_m^n, and we assume without restriction that Bob recovers a binary description of x^n. Each element of $\mathcal{X}$ is uniquely described by an M-bit label ($M \geq \log_2|\mathcal{X}|$). We introduce M labeling functions $\ell_k : \mathcal{X} \to \{0,1\}$, ($k \in \{0\ldots M-1\}$), which associate to any element of $\mathcal{X}$ the kth bit of its binary label. As suggested in [38], Alice generates the additional information for Bob by computing syndromes of the sequence $\{\ell_k(x_i)\}_{k=0\ldots M-1}^{i=0\ldots n-1}$ according to some binary codes.

Given the particular Gaussian correlation considered here, the reconciliation of X and Y_m is similar to a coded modulation scheme, where Alice transmits her data over a Gaussian channel using a pulse-amplitude-modulation scheme. Most standard modulation techniques such as bit interleaved coded modulation (BICM) [39] or multilevel coding/multistage decoding (MLC/MSD) [40] schemes can therefore be adapted for reconciliation. In the case of a BICM-like reconciliation, a single syndrome is computed on an interleaved version of the bit sequence $\{\ell_k(x_i)\}_{k=0\ldots M-1}^{i=0\ldots n-1}$, whereas in the case of MLC/MSD-like reconciliation, the m syndromes of the subsequences $\{\ell_k(x_i)\}_{i=0\ldots n-1}$ ($k \in \{0\ldots M-1\}$) are computed successively, as illustrated in Fig. 7. Because of the similarity with a coded modulation scheme, the support $\mathcal{X}$ of the RV X will be referred to as a *constellation*.

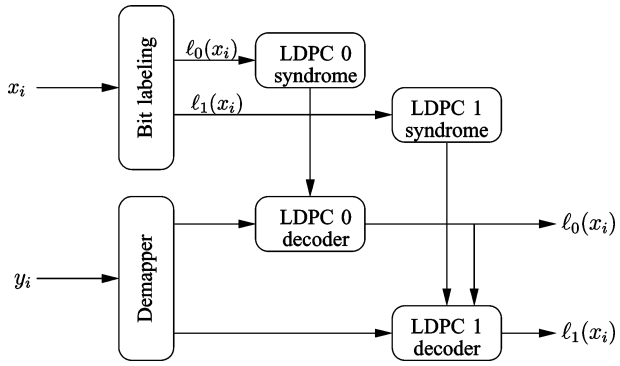

Fig. 7. Principle of MLC/MSD reconciliation in the case $M = 2$.

In what follows, we describe a reconciliation algorithm adapted from the last scheme. This choice is motivated by the fact that BICM is known to be suboptimal over the Gaussian channel; hence, the reconciliation of the RVs X and Y_m with a BICM-like scheme always requires strictly more than $H(X|Y_m)$ additional bits per symbol. Moreover, MLC/MSD is based on several component codes and, therefore, it offers more flexibility on the code design than BICM [41].

The proposed reconciliation algorithm is an MLC/MSD-like reconciliation that uses binary LDPC component codes. Other classes of codes, such as turbo codes, could be used as well; however, LDPC have already proved their worthy performance for error correction and side information coding [42]. Moreover, the belief-propagation algorithm can easily be generalized to account for the correlation between the subsequences $\{\ell_k(x_i)\}_{i=0\ldots n-1}$ ($k \in \{0\ldots M-1\}$). We use the following notation to describe the algorithm:

- $b_i^k = \ell_k(x_i)$ ($i \in \{0\ldots n-1\}, k \in \{0\ldots M-1\}$);
- $c(k)$ represents the number of check nodes at the kth level ($c(k)$ depends on the rate R^k of the code used at level k and is discussed in Section IIII-B.2);
- $m_{ij}^{(k,l)}$ denotes a message from the variable node v_i^k ($i \in \{0\ldots n-1\}$) to the check node c_j^k ($j \in \{0\ldots c(k)-1\}$) of the kth level in the lth iteration, and similarly, $m_{ji}^{(k,l)}$ denotes a message from the check node c_j^k to the variable node v_i^k of the kth level in the lth iteration;
- $\mathcal{M}_i^k$ denotes the set of all check nodes connected to the variable node v_i^k of the kth level, and $\mathcal{N}_j^k$ denotes the set of all variables nodes connected to the check node c_j^k of the kth level;
- $s(c)$ is the syndrome bit associated to the check node c.

The M levels are decoded successively, and the update equations of the messages in the lth iteration of the belief propagation

at a given level k are

$$\forall\, i \in \{0 \dots n-1\}, \quad \forall\, j \in \mathcal{M}_i^k$$
$$m_{ij}^{(k,l)} = \begin{cases} m_i^{(k,0)}, & \text{if } l = 0 \\ m_i^{(k,0)} + \sum\limits_{c_p \in \mathcal{M}_i^k \setminus c_j} (1 - 2s(c_p)) m_{pi}^{(k,l)} \end{cases} \quad (19)$$

$$\forall\, i \in \{0 \dots n-1\}, \quad \forall\, j \in \mathcal{M}_i^k$$
$$\lambda_i^{(k,l)} = \begin{cases} m_i^{(k,0)}, & \text{if } l = 0 \\ m_{i,j}^{(k,l)} + (1 - 2s(c_j)) m_{ji}^{(k,l)} \end{cases} \quad (20)$$

$$\forall\, j \in \{0 \dots c(k)-1\}, \quad \forall\, i \in \mathcal{N}_j^k$$
$$m_{ji}^{(k,l)} = \log \frac{1 + \prod_{v_p \in \mathcal{N}_j^k \setminus v_i} \tanh \frac{m_{pj}^{(k,l-1)}}{2}}{1 - \prod_{v_p \in \mathcal{N}_j^k \setminus v_i} \tanh \frac{m_{pj}^{(k,l-1)}}{2}} \quad (21)$$

where we define $m_i^{(k,0)}$ as shown in (22) at the bottom of the page. It can be shown that if the Tanner graphs of the LDPC component codes do not contain cycles, the values $\lambda_i^{(k,l)}$ converge to the true *a posteriori* log-likelihood ratios

$$\log \frac{P\left[b_i^k = 1 | b_i^0 \dots b_i^{k-1}, y_{m,i}\right]}{P\left[b_i^k = 0 | b_i^0 \dots, b_i^{k-1}, y_{m,i}\right]} \quad (23)$$

in a finite number of iterations. Finally, the decision on the value of b_i^k is made based on the sign of $\lambda_i^{(k,l_{\max})}$. In practice, even when the Tanner graphs contain cycles, this belief-propagation algorithm performs reasonably well.

The only difference between (19)–(21) and the standard update rules of belief propagation is the term $m_i^{(k,0)}$, which takes into account both the *intrinsic* information available from the observation $y_{m,i}$ as well as the *extrinsic* information available from the decoding of the other levels $p \neq k$. Equation (22) is similar to the update rule of a single-input single-output (SISO) demodulator; however, it should be noted that it involves the joint probability $p(y_m, \hat{x})$ (and not the conditional probability $p(y_m|\hat{x})$) to account for the nonuniform distribution of the symbols in $\mathcal{X}$. In theory, it should be sufficient to decode each level only once, however, in practice, performing several iterations between the levels might help improve the performance of the overall scheme. These practical issues are discussed in Section III-B.2. Finally, let us point out that the algorithms described in [42]–[44] are special cases of this general algorithm.

2) Code Rate Assignment: The optimal code rates required at each level $k \in \{0, \dots, M-1\}$ are those enforced by MSD. In fact, from the chain rule of entropy we have

$$\begin{aligned} H(X|Y_m) &= H(\ell_0(X), \dots, \ell_{M-1}(X)|Y_m) \\ &= \sum_k H(\ell_k(X)|\ell_0(X), \dots, \ell_{k-1}(X), Y_m). \end{aligned} \quad (24)$$

Hence, the $H(X|Y_m)$ bits per symbol required for reconciliation can be obtained by disclosing successively

$$H(\ell_k(X)|\ell_0(X), \dots, \ell_{k-1}(X), Y_m)$$

bits per symbol. The optimal code rate required at each level k is therefore

$$R_{opt}^k = 1 - H(\ell_k(X)|\ell_0(X), \dots, \ell_{k-1}(X), Y_m). \quad (25)$$

Equation (24) guarantees the optimality of the reconciliation scheme for any labeling; however, the practical efficiency of the reconciliation strongly depends on the mapping used. In fact, the performance of the reconciliation relies on our ability to construct capacity approaching codes for all levels k, which might not be possible if the required code rates are too low. We investigated several labeling strategies and realized that the natural binary mapping was the best compromise. This mapping assigns to each symbol $\hat{x}_j \in \mathcal{X}$ the M-bit representation of $j + (2^M - |\mathcal{X}|)/2$. Note that $\ell_0(\hat{x}_j)$ is the least significant bit of the M-bit representation. Fig. 8 shows the rates required for a constellation of size 12, with symbols and probabilities given in Table I, as a function of $10\log_{10}(\gamma_m)$.

