Baldi *et al. EURASIP Journal on Wireless Communications and Networking* (2015) 2015:232
DOI 10.1186/s13638-015-0463-6

EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Security gap analysis of some LDPC coded transmission schemes over the flat and fast fading Gaussian wire-tap channels

Marco Baldi*, Nicola Maturo, Giacomo Ricciutelli and Franco Chiaraluce

Abstract

It is known that the error rate can be used as a measure of reliability and security over the wire-tap channel when practical, finite length codes are used for transmission, and the security gap is an error rate based metric able to jointly treat these two aspects. In this paper, we consider several low-density parity-check (LDPC) coded transmissions, which represent the state of the art for transmissions over the wire-tap channel and we assess and compare their security gap performance. We consider two kinds of wire-tap channels: the flat and the fast fading wire-tap channels with additive white Gaussian noise. As a reference, we use the progressive edge growth (PEG) algorithm for the design of unstructured LDPC codes and compare its performance with that of four approaches for designing structured LDPC codes. We analyze both systematic and non-systematic transmissions and show that some structured code design techniques are able to achieve comparable or even better performance than the PEG algorithm over the considered channels, while taking advantage of their simpler encoding and decoding procedures.

Keywords: AWGN wire-tap channel; Fast fading wire-tap channel; LDPC codes; Physical layer security; Security gap

1 Introduction

Physical layer security (PLS) is a breakthrough in communications security paradigms, since it allows to achieve secure transmissions without the need of any form of pre-shared secret within the group of legitimate users. A first level of security, in fact, can be achieved through the physical layer, only exploiting the difference between the channels of legitimate receivers and those of potential eavesdroppers. Such a security level may suffice by itself or, more frequently, may constitute a basis for higher layer cryptographic protocols.

This setting is well represented by the simple wire-tap channel model [1], in which there is a transmitter (Alice) sending some confidential information to a legitimate receiver (Bob), in the presence of an eavesdropper (Eve). The transmission technique used by Alice is perfectly known by both Bob and Eve. However, the channel between Alice and Bob is inherently different from the channel between Alice and Eve; hence, only based on this difference, there is the expectation that the information sent from Alice to Bob is not successfully retrieved by Bob.

In this paper, we focus on the Gaussian wire-tap channel model, for which transmission security can be achieved only when Bob's channel has a higher signal-to-noise ratio (SNR) than Eve's channel [2]. As a metric for PLS, we use a parameter which allows for a straightforward assessment and comparison of practical transmission schemes, based on the error rate achieved by Bob and Eve. This parameter is the so-called *security gap*, first introduced in [3]. It is defined as the quality ratio between Bob's and Eve's channels that is required to achieve a sufficient level of PLS, while ensuring that Bob reliably receives the transmitted information. An analytical definition of the security gap will be given in Section 2.

It must be said that other performance metrics exist and are also often used for assessing transmissions over this kind of channels. However, the error rate and the security gap have the advantage to depend on all the characteristics of the code used for transmission. Therefore, they allow to assess each specific code and compare its performance

*Correspondence: m.baldi@univpm.it
Dipartimento di Ingegneria dell'Informazione (DII), Università Politecnica delle Marche, Via Brecce Bianche, 60131, Ancona, Italy

with others (for example, having exactly the same parameters, but designed with a different technique). Among the other metrics, an important role is played by information theoretic tools, which allow to estimate the maximum amount of secret information that can travel from Alice to Bob. This way, the ultimate capacity limits can be computed (see, for example, [4, 5]). However, finding practical transmission techniques which are actually able to approach these bounds is still an open challenge. Another very useful security metric is the eavesdropper's equivocation rate on the secret message [6, 7]. The error rate, however, provides a more direct metric also in practical experiments [8] and is more suited for the comparison between different coding schemes, which is the main target of this paper.

The security gap measures the possibility to have reliable and secure transmissions even with a small degradation of Eve's channel with respect to Bob's channel. If this occurs, the security gap is small, that is, close to 1. On the contrary, if the security gap is large, that is, much greater than 1, a great difference between Bob's and Eve's channels is required, which is, obviously, a less favorable operation condition.

Figure 1 provides a pictorial representation of two cases in which the security gap is large (a) and small (b), respectively. In the figure, we consider the presence of Alice (A), Bob (B), and two eavesdroppers (E_1 and E_2). The inner region (green) defines the zone where Bob should stand in order to enjoy a sufficiently low error rate. The outer region (red) instead is the zone where eavesdroppers should be, since their error rate is sufficiently high to ensure security. The critical region is the intermediate one (grey), where a legitimate receiver cannot stand, since its error rate would be too high, while a wiretapper—like E_1 in Fig. 1a—can eavesdrop a non-negligible amount of information, as its error rate is not sufficiently high. Therefore, such an area is useless for the purposes of transmission, and the security gap gives a measure of its extension. When the security gap is small, the grey area is small as well, and the transition from the region reserved to legitimate receivers to the region where eavesdroppers should stay becomes sharper.

In this paper, the security gap is first computed in the presence of thermal noise only, that is, over the flat additive white Gaussian noise (AWGN) channel and then also in the presence of fast fading (FF). We focus on state-of-the-art low-density parity-check (LDPC) codes, which are capacity-achieving codes under belief propagation (BP) iterative decoding [9], and have been shown to achieve astonishing performance over the wire-tap channel as well [4]. However, previous works in this line of research have mostly been focused on flat AWGN channels. In [3, 10, 11], it has been shown that an effective way of reducing the security gap consists in using punctured LDPC codes over these channels. On the other hand, the use of punctured codes brings the disadvantage of an increase in the power consumption. In some of our previous papers [12–14], we have demonstrated that similar, and even larger, reductions in the security gap can be achieved by using scrambled transmissions, and with considerable power saving with respect to punctured codes. A similar approach can also be used in the context of IEEE 802.11 wireless networks, where less powerful convolutional codes are used in the place of LDPC codes [15]. More recently, the same strategies have also been extended to the Rayleigh fading channel [16] and to the broadcast channel with confidential messages [17, 18].

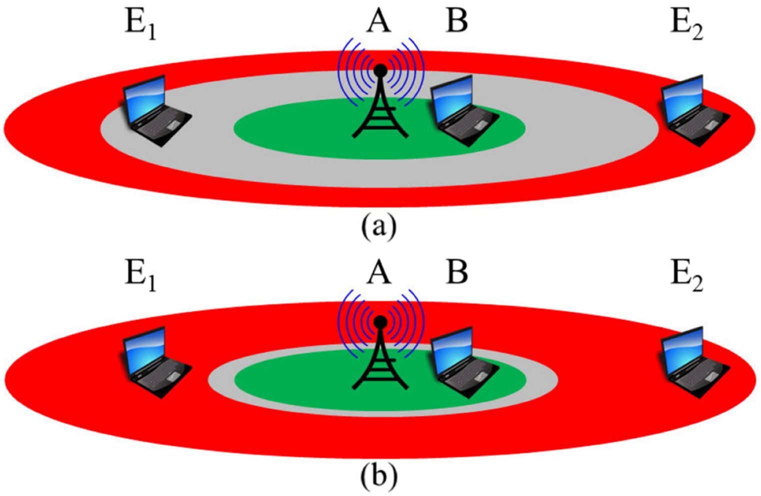


Fig. 1 Effect of large (**a**) and small (**b**) security gaps

In this paper, we address the problem of choosing an LDPC code design technique with the aim of reducing the security gap over flat and FF wire-tap channels. For this purpose, we consider some different LDPC code construction techniques and assess their performance in such a framework. We evaluate the security gap, through numerical simulations, for each of the considered code design techniques. Information scrambling can contribute to reduce the security gap; thus, we extend the comparative analysis in the presence of such an option, applied to single frames or even to multiple concatenated frames. At the transmitter, scrambling permits to realize non-systematic coding, which is an essential prerequisite for security (also puncturing achieves the same result, but in a different manner). At the receiver, the corresponding descrambler, necessary to re-obtain the information vector, allows to increase the number of residual errors outgoing Eve's decoder. In particular, scrambling is defined *perfect* when even a single error at the descrambler input produces about half of the information bits in error at the output and with randomly distributed error positions. In our previous papers [14, 15], we have verified that perfect scrambling is rather easy to approach in practice.

In this work, we provide clear indications about the code design techniques which are preferable to use for reducing the security gap when systematic or scrambled transmissions are implemented. As already mentioned, alternatively to scrambling, we could use puncturing to achieve non-systematic coding and repeat the same comparative assessment, although we do not expect that different conclusions would result. A preliminary version of this analysis was presented in [19] where, however, only flat Gaussian wire-tap channels were considered.

The organization of the paper is as follows. In Section 2, we introduce the channel models and the basic notation and definitions. In Section 3, we describe the LDPC code design techniques that we consider, whose performance is assessed in Section 4 for the wire-tap channel models of interest. Finally, Section 5 concludes the paper.

2 System model and notation

In the wire-tap channel model that we consider, Alice wishes to send a secret $1 \times k$ binary information vector $\mathbf{u}$ to Bob. For this purpose, she encodes $\mathbf{u}$ into a $1 \times n$ binary codeword $\mathbf{c}$, with $n > k$, and transmits it over the channel. In the following, we assume that transmission employs binary phase shift keying (BPSK) modulation. The codeword $\mathbf{c}$ is received by Bob and Eve through two different channels, corrupted by AWGN with different noise variance.

Two kinds of channel are considered in this paper: the first one is a flat AWGN channel, where only thermal noise is present, and the second one is an FF channel corrupted by AWGN, where each transmitted bit experiences a different channel gain, in addition to thermal noise.

Both these scenarios are covered by the model reported in Fig. 2, where w_{B} and w_{E} represent AWGN samples. For the flat AWGN channel, the coefficients h_{B} and h_{E} are constant and equal to 1. Hence, the SNR per bit, noted by γ in the following, is simply given by the ratio E_b/N_0 between the energy per bit and the one-side power spectral density of the thermal noise.

For the FF channel, instead, h_{B} and h_{E} represent the fading coefficients for Bob's and Eve's channels, respectively, which are Rayleigh distributed.

More precisely, the real and imaginary parts of h_{B} and h_{E} are Gaussian random variables with mean 0 and variance 1/2; hence, the squared modulus of h_{B} and h_{E} is chi-square distributed. The thermal noise is present also in this case. It follows that the SNR per bit (which has to be specialized for Bob and Eve, but we omit the subscripts B and E for the sake of simplicity), $\gamma = |h|^2 E_b/N_0$, is chi-square distributed as well, with probability density function:

$$p_\Gamma(\gamma) = \frac{1}{\overline{\gamma}} e^{-\gamma/\overline{\gamma}}, \quad \gamma \geq 0, \tag{1}$$

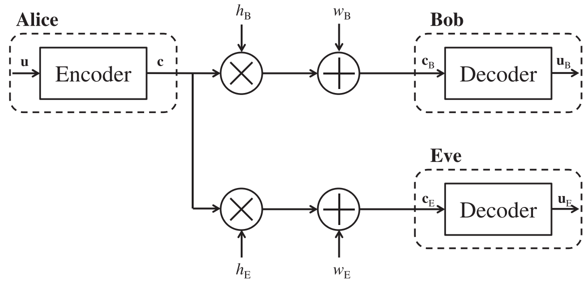
where $\overline{\gamma} = E_b/N_0$ is the mean value.

Contrary to the flat AWGN channel, where the bit error rate (BER) is fixed for a given SNR, for the FF channel, the bit error rate is a random variable as well, with a mean value

$$\overline{P_b} = \int_0^\infty \mathrm{Q}\left(\sqrt{2\gamma}\right) p_\Gamma(\gamma) d\gamma = \frac{1}{2}\left[1 - \sqrt{\frac{\overline{\gamma}}{1+\overline{\gamma}}}\right] \tag{2}$$

where $\mathrm{Q}(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt$ is the complementary distribution function of the zero-mean, unit-variance Gaussian distribution.

Equation (2) refers to the case of the absence of coding. If an error correcting code with rate $R = k/n$ is applied, the argument of the function Q(.) must be replaced with $\sqrt{2\gamma R}$ and $\overline{P_b}$ has the meaning of mean channel bit error rate, while the BER at the decoder output must be computed by taking into account the effect of the decoding algorithm.



Alice
u
Encoder
c
h_{B}
w_{B}
Bob
$\mathbf{c}_{\mathrm{B}}$
Decoder
$\mathbf{u}_{\mathrm{B}}$
Eve
$\mathbf{c}_{\mathrm{E}}$
Decoder
$\mathbf{u}_{\mathrm{E}}$
h_{E}
w_{E}

Fig. 2 Wire-tap channel model

Since we assume that Alice sends messages divided into frames of n bits each, we can get an estimate of the mean frame error rate (FER) as

$$\overline{P_f} = 1 - \left(1 - \overline{P_b}\right)^n . \tag{3}$$

In the presence of coding, the previous considerations on $\overline{P_b}$ apply and the FER is evaluated at the decoder output.

For both the flat and the FF channels, the security gap S_g can be formally defined as follows. Let us fix two suitable thresholds for Bob's and Eve's FER, named $P_f^{\mathrm{B}}\Big|_{\mathrm{th}}$ and $P_f^{\mathrm{E}}\Big|_{\mathrm{th}}$, respectively. In order to have reliability, we impose that Bob's mean FER is $\leq P_f^{\mathrm{B}}\Big|_{\mathrm{th}}$; dually, in order to have security, we impose that Eve's mean FER is $\geq P_f^{\mathrm{E}}\Big|_{\mathrm{th}}$. On the other hand, taking into account the error rate dependence on the SNR, the same conditions can be translated in terms of the channel quality by imposing $\overline{\gamma_{\mathrm{B}}} \geq \gamma_{\mathrm{B}}|_{\mathrm{th}}$ and $\overline{\gamma_{\mathrm{E}}} \leq \gamma_{\mathrm{E}}|_{\mathrm{th}}$, where $\gamma_{\mathrm{B}}|_{\mathrm{th}}$ and $\gamma_{\mathrm{E}}|_{\mathrm{th}}$ are the SNR values corresponding to $P_f^{\mathrm{B}}\Big|_{\mathrm{th}}$ and $P_f^{\mathrm{E}}\Big|_{\mathrm{th}}$, respectively, and $\overline{\gamma_{\mathrm{B}}}$ and $\overline{\gamma_{\mathrm{E}}}$ are the mean SNRs for Bob and Eve, respectively.