The optimal rates of the two uppermost levels are equal to 1 over a wide range of SNRs, which greatly simplifies code design by effectively requiring only two codes. We carried out extensive simulations, and observed that for any value of the SNR, adjusting the constellations size N_c to satisfy $H(X) \approx 0.5\log_2(1 + SNR) + 1$ requires at most two codes while $I(X; Y_m)$ is maintained within a hundredth of a bit of its maximum value.

The natural mapping has the property of preserving the symmetry on the probability distribution of the random variable X

$$\forall\, k \in \{0, \dots, m-1\}, \ \forall\, y \in \mathbb{R}, \ \forall\, \hat{x}_j \in \mathcal{X}, \quad p(y, \ell_k(\hat{x}_j)) = p(-y, \ell_k(\hat{x}_j) \oplus 1). \quad (26)$$

In the first stage of the algorithm, when the bits of the 0th level are decoded, this property implies that the equivalent channel seen by the bits is output-symmetric and that these bits are also uniformly distributed. Consequently, the probability of decoding error is the same for linear LDPC codes and LDPC coset codes, which allows us to use linear LDPC codes designed with the standard density evolution method [45]. This property does not hold when decoding the following levels, however, recent results suggest that linear LDPC codes may still perform well with our coset coding scheme [46]. In order to further simplify the code design, we use irregular LDPC codes optimized for antipodal signaling over the AWGN channel as

$$m_i^{(k,0)} = \log \frac{\sum\limits_{\hat{x} \in \mathcal{X}: \ell_k(\hat{x}) = 1} p(y_{m,i}, \hat{x}) \exp\left[- \sum\limits_{p \neq k} (1 - \ell_p(\hat{x})) \left(\lambda_i^{(p,l_{\max})} - m_i^{(p,0)} \right) \right]}{\sum\limits_{\hat{x} \in \mathcal{X}: \ell_k(\hat{x}) = 0} p(y_{m,i}, \hat{x}) \exp\left[- \sum\limits_{p \neq k} (1 - \ell_p(\hat{x})) \left(\lambda_i^{(p,l_{\max})} - m_i^{(p,0)} \right) \right]}. \quad (22)$$

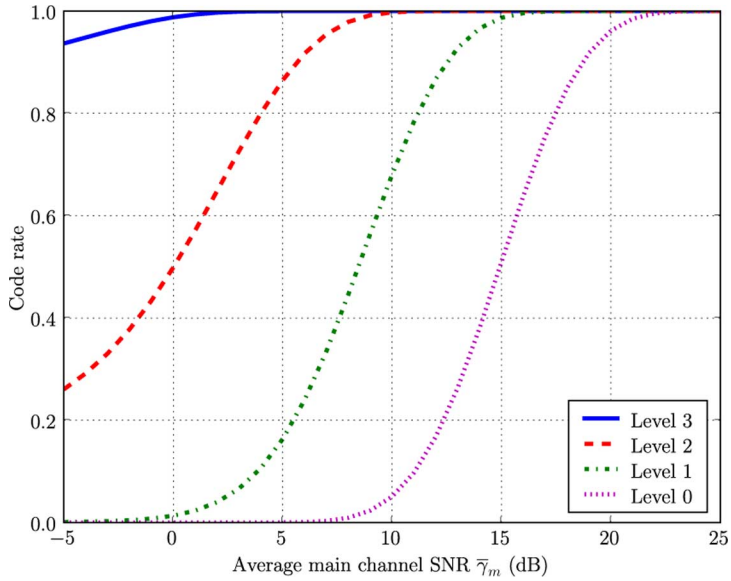

Fig. 8. Optimal code rates required for the constellation of Table I.

TABLE I
CONSTELLATION OPTIMIZED TO MAXIMIZE $I(X;Y_m)$ AT AN SNR OF 13 dB

$\hat{x}$	-2.836	-2.320	-1.804	-1.289	-0.773	-0.258	0.258	0.773	1.289	1.804	2.320	2.836
P[$\hat{x}$]	0.0040	0.0146	0.0414	0.0904	0.1522	0.1974	0.1974	0.1522	0.0904	0.0414	0.0146	0.0040
$\ell_0(\hat{x})$	0	1	0	1	0	1	0	1	0	1	0	1
$\ell_1(\hat{x})$	1	1	0	0	1	1	0	0	1	1	0	0
$\ell_2(\hat{x})$	0	0	1	1	1	1	0	0	0	0	1	1
$\ell_3(\hat{x})$	0	0	0	0	0	0	1	1	1	1	1	1

component codes. The block length used is $200,000$ and the Tanner graphs are randomly generated while avoiding cycles of length two and four. Despite this long block length, the performances of all constructed codes are still well below those of their ideal capacity achieving counterparts, therefore, perfect error correction is only achieved by lowering the code rates at each level. Unfortunately, reducing the rate of all component codes discloses far too many bits; however, as described below, a careful choice of the code rate that takes into account multiple iterations between levels makes it possible to maintain a good level of efficiency.

Our practical code rate assignment is based on an analysis of the decoding process using Extrinsic Information Transfer (EXIT) charts [47]. Although a theoretical result sustaining EXIT charts does not exist for the Gaussian channel, they emerge as a convenient tool to predict the exchange of information between the demappers and decoders involved in an iterative decoding scheme. The predictions are based on how much extrinsic information (I_E) can be computed from *a priori* information (I_A) for each demapper or decoder. There is no closed-form expression neither for the EXIT curve $I_E = T_d(I_A)$ of the demapper characterized by (22) nor for the LDPC EXIT curve $I_E = T_c(I_A)$ for 100 iterations; however, they can be obtained via Monte Carlo simulations assuming Gaussian *a priori* information [47]. Examples of transfer curves are shown in Fig. 9. We observed that low-rate codes gather extrinsic information at a slower pace than high-rate codes, therefore, we decided to correct all errors by reducing the rate

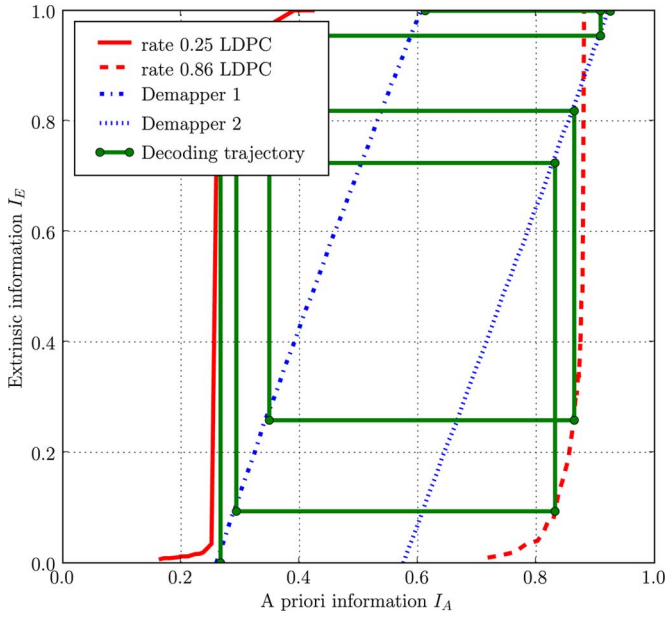

Fig. 9. Iterative decoding trajectory averaged over 10 realizations.

of the highest rate code and by using iterations between levels to compensate for the poor performance of the lower rate code.

Let us now illustrate how code rates can be chosen based on an example. Suppose that the SNR is 13 dB, for which a good choice of the constellation is given in Table I. In theory, one needs two ideal codes with rate 0.264 and 0.928. Instead, we

TABLE II
EFFICIENCY RESULTS

$10\log_{10}\gamma_m$	$\lvert\mathcal{X}\rvert$	$I(X;Y_m)$	C_m	$H(X)$	Optimal rates	Practical rates	Efficiency
2 dB	4	0.684	0.685	1.603	0.189/0.891	0.16/0.86	90.9%
7 dB	6	1.291	1.294	2.109	0.257/0.925/1	0.24/0.86/1	90.9%
10 dB	8	1.726	1.730	2.502	0.286/0.938/1	0.27/0.88/1	95.71%
13 dB	12	2.192	2.194	3.000	0.264/0.928/1/1	0.25/0.86/1/1	96.15%
20 dB	28	3.327	3.329	4.149	0.254/0.923/1/1/1	0.24/0.86/1/1/1	97.6%

use a code with rate 0.25 at the first level and look for a high rate code that gathers enough extrinsic information to start the decoding process and correct all errors with *a priori* information of 0.928. As shown in Fig. 9, a code with rate 0.86 is a good compromise. It is interesting to note that despite the approximations made in the computation of the EXIT curves, the real decoding trajectory is close to the expected behavior.