The security gap is defined as

$$S_g = \frac{\gamma_{\mathrm{B}}|_{\mathrm{th}}}{\gamma_{\mathrm{E}}|_{\mathrm{th}}}. \tag{4}$$

According to this definition, it is evident that S_g, that is always greater than 1, should be kept as close to 1 as possible, in such a way that the reliability and security targets are reached even with a small degradation of Eve's channel quality with respect to Bob's.

An example of S_g computation is shown in Fig. 3, where the SNR is expressed in dB (which justifies the difference in place of the ratio). Based on its definition, it is clear that the security gap depends on the steepness of the FER curve: the steeper the slope, the smaller the security gap.

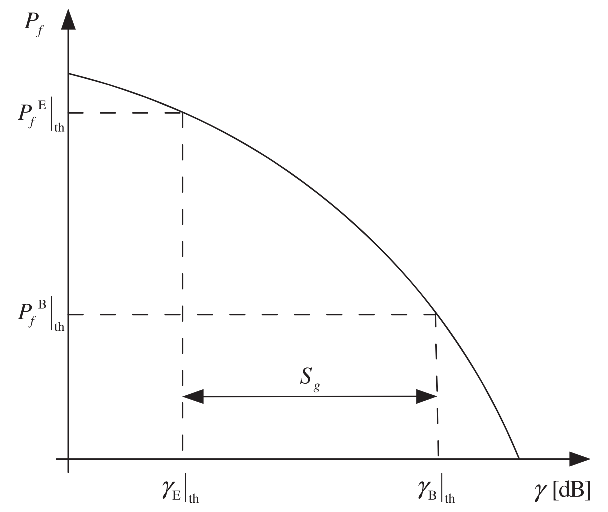


Fig. 3 Pictorial representation of the security gap

It is also evident that S_g can be equally determined after having fixed the threshold values $P_b^{\mathrm{B}}|_{\mathrm{th}}$ and $P_b^{\mathrm{E}}|_{\mathrm{th}}$ on the BER instead of the FER. Actually, this is the choice that will be done in Section 4, which is devoted to the presentation of the numerical results.

The value of S_g clearly depends on the decoder used by Bob and Eve, respectively. Since we focus on LDPC codes, it is natural to consider BP iterative decoding, which ensures near-optimum performance with limited complexity. Hence, we assume that both Bob and Eve use the BP decoder.

As mentioned above, an important target from the PLS standpoint is to keep the security gap as small as possible. Since systematic transmission yields large security gaps, in [3, 10, 11], the use of punctured codes is proposed, by associating the secret bits to punctured bits. As shown in [12–14], an alternative solution is to scramble the information bits prior to encoding them. This approach allows achieving similar or even better reductions in the security gap than puncturing; moreover, a smaller signal power is required to achieve Bob's reliability target.

Scrambling can be applied to single frames. Better performance, however, can be achieved when L information vectors ($L > 1$) are concatenated together and then multiplied by a $kL \times kL$ non-singular scrambling matrix. Then, the resulting vector is divided again into L subvectors, which are individually encoded and transmitted. At the receiver side, after having received the corresponding L codewords, and having exploited the channel code to correct the errors affecting them, the received information vectors are concatenated again and descrambled together through the inverse scrambling matrix. This way, the message transmitted by Alice is recovered only if all the errors affecting the L vectors have been corrected. Otherwise, during descrambling, a single residual bit error can be spread over all L vectors, thus causing maximum uncertainty. Hence, only Bob, who is very likely able to correct all the errors induced by the channel, can recover the message transmitted by Alice, while Eve suffers a BER close to 0.5.

As we have shown in [12–14], when the scrambling matrix is a random dense matrix, it is able to approach the effect of a perfect scrambler, which increases and spreads ideally (i.e., with maximum uncertainty) the residual errors over the received vectors. In this case, the BER equals half the FER, since a frame which is received in error corresponds to an error rate approximately equal to 0.5 on its bits, after descrambling. This effect is further emphasized when $L > 1$, since, in this case, a single frame received in error within a block of L frames implies that all the L frames are in error after descrambling. Despite the condition of a BER equal to 0.5 coincides with achieving the maximum uncertainty for Eve, it must be observed that the error positions after descrambling are not independent and identically distributed (i.i.d.). Therefore, we cannot state that this system achieves perfect secrecy [1], since a BER equal to 0.5 does not coincide with maximum entropy at Eve's (as it would occur in the case of i.i.d. error positions).

3 LDPC code construction techniques

In this section, we describe five LDPC code design techniques which we consider for assessing their performance in terms of security gap over the considered wire-tap channels.

We use as a benchmark the progressive edge growth (PEG) code design technique [20], which is a well-consolidated solution for designing very good unstructured LDPC codes. The PEG technique aims at maximizing the length of the local cycles in the Tanner graph associated with an LDPC code. This allows to achieve very good performance under BP decoding, which is strongly influenced by the Tanner graph properties. On the other hand, LDPC codes designed through the PEG algorithm have parity-check matrices without any inner structure, which may be responsible for a significant complexity when encoding and decoding are implemented in hardware.

For this reason, several techniques have been proposed in the literature to design codes having structured parity-check matrices, which facilitate the hardware and even software implementation. We consider four different methods to design structured LDPC codes and assess their security gap performance in comparison with that achieved through the PEG algorithm. These techniques are briefly reminded next.

3.1 Quasi-cyclic codes

Quasi-cyclic (QC) LDPC codes are a class of codes able to join the excellent performance of LDPC iterative decoding with the low complexity encoding which characterizes QC codes. In fact, QC codes have the desirable property of being encodable through simple barrel shift registers, which have complexity increasing in the code redundancy. We remind that a code is QC if a shift of a codeword by n_0 positions yields another (or the same) codeword. A cyclic code is a special case of QC code (corresponding to $n_0 = 1$).

QC-LDPC codes have structured generator and parity-check matrices, formed by circulant blocks. Several ways of designing QC-LDPC codes are known in the literature. Two main classes are those using cyclic permutation matrices, like array LDPC codes [21], and those using general sparse circulant matrices [22].

The latter, in particular, contain a class of very simple codes which are able to achieve good performance, especially at high code rate. They are characterized by a parity-check matrix in the form of a single row of circulant blocks [23]:

$$\mathbf{H} = \left[\mathbf{H}_0|\mathbf{H}_1|\ldots|\mathbf{H}_{n_0-1}\right], \tag{5}$$

where $\mathbf{H}_i, i = 0, 1, \ldots, n_0 - 1$ is an $r \times r$ circulant matrix, being r the number of redundancy bits. We consider QC-LDPC codes having a parity-check matrix in the form (5), with constant column weight equal to d_v. In this case, it can easily be shown that the code minimum distance is $\leq 2d_v$ and the corresponding multiplicity is $\approx \binom{n_0}{2}$ [22].

3.2 Serially concatenated codes

Another powerful, though simple, class of structured LDPC codes is represented by multiple serially concatenated multiple parity-check (M-SC-MPC) codes [24]. These codes exploit the serial concatenation of very simple components, similarly to what is proposed in [25], where single parity-check component codes are used. By employing different component codes, which however remain very simple, M-SC-MPC codes are described through sparse parity-check matrices which ensure good performance under BP decoding.

As shown in Fig. 4, an M-SC-MPC code is obtained as the serial concatenation of M component codes, each with k_i information bits and r_i redundancy bits, with $i = 1, 2, \ldots, M$. The serial concatenation is systematic; hence, each component code appends its r_i redundancy bits to the input codeword. The i-th component MPC code computes its j-th redundancy bit, with $j = 1, \ldots, r_i$, as the EX-OR of the codeword bits whose indexes are smaller than j by an integer multiple of r_i. It follows from its definition that an M-SC-MPC code has a lower triangular parity-check matrix with a simple inner structure. An example of such structure is given in Fig. 5, for a code with $M = 3$. The black diagonals denote symbols 1, while the other symbols are 0. The structured nature of M-SC-MPC codes makes their encoding very easy [24], and also, the implementation of LDPC decoders may benefit by the form of their parity-check matrix.

3.3 Interleaved product LDPC codes

It is known that a special structure of LDPC code can be obtained in the form of a bi-dimensional product code using two smaller LDPC codes as components [26, 27].

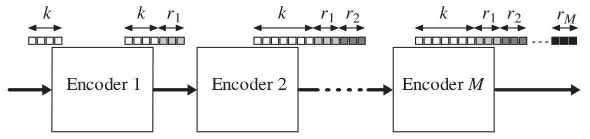


Fig. 4 M-SC-MPC encoder

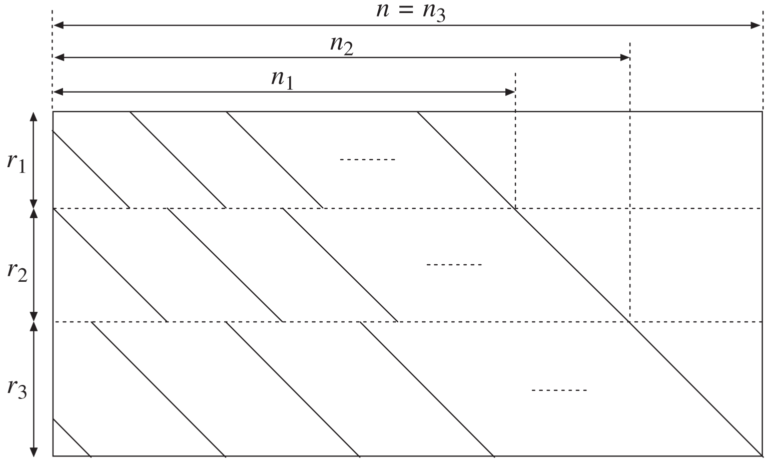


Fig. 5 Parity-check matrix of an M-SC-MPC code with $M = 3$

Noting by d_a and d_b, respectively, the minimum distances of the two component codes, a distinctive feature of the product code is the "multiplicative property", by virtue of which the minimum distance d_p of the product code can be obtained as $d_p = d_a d_b$.

However, the codes obtained rarely exhibit good performance under BP decoding due to the very regular structure of their Tanner graph. This drawback can be overcome by introducing an interleaver between the two component codes [28]. Interleaving is crucial in the design of turbo codes, and it is also exploited in the design of turbo product codes [29]. In particular, we are interested in the use of column interleavers that are able to preserve the multiplicative property. This result is achieved by interleaving only one of the two component codes. In other terms, a column interleaver only permutes the elements within each row of the encoding matrix. Since the interleaver acts after row encoding, the effect of the row component code is unaltered and, before column encoding, at least d_a columns contain a symbol 1. It follows that the code minimum distance remains $d_p = d_a d_b$.

A further benefit of interleaving is that it also helps in reducing the number of minimum weight codewords [28]. As a counterpart, the use of an interleaver produces a slight increase in the complexity that however remains limited because of the very simple encoding procedure which is typical of product codes.

3.4 Progressive differences convolutional LDPC codes

Recently, an increasing interest has been devoted to LDPC convolutional codes, which are able to join the advantages of convolutional codes with the very good performance of LDPC codes. In particular, convolutional codes have the advantage to be encodable through very simple circuits and to allow decoding based on a sliding window, which does not need the whole stream to be received before starting to decode it.

A particularly interesting class of LDPC convolutional codes is that of time-invariant codes, which are able to achieve very good performance with limited complexity [30]. In this paper, we focus on the technique we have proposed in [31], which is able to design codes, named progressive difference convolutional low-density parity-check (PDC-LDPC) codes that are characterized by a very small constraint length (that is, a relatively small number of memory elements in the encoder shift registers). This permits us to design even rather short convolutional codes and to easily terminate them without incurring significant losses in the code rate.

PDC-LDPC codes are based on ordered sets of progressive differences as separations between symbols 1 in their parity-check matrix columns and exhibit the important features to have, by construction, known minimum distance (independently of the rate) and Tanner graphs without cycles.

4 Security gap assessment

In order to assess the performance of the considered LDPC code design techniques from the PLS standpoint, we have used them to design five LDPC codes having fixed code length and rate, and we have estimated their security gap through numerical simulations. All the considered codes have length $n = 1024$ and nominal rate $R = 3/4$ (as specified below, the rate is slightly different for the interleaved product code). The first code is a reference LDPC code designed through the PEG algorithm, having constant variable node degree equal to 5. The second code is a QC-LDPC code with a parity-check matrix in the form (5): it consists of four 256×256 circulant matrices having row and column weight equal to 5. It has been designed through the random difference families technique [32], which ensures that there are no short cycles in the associated Tanner graph. The third code is an M-SC-MPC code having $M = 5$ component MPC codes, with $r_1 = 45$, $r_2 = 47$, $r_3 = 52$, $r_4 = 53$, and $r_5 = 59$. The fourth code is an interleaved product code having, as components, a $(n_1 = 64, k_1 = 51)$ PEG code and a $(n_2 = 16, k_2 = 15)$ single parity-check code. In this case, the code rate is 0.747, that is, slightly lower than 3/4. Moreover, the resulting parity-check matrix column weight is smaller than for the other codes due to the constraints imposed by the product code structure. In fact, the mean column weight is 2.71, while it is about 5 for the other codes. The last code is a PDC-LDPC code with parity-check matrix column weight 5. We have used a tail-biting termination to comply with the fixed code length and code rate.

The log-likelihood ratio sum product algorithm (LLR-SPA) with floating-point variables [33] is used for LDPC decoding of all the considered schemes. This choice ensures in fact a minor influence of finite precision problems with respect to belief propagation iterative decoding algorithms. According to the channel models in Section 2, the symbol received upon transmission of a symbol x is obtained as $y = hx + w$ (see Fig. 2), where h is the Rayleigh distributed channel gain experienced at the corresponding symbol time and w is a thermal noise sample. For the BPSK modulation, here considered, the corresponding a priori LLR is computed as $M(y) = 4y\gamma R$ [13]. The values of $M(y)$ for each received symbol are the starting point for the LLR-SPA iterative decoding algorithm.

We assume that the receiver is able to reconstruct exactly the received signal phase, which is a necessary condition to use phase shift keying modulation efficiently, but it has not complete channel state information.

Hence, the a priori LLR is obtained by using the mean SNR value $\overline{\gamma} = E_b/N_0$ and results in $M(y) = 4yE_s/N_0$, where $E_s = E_bR$ is the energy per channel symbol. It is interesting to observe that $M(y)$ is the same for both the flat and the FF channels.