3) Efficiency Results: The results obtained for various values of the SNR are summarized in Table II. For each SNR, the size of the constellation $\mathcal{X}$, the position of constellation points, and the probability distribution are optimized according to the procedure described earlier. This ensures that $|I(X;Y_m) - C_m| \leq 0.005$ bits and limits the number of required codes to two. Let us point out that our method achieves good efficiency provided that the following two conditions are met. First, the constellation size required to maximize $I(X;Y_m)$ must be $|\mathcal{X}| \geq 4$ so that two LDPC codes can be used. Second, the code rates required cannot be too small, so that we can construct good finite length codes. This limits the applicability of the algorithm to situations where the SNR is above 2 dB.

IV. PERFORMANCE EVALUATION

A. Performance Metrics for Secure Communications

The information-theoretically secure rates of the secret key agreement protocol can be assessed only if the keys are used in conjunction with a one-time pad. However, in principle, the protocol could also be tailored to standard encryption algorithms offering computational complexity. Although no information-theoretic security can be guaranteed in this latter case, combining a physical-layer key-generation technique with a symmetric encryption scheme can still be a valid way of enhancing security. In fact, key-generation rates can be substantially higher than those offered by public-key schemes; moreover, keys generated from the physical layer are independent from one another, which ensures that the security of the system is re-initialized at each round of key-generation. An attacker who gains access to one key would be none the wiser once the key is renewed. Based on these considerations, we evaluate the performance of the opportunistic protocol using the following metric.

Definition 1: The average[1] η-secure throughput $\overline{T}_s(\eta)$ of a secret key agreement protocol is the average number of cyphertext bits transmitted per channel use, when the cyphertext is obtained with a symmetric encryption scheme such that the ratio of secret key bits used per cyphertext bit is η.

In the above definition, the secret key bits generated do not contribute to $\overline{T}_s(\eta)$ since the keys themselves do not convey any information. The case $\eta = 1$ corresponds to the situation where one bit of secret key is used for each bit of cyphertext. Without loss of generality, we can assume that the encryption scheme is a one-time pad, and therefore, $\overline{T}_s(1)$ measures an average communication rate with perfect security. When $\eta < 1$, $\overline{T}_s(\eta)$ loses all significance in terms of information-theoretically secure communication rate; however, if k_s is the key length required by an encryption scheme, the corresponding key renewal rate is k_s/η channel uses.

Unlike wiretap coding, where messages are transmitted directly and securely, secret key agreement requires additional communication to distill a key and send an encrypted message. Here, since we do not assume the existence of an additional public and error-free channel, parts of the available communication rate have to be sacrificed for that purpose. We formalize this constraint by introducing the following metric.

Definition 2: The average η-communication throughput $\overline{T}_c(\eta)$ is the average number of message bits per channel used that can be transmitted in addition to the message required for reconciliation and privacy amplification and to the messages encrypted with the keys.

Clearly, $\overline{T}_s(\eta)$ and $\overline{T}_c(\eta)$ are not independent and, by definition, take only positive values. We are now ready to characterize the maximum secure throughput of the protocol.

To simplify the notation, we use the following conventions. For a given parameter $\alpha(\gamma_m, \gamma_w)$ depending on the fading realizations (γ_m, γ_w) and a set $\mathcal{D}$ of fading realizations, we let $\langle\alpha\rangle_{\mathcal{D}}$ denote the average of $\alpha(\gamma_m, \gamma_w)$ over $\mathcal{D}$. We also assume that the coherence time of the channel is large enough, so that the block length n is large and the parameters s, r_0 of privacy amplification can be neglected, and that Alice and Bob can always communicate over the main channel at rate close to the capacity.

Proposition 4: The maximum secure throughput $\overline{T}_s(\eta)$ achievable by the opportunistic secret key agreement protocol is

$$\max_{\tau\geq 0,\kappa\geq\kappa_{min}} \eta^{-1}\langle\beta I(X;Y_m) - I(X;Y_w)\rangle_{\mathcal{D}(\tau,\kappa)}$$

subject to

$$\langle C_m\rangle_{\mathcal{D}^c(\tau,\kappa)} - \langle 2H(X) + \beta(\eta^{-1}-1)I(X;Y_m) - \eta^{-1}I(X;Y_w)\rangle_{\mathcal{D}(\tau,\kappa)} \geq 0 \quad (27)$$

where $\mathcal{D}^c(\tau,\kappa)$ denotes the complement of $\mathcal{D}(\tau,\kappa)$ in $\mathbb{R}_+^2$ and κ_{min} is imposed by the reconciliation algorithm.

Proof: When the fading realizations $(\gamma_m, \gamma_w) \in \mathcal{D}(\tau,\kappa)$, opportunistic transmission is performed. From (17), we know that the average number of key bits extractable per channel use is

$$\langle\beta I(X;Y_m) - I(X;Y_w)\rangle_{\mathcal{D}(\tau,\kappa)}$$

[1]The average is taken over all channel realizations.

and, therefore, the average secure throughput is

$$\overline{T}_s(\eta) = \eta^{-1}\langle \beta I(X;Y_m) - I(X;Y_w)\rangle_{\mathcal{D}(\tau,\kappa)}. \tag{28}$$

From (14), we also know that the average number of bits per channel use that have to be transmitted for reconciliation is

$$\langle H(X) - \beta I(X;Y_m)\rangle_{\mathcal{D}(\tau,\kappa)}. \tag{29}$$

The average number of bits per channel use required by privacy amplification depends on the number of bits required to identify a given universal hash function within its family. The minimum size of a family of universal hash functions $\mathcal{G} : \{0,1\}^{n_{\rm rec}} \to \{0,1\}^k$ is known to be at least $2^{n_{\rm rec}-k}$[48], and identifying a given function therefore requires the transmission of $n_{\rm rec} - k$ bits; however, no hashing scheme is known to achieve this bound for any $n_{\rm rec}$, therefore, we consider the more realistic situation where the identification requires the transmission of $n_{\rm rec}$ bits. For instance, this can be achieved with the following family [35]:

$$\mathcal{H}_{\mathrm{GF}(2^{n_{\rm rec}})\to\{0,1\}^{n_{\rm key}}} = \{h_c : c \in \mathrm{GF}(2^{n_{\rm rec}})\} \tag{30}$$

where $h_c(x)$ is defined as $n_{\rm key}$ distinct bits of the product cx in a polynomial representation of $\mathrm{GF}(2^{n_{\rm rec}})$. Consequently, the average number of bits per channel use required by privacy amplification is

$$\langle H(X)\rangle_{\mathcal{D}(\tau,\kappa)}. \tag{31}$$

Based on our assumption that Alice and Bob can always communicate at a rate equal to the capacity of the main channel, the average number of bits available for communication in addition to the opportunistic transmissions is

$$\langle C_m\rangle_{\mathcal{D}^c(\tau,\kappa)}. \tag{32}$$

Therefore, the communication throughput is obtained by subtracting (28)–(31) from (32), and recalling that $\overline{T}_c(\eta) \geq 0$ yields the desired result. □

B. Asymptotic Performance Analysis

Obtaining analytical expression for the optimal performance of the opportunistic communication protocol is nontrivial on several accounts. First, the simplification of the expression in Proposition 4 requires the characterization of the tradeoff between $H(X)$ and $I(X;Y_m)$ (or $I(X;Y_w)$) for an arbitrary RV X. For a given $I(X;Y_w)$, we have observed that the Maxwell–Boltzmann distribution of (18) yields a smaller $H(X)$ than most other distributions, but for every pair of fading realizations (γ_m, γ_w) the parameters α and λ have to be optimized, which makes the analytical characterization intractable. Second, the optimal performance depends on the maximization over the parameters τ and κ.

Therefore, the following analysis considers a (suboptimal) protocol where the random symbols sent over the channel during the opportunistic transmissions are chosen from a quadrature amplitude modulation (QAM) constellation with *uniform* probability. We also assume that reconciliation is performed with efficiency $\beta = 1$ for all SNRs, and we fix $\kappa = 0$. To simplify the notation, we denote $\mathcal{D}(\tau, 0)$ by $\mathcal{D}(\tau)$.

Proposition 5 (Adapted From [49]): Let C be the capacity of a complex AWGN channel with input power constraint P, and let $N = \lfloor 2^{C/2+1}\rfloor^2$. If the input symbols X are chosen uniformly at random in a square QAM constellation with N points and uniform spacing Δ along each dimension, where Δ is optimized such that $\mathbb{E}\{X^2\} \leq P$, then the mutual information between the input X and the output Y bounded as

$$C \geq I(X;Y) \geq C - \xi \text{ with } \xi > 0 \text{ independent of } C$$

and the entropy of X is bounded as

$$C + 2 \geq H(X) \geq C.$$

Using these inequalities in the equations of Proposition 4, and noting that $\langle C_m\rangle_{\mathcal{D}^c(\tau)} = F(\overline{\gamma}_m) - \langle C_m\rangle_{\mathcal{D}(\tau)}$ we obtain the bounds shown in (33)–(35) at the bottom of the page, and

$$\begin{aligned} &\eta^{-1}\langle C_m\rangle_{\mathcal{D}(\tau)} - \eta^{-1}\langle C_w\rangle_{\mathcal{D}(\tau)} + \xi P_0(\tau) && (36)\\ &\quad \geq \eta^{-1}\langle \beta I(X;Y_m) - I(X;Y_w)\rangle_{\mathcal{D}(\tau)} && (37)\\ &\quad \geq \eta^{-1}\langle C_m\rangle_{\mathcal{D}(\tau)} - \eta^{-1}\langle C_w\rangle_{\mathcal{D}(\tau)} - \xi P_0(\tau). && (38)\end{aligned}$$

1) Secrecy-Limited Regime: This regime corresponds to the situation where $\overline{\gamma}_m \to 0$, and therefore, the secrecy capacity over the wireless channel is mainly limited by the capacity of the eavesdropper's channel.