4.1 Performance over the flat AWGN channel

Figure 6 reports the BER performance achieved by the designed codes, by using systematic transmission (i.e., without scrambling) over the flat AWGN channel. In order to evaluate the security gap for the considered coding schemes, we fix $P_b^{\mathrm{B}}\big|_{\mathrm{th}} = 10^{-5}$ and $P_b^{\mathrm{E}}\big|_{\mathrm{th}} = 0.4$ (these values are significant enough for practical applications) and determine the corresponding values of $\gamma_{\mathrm{B}}|_{\mathrm{th}}$ and $\gamma_{\mathrm{E}}|_{\mathrm{th}}$, from which the security gap is easily obtained by using (4).

The results of such an evaluation are reported in Table 1. We notice that using systematic transmission yields very large security gaps. In fact, in order to achieve $P_b^{\mathrm{E}}\big|_{\mathrm{th}} = 0.4$, all codes require $\gamma_{\mathrm{E}}|_{\mathrm{th}} = -13.6$ dB, which is a very low signal-to-noise ratio (this value is not covered by the abscissa range in Fig. 6 for better readability of the plots in the region of low error rates). The resulting security gap is in the order of 18 dB, and the smallest value (17.19 dB) is achieved by the M-SC-MPC code.

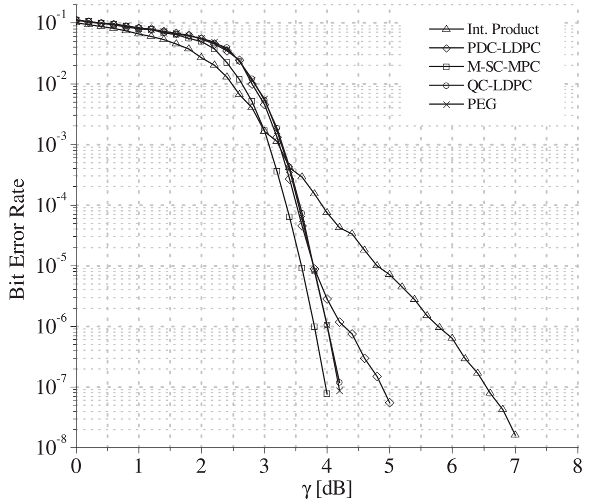


Fig. 6 BER performance with systematic transmission for codes with $n = 1024$ and code rate $R = 3/4$ over the flat AWGN channel

It is interesting to notice that the value of the security gap is determined, on one hand, by the slope of the error rate curve in the waterfall region and, on the other hand, by the slope of the same curve in the flat region. Indeed, these two slopes correspond to quite different code behaviors, the former determining Bob's performance and the latter Eve's performance. The flat region, in particular, is critical, as to achieve $P_b^{\mathrm{E}}\big|_{\mathrm{th}} = 0.4$, as required, forces us to consider very small values of γ.

The situation considerably improves by resorting to scrambling: the BER performance for this case is reported in Fig. 7. By assuming a perfect scrambler which acts on each transmitted frame, the bit error rate is BER = FER/2. A practical perfect scrambler can be approached through a dense $k \times k$ scrambling matrix. As we can see from the figure, the first and most important effect of scrambling is to increase the flatness of the curve in its initial part. As a consequence, $\gamma_{\mathrm{E}}|_{\mathrm{th}}$ is considerably increased, while

Table 1 Security gap with systematic transmission over the flat AWGN channel

Code	$\gamma_{\mathrm{E}}\|_{\mathrm{th}}$ [dB]	$\gamma_{\mathrm{B}}\|_{\mathrm{th}}$ [dB]	S_g [dB]
Int. product	−13.6	4.81	18.41
PDC-LDPC	−13.6	3.78	17.38
M-SC-MPC	−13.6	3.59	17.19
QC-LDPC	−13.6	3.78	17.38
PEG	−13.6	3.78	17.38

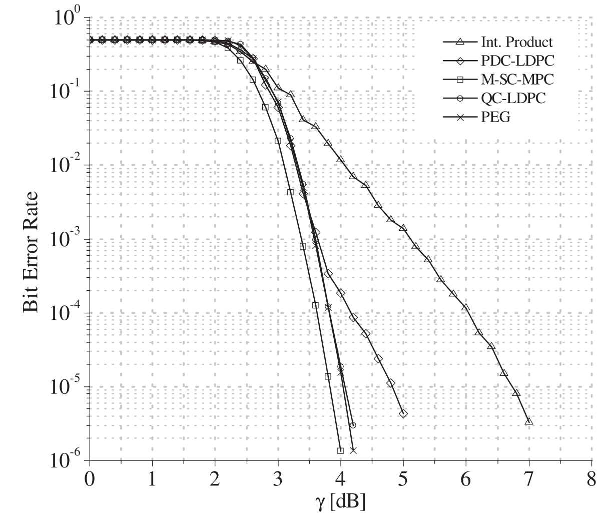


Fig. 7 BER performance with perfect scrambling for codes with $n = 1024$ and code rate $R = 3/4$ over the flat AWGN channel

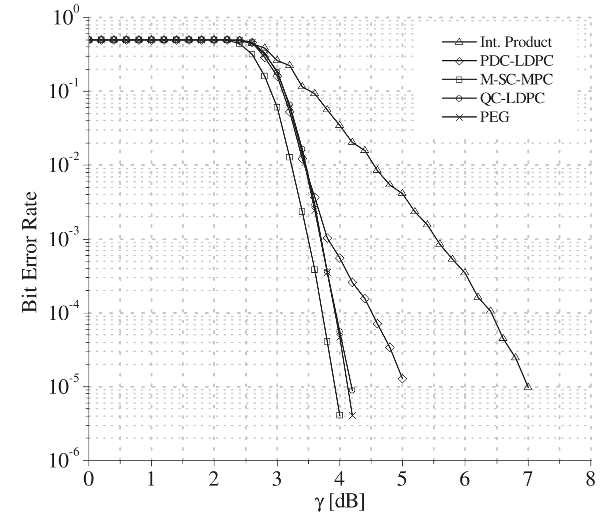


Fig. 8 BER performance with perfect scrambling and $L = 3$ for codes with $n = 1024$ and code rate $R = 3/4$ over the flat AWGN channel

$\gamma_B|_{th}$ is only slightly increased (because the impact on the waterfall region is much less relevant).

The corresponding SNR threshold values are reported in Table 2, together with the security gap. We observe that the use of scrambling allows reducing the security gap down to some dBs, which means to accept a moderate quality difference between Bob's and Eve's channels.

The best result in this case is achieved by the PEG code that yields a security gap equal to 1.62 dB. The security gap of the M-SC-MPC solution, however, is very close, with the additional advantage to require an SNR for Bob that is 0.24 dB smaller than that required by the PEG code.

A further improvement can be achieved by concatenating $L > 1$ messages and scrambling them together. In this case, again under the assumption of perfect scrambling, the relationship between the BER and the FER is as follows:

$$\text{BER} = \frac{1 - (1 - \text{FER})^L}{2}. \tag{6}$$

Figure 8 shows the performance achieved with $L = 3$ and a $3k \times 3k$ perfect scrambler. As reported in Table 3, the security gap is further reduced, with respect to the values in Table 2, at the expense of some additional delay due to frame concatenation. The best results are achieved by the PEG and M-SC-MPC codes, with a security gap $S_g = 1.46$ dB. As in Table 2, Bob's SNR is smaller for the M-SC-MPC code.

4.2 Performance over the fast fading channel

The discussion developed in Section 4.1 can be repeated for the FF channel with AWGN, obtaining similar conclusions. Details are reported next.

Figure 9 shows the BER performance in the case of a systematic transmission, while Table 4 gives the relevant numerical values. Also in this case, we fix $P_b^B|_{th} = 10^{-5}$ and $P_b^E|_{th} = 0.4$ and obtain the corresponding values of $\gamma_B|_{th}$ and $\gamma_E|_{th}$, from which the security gap is computed according to (4).

As expected, because of the presence of fast fading, the security gap is now increased (see Table 1 for comparison). Moreover, as for the flat AWGN channel case, the best performance is achieved by the M-SC-MPC code ($S_g = 21.4$ dB).

Table 2 Security gap with perfect scrambling over the flat AWGN channel

Code	$\gamma_E\|_{th}$ [dB]	$\gamma_B\|_{th}$ [dB]	S_g [dB]
Int. product	2.27	6.74	4.47
PDC-LDPC	2.32	4.83	2.51
M-SC-MPC	2.17	3.80	1.63
QC-LDPC	2.44	4.10	1.66
PEG	2.42	4.04	1.62

Table 3 Security gap with perfect scrambling and $L = 3$ over the flat AWGN channel

Code	$\gamma_E\|_{th}$ [dB]	$\gamma_B\|_{th}$ [dB]	S_g [dB]
Int. product	2.75	7.00	4.25
PDC-LDPC	2.66	5.05	2.39
M-SC-MPC	2.46	3.92	1.46
QC-LDPC	2.68	4.19	1.51
PEG	2.67	4.13	1.46

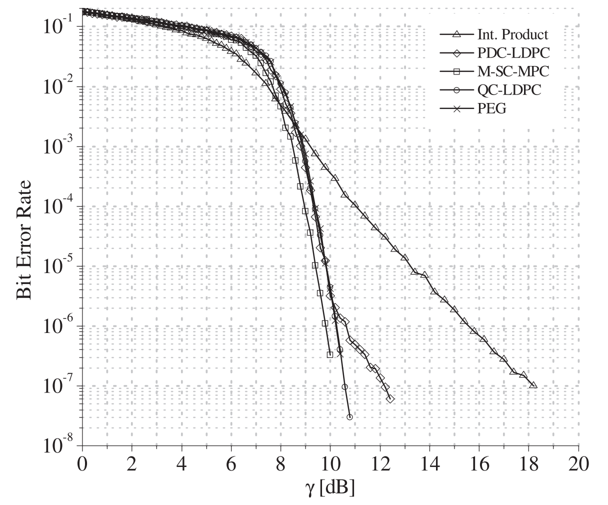


Fig. 9 BER performance with systematic transmission for codes with $n = 1024$ and code rate $R = 3/4$ over the FF channel with AWGN

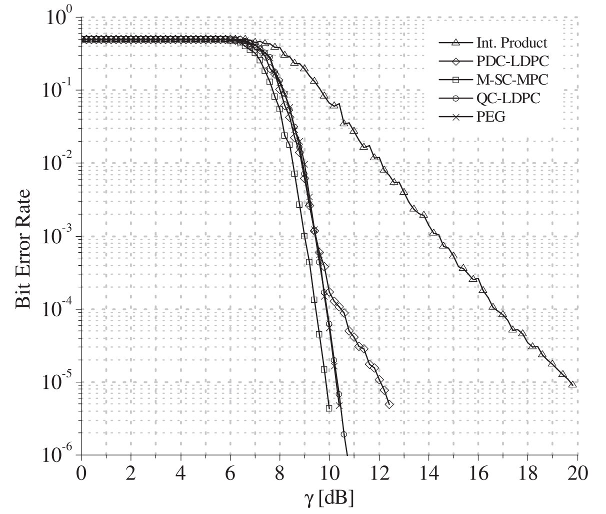


Fig. 10 BER performance with perfect scrambling for codes with $n = 1024$ and code rate $R = 3/4$ over the FF channel with AWGN

Similarly to the flat AWGN channel case, we can improve the security gap performance by resorting to scrambling. Figure 10 and Table 5 refer to the case of perfect scrambling performed over a single frame, while Fig. 11 and Table 6 consider the case of perfect scrambling acting over multiple frames. In both scenarios, the security gap value for the PEG, QC-LDPC, and M-SC-MPC constructions are almost identical, but the M-SC-MPC scheme has the advantage of requiring smaller SNRs. We also observe that, similarly to the flat AWGN channel, the S_g values obtained in the presence of FF are rather small (the only exception is the interleaved product code).

4.3 Eve's ideal performance and outage probability

In the analysis developed so far, we have made two important assumptions on Eve: (i) that she uses the same decoder as Bob and (ii) that we are interested only in her average error rate. The first of these hypotheses may appear weak from the security standpoint, since in PLS, it is usually assumed that Eve does not suffer from limitations in computing power; therefore, she should be able to use the best decoder available. Also, the second hypothesis may appear limiting, since even when performance over a fading channel is good in average terms, an outage event may occur due to oscillations in the channel quality. In this subsection, we remove these two assumptions and show that, despite this, the results of the comparative analysis among the considered code design techniques do not change. Therefore, they can be considered of general validity for the channel setting that is here of interest.

For any code of given length and rate, the best performance achievable under maximum likelihood (ML) decoding in terms of FER is lower bounded by the well-known sphere packing bound (SPB) [34], which is particularly tight to the ML decoder performance in the region of high error rates. Therefore, we can use the SPB to provide a conservative estimate of the performance that Eve can achieve by using ML decoding over a code with given length and rate. A similar approach can also be followed for Bob by considering the well-known union bound, which provides an upper bound on performance under ML decoding, and is usually tight in the regime of low error rates. However, in order to compute the union bound (and its dominant term, in

Table 4 Security gap with systematic transmission over the FF channel with AWGN

Code	$\gamma_E\vert_{th}$ [dB]	$\gamma_B\vert_{th}$ [dB]	S_g [dB]
Int. product	−12.0	13.1	25.1
PDC-LDPC	−12.0	9.8	21.8
M-SC-MPC	−12.0	9.4	21.4
QC-LDPC	−12.0	9.8	21.8
PEG	−12.0	9.8	21.8

Table 5 Security gap with perfect scrambling and L = 1 over the FF channel with AWGN

Code	$\gamma_E\vert_{th}$ [dB]	$\gamma_B\vert_{th}$ [dB]	S_g [dB]
Int. product	7.7	19.7	12.0
PDC-LDPC	6.9	12	5.1
M-SC-MPC	6.6	9.8	3.2
QC-LDPC	7.1	10.2	3.1
PEG	7.0	10.2	3.2