Theorem 2: In the secrecy-limited regime, the secure throughput is bounded from below as

$$\overline{T}_s(\eta) \geq \eta^{-1}\langle C_m - C_w\rangle_{\mathcal{D}(0)} - \xi P_0(0). \tag{39}$$

Proof: By definition of $\langle C_m\rangle_{\mathcal{D}(\tau)}$ and $P_0(\tau)$ we have

$$\forall\, \tau \geq 0 \quad \lim \langle C_m\rangle_{\mathcal{D}(\tau)} = 0 \quad \text{and} \quad \lim P_0(\tau) = 0 \quad \text{when } \overline{\gamma}_m \to 0. \tag{40}$$

Hence, we can take $\tau = 0$ in (35) and (35) is positive for $\overline{\gamma}_m$ small enough. □

Remark 5: This result is somewhat disappointing since the lower bound can be negative; however, in practice, by using a

$$\begin{aligned} &F(\overline{\gamma}_m) - \left(2 + \eta^{-1}\right)\langle C_m\rangle_{\mathcal{D}(\tau)} + \eta^{-1}\langle C_w\rangle_{\mathcal{D}(\tau)} + \xi(\eta^{-1} - 1)P_0(\tau) && (33)\\ &\quad \geq \langle C_m\rangle_{\mathcal{D}^c(\tau)} - \langle 2H(X) + \beta(\eta^{-1} - 1)I(X;Y_m) - \eta^{-1}I(X;Y_w)\rangle_{\mathcal{D}(\tau)} && (34)\\ &\quad \geq F(\overline{\gamma}_m) - \left(2 + \eta^{-1}\right)\langle C_m\rangle_{\mathcal{D}(\tau)} + \eta^{-1}\langle C_w\rangle_{\mathcal{D}(\tau)} - (4 + \xi\eta^{-1})P_0(\tau) && (35)\end{aligned}$$

Maxwell–Boltzmann distribution for the random symbols instead of a uniform distribution, we can expect ξ to be small. Hence, the secure throughput achievable by the protocol in the secrecy-limited regime should be close to the average secrecy capacity of the channel.

2) Communication-Limited Regime: By opposition to the secrecy-limited regime, this regime corresponds to the case where $\overline{\gamma}_m \to \infty$, and therefore the secrecy capacity is mainly limited by the capacity of the main channel.

Theorem 3: In the communication-limited regime, the secure throughput achievable by the opportunistic secret key agreement protocol is such that

$$\overline{T}_s(\eta) = \mathcal{O}\left(\eta^{-1}\log\overline{\gamma}_m\right). \tag{41}$$

Moreover, this throughput is achievable by choosing τ such that $2^\tau = \mathcal{O}(\overline{\gamma}_m)$ and in this case

$$\overline{T}_s(\eta) \approx \eta^{-1}\tau P_0(\tau), \quad \text{when } \overline{\gamma}_m \to \infty. \tag{42}$$

Before proving the result, we introduce a proposition that provides bounds for $\langle C_m\rangle_{\mathcal{D}(\tau)}$ and $\langle C_w\rangle_{\mathcal{D}(\tau)}$ depending on $P_0(\tau)$. The proof of the proposition is given in Appendix C.

Proposition 6: The average value of the main channel capacity over the set $\mathcal{D}(\tau)$ can be bounded as follows:

$$P_0(\tau)\left(\tau - \frac{\overline{\gamma}_w^2(\log 2)^{-1}}{\overline{\gamma}_w + \overline{\gamma}_m 2^{-\tau}}\right) \le \langle C_m\rangle_{\mathcal{D}(\tau)} \le P_0(\tau)\left(\tau + \overline{\gamma}_w + \overline{\gamma}_m 2^{-\tau}(\log 2)^{-1}\right). \tag{43}$$

Likewise, the average value of the wiretap channel capacity over the $\mathcal{D}(\tau)$ can be bounded as follows:

$$0 \le \langle C_w\rangle_{\mathcal{D}(\tau)} \le \frac{\overline{\gamma}_w\overline{\gamma}_m}{\overline{\gamma}_m + \overline{\gamma}_w} P_0(\tau)(\log 2)^{-1}. \tag{44}$$

Proof of Theorem 3: By using the inequalities of Proposition 6 in (35), we obtain the following lower bound on (34):

$$F(\overline{\gamma}_m) - \left(2+\eta^{-1}\right) P_0(\tau)\left(\tau + \overline{\gamma}_w + \overline{\gamma}_m 2^{-\tau}\right) - (4+\xi\eta^{-1})P_0(\tau). \tag{45}$$

For any $\overline{\gamma}_m$, to satisfy the constraint in the maximization of Proposition 4, it suffices to take τ such that

$$F(\overline{\gamma}_m)/\left[\left(2+\eta^{-1}\right)\left(\tau+\overline{\gamma}_w+\overline{\gamma}_m 2^{-\tau}(\log 2)^{-1}\right)+(4+\xi\eta^{-1})\right] \ge P_0(\tau). \tag{46}$$

For any $c_0 > 0$, we can choose τ such that $\overline{\gamma}_m 2^{-\tau} = c_0$, and $\tau = \log_2\overline{\gamma}_m - \log_2 c_0 > 0$ for $\overline{\gamma}_m$ large enough. Since

$$\lim \frac{F(\overline{\gamma}_m)}{\log\overline{\gamma}_m} = 1, \quad \text{when } \overline{\gamma}_m \to \infty$$

the left-hand side of (46) converges to

$$\frac{\log 2}{2+\eta^{-1}} \text{ when } \overline{\gamma}_m \to \infty. \tag{47}$$

From Proposition 1, the right-hand side of (46) is equal to

$$\frac{c_0}{c_0 + \overline{\gamma}_w}\exp\left(-\frac{1-2^{-\tau}}{c_0}\right); \tag{48}$$

therefore, we can always choose c_0 (independent of η) such that (46) is satisfied when $\overline{\gamma}_m \to \infty$. Substituting such a τ in (43) and (44), we have

$$\langle C_m\rangle_{\mathcal{D}(\tau)} = \mathcal{O}\left(\tau P_0(\tau)\right)$$
$$\text{and} \quad \langle C_w\rangle_{\mathcal{D}(\tau)} = \mathcal{O}\left(P_0(\tau)\right)$$

when $\overline{\gamma}_m \to \infty$. Using this in (36) and (38), we obtain the second part of the theorem

$$\eta^{-1}\langle I(X;Y_m) - I(X;Y_w)\rangle_{\mathcal{D}(\tau)} \approx \eta^{-1}\tau P_0(\tau) \quad \text{when } \overline{\gamma}_m \to \infty. \tag{49}$$

The first part of the theorem follows by recalling that $P_0(\tau) = \mathcal{O}(1)$ and $\tau = \mathcal{O}(\log\overline{\gamma}_m)$ when $\overline{\gamma}_m \to \infty$. □

Remark 6: For $\eta = 1$, the result of Theorem 3 states that, in the communication-limited regime, the information-theoretic secure rates achievable by the protocol scale as $\mathcal{O}(\log\overline{\gamma}_m)$, and therefore as $\mathcal{O}\left(\overline{C}_s\right)$. Hence, even if secret key agreement incurs a rate penalty compared to the direct use of wiretap codes, this penalty is a constant fraction of the average secrecy capacity.

C. Simulation Results

In this subsection, we use Monte Carlo simulations to estimate the secure throughput achievable by the protocol. As shown in Table II, our reconciliation algorithm achieves an efficiency above 90% as soon as the SNR of the main channel is above 2 dB. Moreover, extensive simulations show that using a (two-dimensional) Maxwell–Boltzmann distribution of the random symbols during the opportunistic transmissions allows to achieve

$$I(X;Y_m) \approx C_m, \quad I(X;Y_w) \approx C_w, \quad \text{with } H(X) \le C_m + 2. \tag{50}$$

Therefore, all simulations are obtained using these values for $I(X;Y_m)$, $I(X;Y_m)$, and $H(X)$; however, for simplicity we set $\beta = 0.1$, $\kappa = 0$, and we optimize over τ. This choice of parameters provides only an approximation of the achievable secure throughput, but this will be sufficient to confirm the analytical results of the previous section, and, given the good performance of the reconciliation algorithm presented in Section III-B, we can expect the real performance to be quite close.

The average secure throughput for $\eta = 1$ achievable by the opportunistic protocol is shown Fig. 10. As expected, the protocol is in general suboptimal since most of the main channel capacity has to be sacrificed for key agreement. In the secrecy-limited regime, as predicted in the previous section, all additional communications required for reconciliation, privacy amplification, and secure communication can be performed when the secrecy capacity is zero. In this case, $\tau = 0$ and the protocol incurs little loss of secure communication rate. On the contrary, in the communication-limited regime, the secure rate achievable

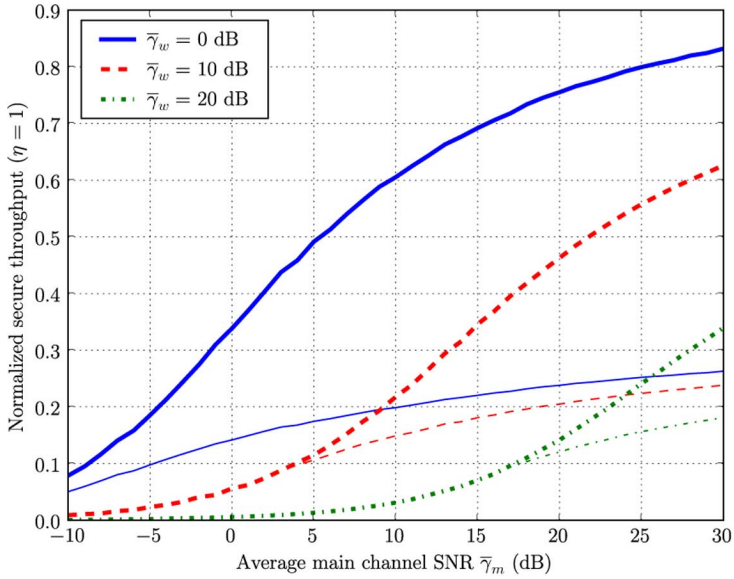

Fig. 10. Average secure throughput (thin lines) and average secrecy capacity (thick lines). All throughputs are normalized to the channel capacity of a Gaussian channel with same average SNR $\overline{\gamma}_m$.

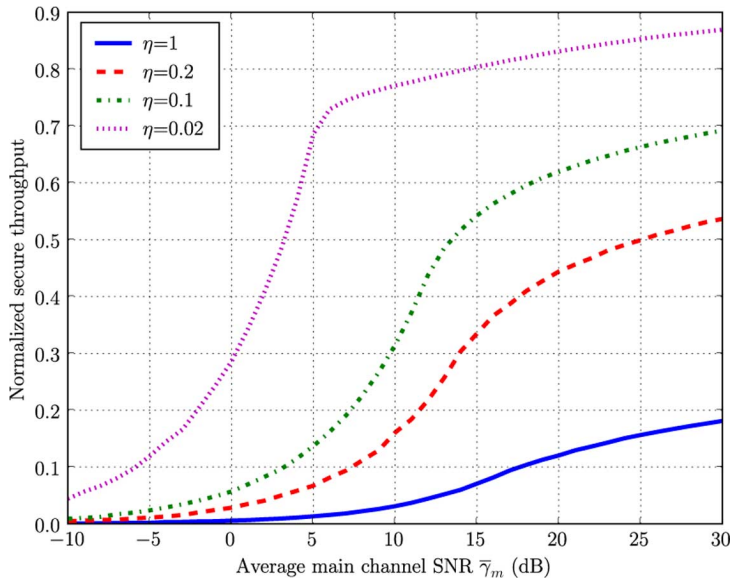

Fig. 11. Secure throughput for various values of η.

by the protocol are much lower than the secrecy capacity of the channel.

Fig. 11 shows the secure throughputs obtained for different values of η. For small values of η, the difference in behavior of the protocol in the secrecy-limited and communication-limited regimes is amplified, and the increase of the secure throughput with the $\overline{\gamma}_m$ changes radically as soon as $\tau > 0$ must be used. Strictly speaking, the protocol does not provide any information-theoretic security in this regime, since the keys generated are used to encode several bits. Nevertheless, this result shows that the protocol provides an efficient and potentially fast way of exchanging information-theoretically secure keys. In this mode of operation, it could be tailored with standard secure encryption algorithms (such as AES with 192 bits) to strengthen the current level of security of wireless communications.

D. Mitigating the Effects of Imperfect CSI

In this last subsection, we consider the situation described in Section II, where Alice has perfect CSI about the main channel fading coefficient, but only partial CSI about the eavesdropper's channel fading coefficient. As mentioned in the preceding subsection, Alice has little choice but to apply the opportunistic protocol blindly, and the keys generated have length

$$\hat{k} = n\left(\beta I\left(X;Y_m\right) - \hat{I}\left(X;Y_w\right)\right) - 2s - 2 - r_0. \qquad (51)$$

Unfortunately, the lower bound on Eve's Rényi entropy is in reality

$$n\left(\beta I\left(X;Y_m\right) - I\left(X;Y_w\right)\right) - 2s - 2. \qquad (52)$$

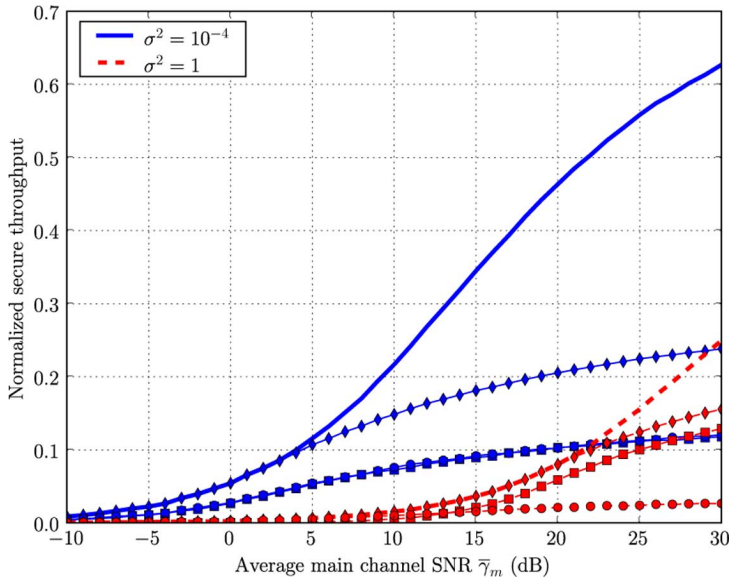

Fig. 12. Impact of imperfect CSI. Thicker lines represent the estimated average secrecy capacity. The diamond lines ($\diamond$) represent Alice's targeted average secure throughput with her imperfect CSI, the square lines ($\boxdot$) and circle lines ($\circ$), respectively, represent the true average secure throughput and average leaked throughput. All throughputs are normalized to the channel capacity of a Gaussian channel with same average SNR $\overline{\gamma}_m$.

Therefore, from Theorem 1, Eve's uncertainty on the final key is

$$H(K|E) \geq \hat{k} - \frac{2^{n\left(I(X;Y_w)-\hat{I}(X;Y_w)\right)-r_0}}{\ln 2}. \tag{53}$$

Clearly, when $I(X;Y_w) < \hat{I}(X;Y_w)$, Alice unnecessarily reduces her secure throughput, but this does not compromise the secrecy of the key; however, when $\hat{I}(X;Y_w) > I(X;Y_w)$, Alice underestimates the information leaked to the eavesdropper and subsequently generates keys whose entropy is not maximum.

Until now, we have assumed that the parameter r_0 was chosen such that $r_0 \ll n$. To mitigate the effect of imperfect CSI, let us now consider the situation where $r_0 \propto n$ and let use define

$$\alpha = \frac{r_0}{n}.$$

From (53), we see that as long as $\hat{I}(X;Y_w) - I(X;Y_w) < \alpha$, the lower bound on $H(\hat{K}|G, E = e)$ approaches $\hat{k}$ exponentially as $n \to \infty$.