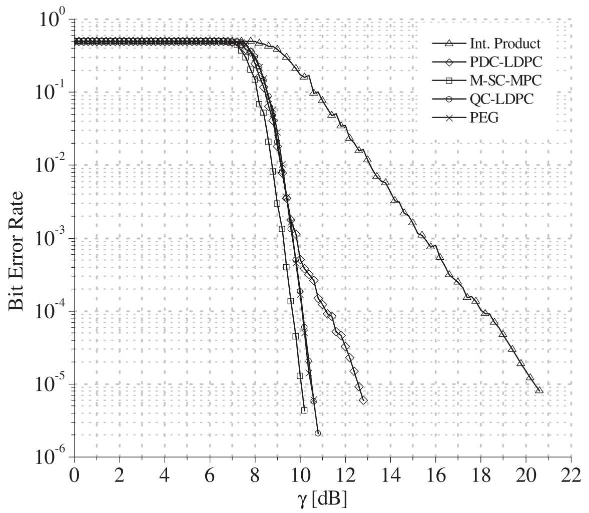


Fig. 11 BER performance with perfect scrambling and $L = 3$ for codes with $n = 1024$ and code rate $R = 3/4$ over the FF channel with AWGN

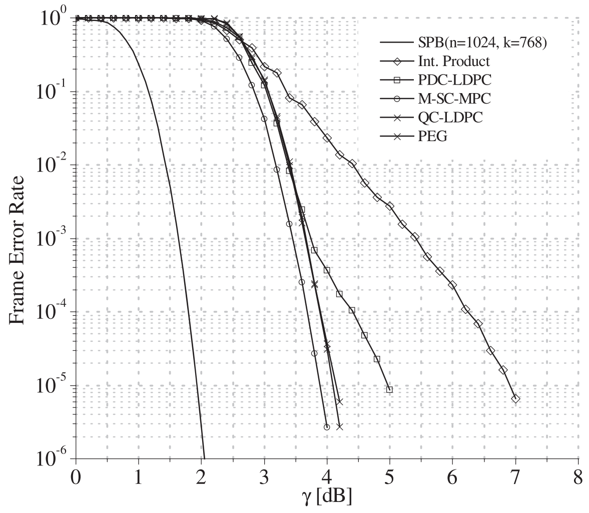


Fig. 12 FER performance with systematic transmission for codes with $n = 1024$ and code rate $R = 3/4$ over the flat AWGN channel and comparison with Shannon's sphere packing bound

particular, which is known as the error floor term), we need the knowledge of the weight spectrum of the code (or, at least, of its minimum distance and the corresponding multiplicity). This is usually unknown for the codes here considered. Moreover, Bob's performance does not affect the security requirements; therefore, we focus on Eve only.

For the case of a flat AWGN channel, the performance estimated through the SPB is reported in Fig. 12, where it is compared with the FER achieved by using the LLR-SPA decoder over the considered codes. If we fix again $P_b^{\mathrm{E}}|_{\mathrm{th}} = 0.4$ and consider perfect scrambling, we obtain that Eve must have an SNR per bit $\leq \gamma_{\mathrm{E}}|_{th}^{\mathrm{SPB}} = 0.55$ dB in order to achieve the security target when she is provided with an ideal decoder. The corresponding security gap values are reported in Table 7. By comparing them with those provided in Table 2, we observe that, by using the ideal decoder, Eve achieves a gain slightly smaller than 2 dB over classical LDPC decoding. This produces an increase in the security gap of the same order. However, the results of the comparative analysis among the several codes are basically unchanged. In fact, the two code constructions which achieve the best performance in terms of security gap are still the PEG and M-SC-MPC designs, while the others are in the same relative positions. The only minor difference is that the PEG code slightly outperformed the M-SC-MPC code for the case of classical LDPC decoding, while the opposite occurs when Eve uses the ideal decoder.

In order to assess performance over the FF channel, we also take into account the probability of occurrence of an outage event concerning the security target. For this purpose, as a further metric, we consider the secrecy outage probability, defined as the probability ξ that Eve's bit error rate falls below $P_b^{\mathrm{E}}|_{\mathrm{th}}$. In order to estimate such a probability, we consider perfect scrambling and follow the approach proposed in [35] for the case of coding across sub-messages. According to such an approach, also followed in [36], ξ can be expressed as

$$\xi = 1 - \left[1 - \exp\left(-\frac{\gamma_{\mathrm{E}}|_{\mathrm{th}}^{\mathrm{AWGN}}}{\gamma_{\mathrm{E}}|_{\mathrm{th}}^{\mathrm{FF}}}\right)\right]^n, \tag{7}$$

Table 6 Security gap with perfect scrambling and $L = 3$ over the FF channel with AWGN

Code	$\gamma_{\mathrm{E}}\vert_{\mathrm{th}}$ [dB]	$\gamma_{\mathrm{B}}\vert_{\mathrm{th}}$ [dB]	S_g [dB]
Int. product	8.9	20.5	11.6
PDC-LDPC	7.6	12.4	4.8
M-SC-MPC	7.3	10	2.7
QC-LDPC	7.7	10.4	2.7
PEG	7.7	10.4	2.7

Table 7 Security gap with perfect scrambling and Eve's ideal decoder over the flat AWGN channel

Code	$\gamma_{\mathrm{E}}\vert_{\mathrm{th}}^{\mathrm{SPB}}$ [dB]	$\gamma_{\mathrm{B}}\vert_{\mathrm{th}}$ [dB]	S_g [dB]
Int. product	0.55	6.74	6.19
PDC-LDPC	0.55	4.83	4.28
M-SC-MPC	0.55	3.80	3.25
QC-LDPC	0.55	4.10	3.55
PEG	0.55	4.04	3.49

where $\gamma_E|_{th}^{AWGN}$ and $\gamma_E|_{th}^{FF}$ are the two threshold values of Eve's average SNR corresponding to the flat AWGN and FF channels, respectively. Starting from (7), we obtain

$$\gamma_E|_{th}^{FF} = -\frac{\gamma_E|_{th}^{AWGN}}{\ln\left[1-\sqrt[n]{1-\xi}\right]}, \tag{8}$$

which allows to compute the threshold value of Eve's average SNR over the FF channel by taking into account possible outage events and fixing the secrecy outage probability ξ.

In order to provide an example, we consider that Eve still uses the ideal decoder, that is, $\gamma_E|_{th}^{AWGN} = \gamma_E|_{th}^{SPB} = 0.55$ dB. By using (8) and considering a secrecy outage probability $\xi = 10^{-3}$, we obtain that over the FF channel, the threshold value for Eve's average SNR per bit becomes $\gamma_E|_{th} = \gamma_E|_{th}^{FF} = -10.86$ dB. The corresponding security gap values are reported in Table 8, by considering the same average values for Bob's SNR per bit used in Table 5, and $L = 1$. We observe that, in comparison with the results in Table 5, the security gap values are significantly increased, but the relative behavior of the considered codes is basically unchanged. The conclusion would be similar by imposing a constraint also on the transmission outage probability, i.e., the probability that Bob's error rate overcomes the threshold $P_b^B|_{th}$. This confirms that the results of the comparative analysis developed in the previous sections have a general meaning, despite that the use of practical LDPC decoders is assumed also for Eve and the probability of occurrence of outage events is not taken into account.

4.4 General remarks

Looking at the results presented in Sections 4.1 and 4.2, we see that the relative behavior of the considered LDPC schemes remains basically unchanged through the various operation conditions. In essence, the performance, in terms of S_g of the M-SC-MPC, the QC-LDPC, and the PEG constructions are very similar; so, they can be considered substantially equivalent. The M-SC-MPC solution, however, has the advantage to require the smallest SNR.