The introduction of imperfect CSI and the use of the parameter α slightly modify the expression of communication throughput given in Proposition 4. $\overline{T}_s(\eta)$ is now given by

$$\max_{\tau\geq 0, \kappa \geq \kappa_{min}} \eta^{-1}\langle \beta I(X;Y_m) - I(X;Y_w) - \alpha \rangle_{\mathcal{D}(\tau,\kappa)}$$

subject to

$$\langle C_m \rangle_{\mathcal{D}^c(\tau,\kappa)} - \langle 2H(X) + \beta(\eta^{-1}-1)I(X;Y_m) - \eta^{-1}I(X;Y_w) - \eta^{-1}\alpha \rangle_{\mathcal{D}(\tau,\kappa)} \geq 0. \tag{54}$$

Contrary to the situation where perfect CSI is available, the average secure throughput defined above is not sufficient to characterize the security of the system. In fact, it only represents Alice's *targeted* secure communication rate, which might be different from the true secure communication rate. Hence, we need to introduce the true average secure throughput $\overline{\mathcal{R}}_s$ and the average leaked throughput $\overline{\mathcal{R}}_l$ defined as

$$\overline{\mathcal{R}}_s = \eta^{-1}\langle \beta I(X;Y_m) - I(X;Y_w) - \alpha \rangle_{\mathcal{D}_s} \tag{55}$$

$$\overline{\mathcal{R}}_c = \eta^{-1}\langle \beta I(X;Y_m) - I(X;Y_w) - \alpha \rangle_{\mathcal{D}_l} \tag{56}$$

where

$$\mathcal{D}_s = \left\{(\hat{\gamma_m}, \gamma_w) : \hat{C}_s \geq \tau, C_m \geq \kappa, \; I(X;Y_w) - \hat{I}(X;Y_w) < \alpha \right\} \tag{57}$$

$$\mathcal{D}_l = \left\{(\hat{\gamma_m}, \gamma_w) : \hat{C}_s \geq \tau, C_m \geq \kappa, \; I(X;Y_w) - \hat{I}(X;Y_w) \geq \alpha \right\}. \tag{58}$$

These expressions cannot be computed in close form but can be obtained with Monte Carlo simulations. We show in Fig. 12 the results obtained for an estimation noise variance of $\sigma^2 = 10$ and $\sigma^2 = 0.0001$ when $\eta = 1$ and $\alpha = 0$ (i.e., the safety parameter $r_0 \ll n$).

Interestingly, as already pointed out in Section II-B2, when Alice has a bad estimation of the eavesdropper's channel fading coefficient, and if the main channel SNR is large, most of the keys generated are still secure. This unexpected behavior is created by the asymmetry of the distribution $p(\hat{\gamma}_w|\gamma_w)$, which forces Alice to underestimate the eavesdropper fading coefficient most of the time. On the other hand, when the estimation of the wiretap CSI improves, the impact of imperfect CSI is somewhat mitigated by increasing the parameter α, which simply plays the role of a safety margin and reduces the length of the generated keys. By increasing α, the average leaked throughput can be made arbitrarily small, at the cost of a decreased secure throughput. Fig. 13 shows the results obtained for $\alpha = 0.1$. When $\sigma^2 = 0.0001$, the secure throughput loss is negligible, however, this slight increase in α suffices to

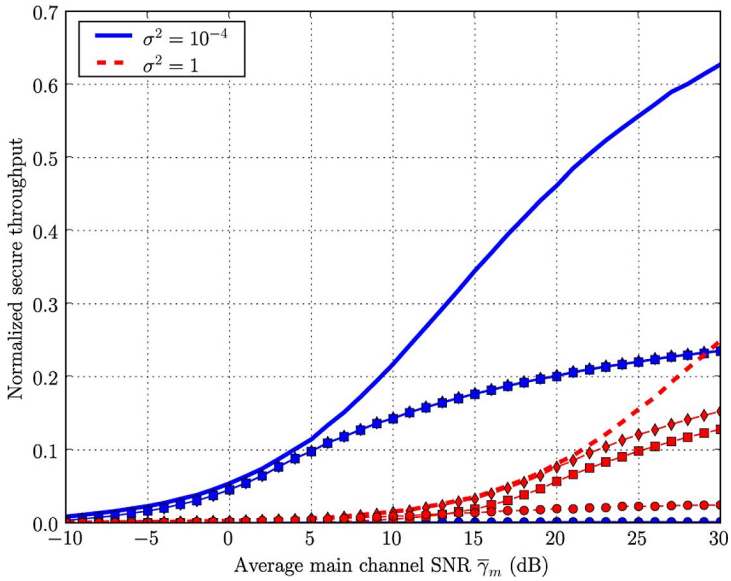

Fig. 13. Mitigation of imperfect CSI. Thicker lines represent the estimated average secrecy capacity. The diamond lines ($\diamond$) represent Alice's targeted average secure throughput with her imperfect CSI, the square lines ($\boxdot$) and circle lines ($\circ$), respectively, represent the true average secure throughput and average leaked throughput. All throughputs are normalized to the channel capacity of a Gaussian channel with same average SNR $\overline{\gamma}_m$.

ensure the secrecy of the keys generated. The mitigation is less effective when $\sigma^2 = 10$, and a further increase of α would be necessary to reduce the leaked throughput.

V. Conclusion

A. Concluding Remarks

We proposed a protocol based on one-way communications providing secure communication over quasi-static wireless channels. This scheme opportunistically exploits the fluctuations of the fading coefficients to generate information-theoretically secure keys, which are then used to encrypt messages prior to transmission. We analyzed the security provided by the protocol in the idealized case where channel state information about the wiretap channel is available, but also showed that secure communication is still achievable in the more realistic situation where only imperfect channel state information can be obtained.

The performance and complexity of the proposed scheme rely mainly on those of the reconciliation algorithm. Our LDPC-based reconciliation method is near-optimal over a wide range of SNRs; however, the memory requirements and the complexity might still be too high for embedded or low-cost systems. In future work, we will investigate new code constructions that reduce the hardware requirements while still maintaining a similar level of performance.

Let us finally mention that even though the encryption used in our scheme could be performed with a one-time pad to ensure perfect secrecy, the protocol may be of higher practical interest if combined with efficient symmetric cyphers (e.g., DES, AES) to achieve high communication rates.

B. Information-Theoretic Versus Computational Security in Wireless Networks

Due to the many fundamental differences between classical cryptography and information-theoretic security, it is useful to recognize what those differences are and how they affect the choice of technology in a wireless scenario. It is fair to state that classical cryptographic security under the computational model offers the following advantages:

- there are so far no publicly known, efficient attacks on public-key systems such as RSA, and hence they are deemed secure for a large number of applications;
- very few assumptions are made about the plaintext to be encoded, and security is provided on a block-to-block basis, meaning as long as the cryptographic primitive is secure, then every encoded block is secure;
- authentication can be achieved by means of public-key cryptography (e.g., RSA);
- systems are widely deployed, technology is readily available and inexpensive.

On the other hand, we must consider also the following disadvantages of the computational model:

- security is based on unproven assumptions regarding the hardness of certain one-way functions; therefore, systems are insecure if assumptions are wrong or if efficient attacks are developed;
- in general, there are no precise metrics or absolute comparisons between various cryptographic primitives that show the tradeoff between reliability and security as a function of the block length of plaintext and cyphertext messages—in general, the security of the cryptographic protocol is measured by whether it survives a set of attacks or not;
- in general, classical ciphers are not information-theoretically secure if the communication channel between friendly parties and the eavesdropper are noiseless, because the secrecy capacity of these application layer systems is zero;
- state-of-the art key distribution schemes for wireless networks based on the computational model require a trusted third party as well as complex protocols and system architectures [50].

The advantages of physical-layer security under the information-theoretic (perfect) security models can be summarized as follows:

- no computational restrictions are placed on the eavesdropper;
- very precise statements can be made about the information that is leaked to the eavesdropper as a function of channel quality and block length of the messages [25];
- physical-layer security as been realized in practice through quantum key distribution [51];
- in theory, suitably long codes used for privacy amplification can get exponentially close to perfect secrecy [25];
- instead of distributing keys it is possible to generate on-the-fly as many secret keys as desired.

In contrast, we have to take into consideration the following disadvantages of information-theoretic security:

- information-theoretic security is an average-information measure. The system can be designed and tuned for a specific level of security—e.g., with very high probability a block is secure, but it may not be able to guarantee security with probability 1;
- it requires assumptions about the communication channels that may not be accurate in practice. In many cases, one would make very conservative assumptions about the channels. This is likely to result in low secrecy capacities and low secret key or -message exchange rates, yielding high security and reliability, yet at low communication rates;
- a few systems (e.g., quantum key distribution) are deployed but the technology is not as widely available and is expensive;
- a short secret key is still required for authentication [5].

In light of the brief comparisons above, it is likely that any deployment of a physical-layer security protocol in a classical system would be part of a "layered security" solution where security is provided at a number of different layers, each with a specific goal in mind. This modular approach is how virtually all systems are designed today, so in this context, physical-layer security provides an additional layer of security that does not exist in today's communication systems.

Appendix A
Proof of Lemma 1

Suppose that both the main and the wiretap channel are complex AWGN channels, i.e., the transmit and receive symbols are complex and both additive noise processes are zero mean circularly symmetric complex Gaussian. The power of the complex input X is constrained according to $\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\{|X(i)|^2\} \leq P$. Since each use of the complex AWGN channel can be viewed as two uses of a real-valued AWGN channel [52, Appendix B], the secrecy capacity of the complex wiretap channel follows from (3) as

$$C_s = \log\left(1+\frac{P}{N_m}\right) - \log\left(1+\frac{P}{N_w}\right)$$

per complex dimension.[2]

[2]Alternatively, this result can be proven by repeating step by step the proofs of [30] using complex-valued random variables instead of real-valued ones.

To complete the proof, we introduce complex fading coefficients for both the main channel and the eavesdropper's channel, as detailed in Section II-A. Since in the quasi-static case H_m and H_w are random but remain constant for all time, it is perfectly reasonable to view the main channel (with fading) as a complex AWGN channel [52, Ch. 5] with SNR $\gamma_m = P|h_m|^2/N_m$ and capacity

$$C_m = \log\left(1+|h_m|^2\frac{P}{N_m}\right).$$

Similarly, the capacity of the eavesdropper's channel is given by

$$C_w = \log\left(1+|h_w|^2\frac{P}{N_w}\right)$$

with SNR $\gamma_w = P|h_w|^2/N_w$. Thus, once again based on (3) and the nonnegativity of channel capacity, we may write the secrecy capacity for one realization of the quasi-static fading scenario as (4).

Appendix B
Proof of Proposition 3

An outage event occurs whenever Alice overestimates the amount of secrecy she can distill from an opportunistic transmission. Therefore

$$\begin{aligned}\mathcal{P}_{\text{out}} &= \mathrm{P}\left[\hat{C}_s > C_s, C_s \geq \tau_s, C_m > \tau_m\right] \leq \mathrm{P}\left[\hat{C}_s > C_s\right] \\ &= \mathrm{P}\left[\hat{\Gamma}_w < \Gamma_w\right].\end{aligned}$$

Now, $\mathrm{P}\left[\hat{\Gamma}_w < \Gamma_w\right]$ can be written as follows:

$$\begin{aligned}\mathrm{P}\left[\hat{\Gamma}_w < \Gamma_w\right] &= \int_0^\infty \mathrm{P}\left[\hat{\Gamma}_w < \Gamma_w | \Gamma_w = \gamma_w\right] p(\gamma_w) d\gamma_w \\ &= \int_0^\infty \left(\int_0^{\gamma_w} p(\hat{\gamma}_w|\gamma_w) d\hat{\gamma}_w\right) p(\gamma_w) d\gamma_w\end{aligned}$$

where $p(\gamma_w)$ is the probability density function of Γ_w (see (2)) and $p(\hat{\gamma}_w|\gamma_w)$ is the probability density function of $\hat{\Gamma}_w$ conditioned on Γ_w. This probability density function is noncentral χ^2 with two degrees of freedom, i.e.,

$$p(\hat{\gamma}_w|\gamma_w) = \frac{1}{2\bar{\gamma}_w\sigma_e^2} e^{-\frac{(\gamma_w+\hat{\gamma}_w)}{2\bar{\gamma}_w\sigma_e^2}} I_0\left(\frac{\sqrt{\gamma_w\hat{\gamma}_w}}{\bar{\gamma}_w\sigma_e^2}\right), \quad \hat{\gamma}_w > 0$$

where $I_0(\cdot)$ is the zeroth-order modified Bessel function of the first kind [53]. Thus, the probability $\mathrm{P}\left[\hat{\gamma}_w < \gamma_w | \gamma_w\right]$ reduces to

$$\begin{aligned}&\mathrm{P}\left[\hat{\Gamma}_w < \Gamma_w | \Gamma_w = \gamma_w\right] \\ &\qquad = 1 - Q_1\left(\sqrt{\gamma_w/(\bar{\gamma}_w\sigma_e^2)}, \sqrt{\gamma_w/(\bar{\gamma}_w\sigma_e^2)}\right)\end{aligned}$$

where $Q_1(\cdot,\cdot)$ is the generalized Marcum Q function [53]. Using standard results for integrals involving the generalized Marcum Q function [54], the upper bound to the outage probability reduces to

$$\mathcal{P}_{\text{out}} \leq \frac{1}{2} - \frac{1}{2}\frac{1}{\sqrt{1+2/\sigma_e^2}}. \tag{59}$$

APPENDIX C
PROOF OF PROPOSITION 6

The main channel capacity averaged over the realization in $\mathcal{D}(\tau)$ can be expanded as follows:

$$\langle C_m\rangle_{\mathcal{D}(\tau)} = \int_{\mathcal{D}(\tau)} \log_2(1+\gamma_m)\, p(\gamma_m)p(\gamma_w)d\gamma_m d\gamma_w \quad (60)$$

$$= \int_{2^\tau-1}^{\infty} \log_2(1+\gamma_m)\, p(\gamma_m) \left(\int_0^{2^{-\tau}(\gamma_m+1)-1} p(\gamma_w)d\gamma_w\right) d\gamma_m \quad (61)$$

$$= \int_{2^\tau-1}^{\infty} \log_2(1+\gamma_m)\, \frac{1}{\overline{\gamma}_m} e^{-\gamma_m/\overline{\gamma}_m} \left(1 - e^{\frac{2^{-\tau}(\gamma_m+1)-1}{\overline{\gamma}_m}}\right) d\gamma_m \quad (62)$$

$$= \int_{2^\tau-1}^{\infty} \log_2(1+\gamma_m)\, \lambda_1 e^{-\gamma_m\lambda_1} d\gamma_m - \frac{\overline{\gamma}_w}{\overline{\gamma}_w + 2^{-\tau}\overline{\gamma}_m} e^{-\frac{2^{-\tau}-1}{\overline{\gamma}_w}} \int_{2^\tau-1}^{\infty} \log_2(1+\gamma_m)\, \lambda_2 e^{-\lambda_2\gamma_m} d\gamma_m \quad (63)$$

where

$$\lambda_1 = \frac{1}{\overline{\gamma}_m} \quad \text{and} \quad \lambda_2 = \frac{\overline{\gamma}_w + \overline{\gamma}_m 2^{-\tau}}{\overline{\gamma}_w\overline{\gamma}_m}.$$

To obtain simple bounds of this expression, we introduce a simple lemma.

Lemma 2: $\forall\, \lambda > 0$, we have

$$e^{-\lambda x}\log(1+x) \le \int_x^{\infty} \log(1+z)\,\lambda e^{-\lambda z} dz \le e^{-\lambda x}\log(1+x) + \frac{e^{-\lambda x}}{\lambda(x+1)} \quad (64)$$

Proof: The upper bound in the lemma follows by integrating the left-hand side by parts as

$$\int_x^{\infty} \log(1+z)\,\lambda e^{-\lambda z} dz = e^{-\lambda x}\log(1+x) + e^{\lambda}\mathrm{E}_1((x+1)\lambda) \quad (65)$$

where $\mathrm{E}_1(x)$ is the exponential-integral function. The result follows by bounding the exponential-integral function as $\mathrm{E}_1(x) \le e^{-x}/x$. The lower bound follows by noting that $\log(1+z) \ge \log(1+x)$ for $z \ge x$, therefore

$$\int_x^{\infty} \log(1+z)\,\lambda e^{-\lambda z} dz \ge \log(1+x)\int_x^{\infty} \lambda e^{-\lambda z} dz = e^{-\lambda x}\log(1+x). \quad (66)$$

□

By applying the lemma on each of the two terms of the right-hand side, we obtain

$$\langle C_m\rangle_{\mathcal{D}(\tau)} \le \tau e^{-\frac{2^\tau-1}{\overline{\gamma}_m}} + \frac{e^{-\frac{2^\tau-1}{\overline{\gamma}_m}}}{2^\tau\log 2}\overline{\gamma}_m - \frac{\overline{\gamma}_w}{\overline{\gamma}_w + 2^{-\tau}\overline{\gamma}_m} e^{-\frac{2^{-\tau}-1}{\overline{\gamma}_w}} \tau e^{-\frac{\overline{\gamma}_w+\overline{\gamma}_m 2^{-\tau}}{\overline{\gamma}_m\overline{\gamma}_m}(2^\tau-1)}$$

$$= e^{-\frac{2^\tau-1}{\overline{\gamma}_m}} \left(\tau + \frac{\overline{\gamma}_m}{2^\tau\log 2} - \tau\frac{\overline{\gamma}_w}{\overline{\gamma}_w + 2^{-\tau}\overline{\gamma}_m}\right) = P_0(\tau)\left(\tau + \overline{\gamma}_w + \overline{\gamma}_m 2^{-\tau}(\log 2)^{-1}\right). \quad (67)$$

Likewise, by reversing the bounds we obtain

$$\langle C_m\rangle_{\mathcal{D}(\tau)} \ge \tau e^{-\frac{2^\tau-1}{\overline{\gamma}_m}} - \frac{\overline{\gamma}_w}{\overline{\gamma}_w + 2^{-\tau}\overline{\gamma}_m} e^{-\frac{2^{-\tau}-1}{\overline{\gamma}_w}} \times \left(\tau + \frac{1}{2^\tau\log 2}\frac{\overline{\gamma}_w\overline{\gamma}_m}{\overline{\gamma}_w + \overline{\gamma}_m 2^{-\tau}}\right) \times e^{-\frac{\overline{\gamma}_w+\overline{\gamma}_m 2^{-\tau}}{\overline{\gamma}_m\overline{\gamma}_m}(2^\tau-1)} \quad (68)$$

$$= e^{-\frac{2^\tau-1}{\overline{\gamma}_m}} \left(\tau - \tau\frac{\overline{\gamma}_w}{\overline{\gamma}_w + 2^{-\tau}\overline{\gamma}_m} - \frac{\overline{\gamma}_w}{\overline{\gamma}_w + 2^{-\tau}\overline{\gamma}_m}\frac{1}{2^\tau\log 2}\frac{\overline{\gamma}_w\overline{\gamma}_m}{\overline{\gamma}_w + \overline{\gamma}_m 2^{-\tau}}\right) \quad (69)$$

$$= P_0(\tau)\left(\tau - \frac{1}{\log 2}\frac{\overline{\gamma}_w^2}{\overline{\gamma}_w + \overline{\gamma}_m 2^{-\tau}}\right). \quad (70)$$

To bound the wiretap channel capacity averaged over the realizations in $\mathcal{D}(\tau)$ we write

$$\langle C_w\rangle_{\mathcal{D}(\tau)} = \int_{\mathcal{D}(\tau)} \log_2(1+\gamma_w)\, p(\gamma_m)p(\gamma_w)d\gamma_m d\gamma_w \quad (71)$$

$$= \int_0^{\infty} \log_2(1+\gamma_w)p(\gamma_w) \left(\int_{2^\tau(1+\gamma_w)-1}^{\infty} p(\gamma_m)d\gamma_m\right) d\gamma_w \quad (72)$$

$$= \int_0^{\infty} \log_2(1+\gamma_w)p(\gamma_w) \left(e^{-\frac{2^\tau(1+\gamma_w)-1}{\overline{\gamma}_m}}\right) d\gamma_w \quad (73)$$

$$= P_0(\tau)\int_0^{\infty} \log_2(1+\gamma_w)\frac{\overline{\gamma}_m + \overline{\gamma}_w 2^\tau}{\overline{\gamma}_w\overline{\gamma}_m} e^{-\frac{\overline{\gamma}_m+\overline{\gamma}_w 2^\tau}{\overline{\gamma}_w\overline{\gamma}_m}\gamma_w} d\gamma_w. \quad (74)$$

The result follows by noting that for any $\tau \ge 0$

$$0 \le \int_0^{\infty} \log_2(1+\gamma_w)\frac{\overline{\gamma}_m + \overline{\gamma}_w 2^\tau}{\overline{\gamma}_w\overline{\gamma}_m} e^{-\frac{\overline{\gamma}_m+\overline{\gamma}_w 2^\tau}{\overline{\gamma}_w\overline{\gamma}_m}\gamma_w} d\gamma_w \le \frac{1}{\log 2}\int_0^{\infty} \gamma_w\frac{\overline{\gamma}_m + \overline{\gamma}_w 2^\tau}{\overline{\gamma}_w\overline{\gamma}_m} e^{-\frac{\overline{\gamma}_m+\overline{\gamma}_w 2^\tau}{\overline{\gamma}_w\overline{\gamma}_m}\gamma_w} d\gamma_w = \frac{1}{\log 2}\frac{\overline{\gamma}_w\overline{\gamma}_m}{\overline{\gamma}_m + \overline{\gamma}_w 2^\tau} \le \frac{1}{\log 2}\frac{\overline{\gamma}_w\overline{\gamma}_m}{\overline{\gamma}_m + \overline{\gamma}_w}. \quad (75)$$

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1948.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[4] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

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

[6] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[7] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. IEEE Military Communications Conf. (IEEE MILCOM 2005)*, Atlantic City, NJ, Oct. 2005, pp. 1–6.

[8] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. 62nd IEEE Vehicular Technology Conf. (VTC-2005-Fall)*, Dallas, TX, Sep. 2005, vol. 3, pp. 1906–1910.

[9] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT 2005)*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

[10] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 356–360.

[11] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secrecy capacity region of fading broadcast channels," in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, Jun. 2007, pp. 1291–1295.

[12] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. 44th Annu. Allerton Conf. Communications, Control and Computing*, Monticello, IL, Sep. 2006, pp. 841–848.

[13] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, Jun. 2007, pp. 1306–1310.

[14] G. D. Forney Jr. and G. Ungerboeck, "Modulation and coding for linear gaussian channels," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2384–2415, Oct. 1998.

[15] E. Biglieri, J. Proakis, and S. Shamai (Shitz), "Fading channels: Information-theoretic and communications aspects," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2619–2692, Oct. 1998.

[16] L. H. Ozarow and A. D. Wyner, "Wire tap channel II," *AT&T Bell Lab. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, Dec. 1984.

[17] V. Wei, "Generalized hamming weights for linear codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, Sep. 1991.

[18] A. Thangaraj, S. Dihidar, 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.

[19] R. Liu, Y. Liand, H. V. Poor, and P. Spasojević, "Secure nested codes for type ii wiretap channels," in *Proc. 2007 IEEE Information Theory Workshop*, Lake Tahoe, CA, Sep. 2007, pp. 337–342.

[20] M. Hayashi, "Exponents of channel resolvability and wire-tapped channel," in *Proc. IEEE Int Symp. Information Theory and Its Applications (ISITA)*, Parma, Italy, 2004, pp. 1080–1085.

[21] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, Apr. 2006.

[22] J. Muramatsu, "Secret key agreement from correlated source outputs using low density parity check matrices," *IEICE Trans. Fund. Elec. Commun. Comp.*, vol. E89-A, no. 7, pp. 2036–2046, Jul. 2006.

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

[24] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, Mar. 1999.

[25] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[26] G. V. Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum-distributed Gaussian key," *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 394–400, Feb. 2004.

[27] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology—Eurocrypt 2000 (Lecture Notes in Computer Science)*, B. Preneel, Ed. Berlin, Germany: Springer-Verlag, pp. 351–351.

[28] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[29] S. Nitinawarat, "Secret key generation for correlated Gaussian sources," in *Proc. 45th Annu. Allerton Conf. Communications, Control and Computing*, Monticello, IL, Sep. 2007, pp. 1054–1058.

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

[31] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2001.

[32] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 4, pp. 471–480, Jul. 1973.

[33] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comp. Syst. Sci.*, vol. 18, pp. 143–154, 1979.

[34] C. Cachin and U. M. Maurer, "Linking information reconciliation and privacy amplification," *J. Cryptol.*, vol. 10, no. 2, pp. 97–110, Mar. 1997.

[35] M. N. Wegman and J. Carter, "New hash functions and their use in authentication and set equality," *J. Comp. Sci. Syst.*, vol. 22, pp. 265–279, 1981.

[36] N. Varnica, X. Ma, and A. Kavčić, "Capacity of power constrained memoryless awgn channels with fixed input constellations," in *Proc. IEEE Global Telecommunications Conf. (IEEE GLOBECOM '02)*, Taipei, Taiwan, Nov. 2002, vol. 2, pp. 1339–1343.

[37] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology-Eurocrypt'93 (Lecture Notes in Computer Science)*, T. Helleseth, Ed. Berlin, Germany: Springer-Verlag, 1993, pp. 411–423.

[38] A. Wyner, "Recent results in the shannon theory," *IEEE Trans. Inf. Theory*, vol. IT20, no. 1, pp. 2–10, Jan. 1974.

[39] G. Caire, G. Taricco, and E. Biglieri, "Bit-interleaved coded modulation," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 927–946, May 1998.

[40] U. Wachsmann, R. F. H. Fischer, and J. B. Huber, "Multilevel codes: Theoretical concepts and practical design rules," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1361–1391, Jul. 1999.

[41] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, "LDPC-based Gaussian key reconciliation," in *Proc. IEEE Information Theory Workshop*, Punta del Este, Uruguay, Mar. 2006, pp. 116–120, arXiv: cs.IT/0509041.

[42] A. D. Liveris, Z. Xiong, and C. N. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Commun. Lett.*, vol. 6, no. 10, pp. 440–442, Oct. 2002.

[43] Y. Nana, E. Sharon, and S. Litsyn, "Improved decoding of LDPC coded modulations," *IEEE Commun. Lett.*, vol. 10, no. 5, pp. 375–377, May 2006.

[44] J. Chen, D. He, and A. Jagmohan, "Slepian-Wolf code design via source-channel correspondence," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 2433–2437.

[45] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.

[46] C.-C. Wang, S. R. Kulkarni, and H. V. Poor, "Density evolution for asymmetric memoryless channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4216–4236, Dec. 2005.

[47] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Commun.*, vol. 49, no. 10, pp. 1727–1737, Oct. 2001.

[48] D. R. Stinson, "Universal hashing and authentication codes," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1991, vol. 576, pp. 74–85.

[49] L. Ozarow and A. Wyner, "On the capacity of the Gaussian channel with a finite number of input levels," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1426–1428, Nov. 1990.

[50] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," *IEEE Pers. Commun.*, vol. 1, no. 1, pp. 25–31, 1993.

[51] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computer Systems and Signal Processing.*, Bangalore, India, 1984, pp. 175–179.

[52] D. N. C. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[53] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2001.

[54] M. Simon and M. -S. Alouini, "Some new results for integrals involving the generalized Marcum q function and their application to performance evaluation over fading channels," *IEEE J. Wireless Commun.*, vol. 2, no. 4, pp. 611–615, Jul. 2003.