On the contrary, the other two constructions exhibit some penalty. This is always true for the interleaved product code that suffers from the impact of the lower parity-check matrix column weight imposed by the constraints due to the product code structure. The PDC-LDPC code, in turn, exhibits an error floor that, at the reliability target of 10^{-5}, has no effect for the case of flat AWGN channel without scrambling (see Fig. 6), while produces a loss in all the other, more significant, cases.

In conclusion, the relative behavior of the considered classes of codes basically depends on their inherent properties and is substantially the same for any considered scenario. On the contrary, the required values of SNR and the security gaps are scenario-dependent. So, though demonstrated for a specific choice of n and R, the conclusions drawn appear rather general and can be extended to other values of code length and rate.

Table 8 Security gap with perfect scrambling and $L = 1$ over the FF channel with Eve's ideal decoder and secrecy outage probability $\xi = 10^{-3}$

Code	$\gamma_E\|_{th}$ [dB]	$\gamma_B\|_{th}$ [dB]	S_g [dB]
Int. product	−10.86	19.7	30.56
PDC-LDPC	−10.86	12	22.86
M-SC-MPC	−10.86	9.8	20.66
QC-LDPC	−10.86	10.2	21.06
PEG	−10.86	10.2	21.06

5 Conclusions

We have assessed the performance achievable by some LDPC code design techniques in terms of the security gap over the AWGN and the fast Rayleigh fading wire-tap channels. We have considered both systematic and scrambled transmissions and frame concatenation before scrambling. Assuming the PEG code design algorithm as a reference, we have compared its performance with that of four techniques for designing structured LDPC codes. Our results show that M-SC-MPC codes and QC-LDPC codes generally exhibit performance comparable and sometimes even better than that resulting from the application of the PEG algorithm. Hence, we can conclude that M-SC-MPC and QC-LDPC codes represent valid alternatives to PEG codes for the use in this framework, as they allow to take advantage of the structured nature of their characteristic matrices, while achieving very good performance from the PLS standpoint. On the contrary, the solution exploiting interleaved product codes, though being characterized by low complexity, is generally inefficient from the security gap standpoint.

The analysis developed in this paper is a first step towards the choice of good code design techniques for supporting joint security and reliability of transmissions.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

This work was supported in part by the MIUR project ESCAPADE (Grant RBFR105NLC) under the "FIRB–Futuro in Ricerca 2010" funding program.

Received: 12 May 2015 Accepted: 12 October 2015
Published online: 21 October 2015

References

1. AD Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
2. S Leung-Yan-Cheong, M Hellman, The Gaussian wire-tap channel. IEEE Trans. Inform. Theory. **24**(4), 451–456 (1978)

3. D Klinc, J Ha, SW McLaughlin, J Barros, B-J Kwak, *Proc. IEEE Information Theory Workshop (ITW 2009)*. LDPC codes for the Gaussian wiretap channel, (Taormina, Italy, 2009), pp. 95–99
4. A Thangaraj, S Dihidar, AR Calderbank, SW McLaughlin, J-M Merolla, Applications of LDPC codes to the wiretap channel. IEEE Trans. Inform. Theory. **53**(8), 2933–2945 (2007)
5. Y Liang, HV Poor, S Shamai (Shitz), LDPC block and convolutional codes based on circulant matrices. IEEE Trans. Inform. Theory. **54**(6), 2470–2492 (2008)
6. CW Wong, TF Wong, JM Shea, Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel. IEEE Trans. Inf. Forensics Secur. **6**(3), 551–564 (2011)
7. M Baldi, G Ricciutelli, N Maturo, F Chiaraluce, *Proc. IEEE International Conference on Communications (ICC, 2015) - Workshop on Wireless Physical Layer Security*. Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel, (London, UK, 2015), pp. 446–451
8. J Lu, J Harshan, F Oggier, in *Proc. IEEE Information Theory Workshop (ITW 2014)*. A USRP implementation of wiretap lattice codes (Hobart, Tasmania, 2014), pp. 316–320
9. TJ Richardson, RL Urbanke, The capacity of low-density parity-check codes under message-passing decoding. IEEE Trans. Inform. Theory. **47**(2), 599–618 (2001)
10. D Klinc, J Ha, SW McLaughlin, J Barros, B-J Kwak, *Proc. IEEE Global Telecommunications Conference (GLOBECOM, 2009)*. LDPC codes for physical layer security, (Honolulu, HI, 2009), pp. 1–6
11. D Klinc, J Ha, SW McLaughlin, J Barros, B-J Kwak, LDPC codes for the Gaussian wiretap channel. IEEE Trans. Inf. Forensics Secur. **6**(3), 532–540 (2011)
12. M Baldi, M Bianchi, F Chiaraluce, *Proc. IEEE Information Theory Workshop (ITW 2010)*. Non-systematic codes for physical layer security, (Dublin, Ireland, 2010)
13. M Baldi, M Bianchi, F Chiaraluce, *Proc. IEEE International Conference on Communications (ICC, 2011) - Workshop on Physical Layer Security*. Increasing physical layer security through scrambled codes and ARQ, (Kyoto, Japan, 2011)
14. M Baldi, M Bianchi, F Chiaraluce, Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: a security gap analysis. IEEE Trans. Inf. Forensics Secur. **7**(3), 883–894 (2012)
15. M Baldi, M Bianchi, N Maturo, F Chiaraluce, A physical layer secured key distribution technique for IEEE 802.11g wireless networks. IEEE Wireless Commun. Lett. **2**(2), 183–186 (2013)
16. M Baldi, M Bianchi, N Maturo, F Chiaraluce, *Proc. 9th International Wireless Communications and Mobile Computing Conference (IWCMC 2013)*. A tight estimation of the security gap over the fast fading wiretap channel, (Cagliari, Italy, 2013), pp. 143–148
17. M Baldi, N Maturo, G Ricciutelli, F Chiaraluce, *Proc. 21st International Conference on Telecommunications (ICT 2014)*. LDPC coded transmissions over the Gaussian broadcast channel with confidential messages, (Lisbon, Portugal, 2014)
18. M Baldi, N Maturo, G Ricciutelli, F Chiaraluce, *Proc. IEEE International Conference on Communications (ICC 2014) – Workshop on Wireless Physical Layer Security*. Practical LDPC coded modulation schemes for the fading broadcast channel with confidential messages, (Sydney, Australia, 2014), pp. 759–764
19. N Maturo, M Baldi, M Bianchi, F Chiaraluce, *Proc. International Conference on Telecommunications and Signal Processing (TSP 2013)*. Security gap performance of some LDPC code constructions, (Rome, Italy, 2013), pp. 77–81
20. XY Hu, E Eleftheriou, *Proc. IEEE Global Telecommunications Conference (GLOBECOM'01)*. Progressive edge-growth Tanner graphs, (San Antonio, Texas, 2001), pp. 995–1001
21. M Baldi, M Bianchi, G Cancellieri, F Chiaraluce, T Kløve, *Proc. International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2012)*. On the generator matrix of array LDPC codes, (Split, Croatia, 2012)
22. M Baldi, F Bambozzi, F Chiaraluce, On a family of circulant matrices for quasi-cyclic low-density generator matrix codes. IEEE Trans. Inform. Theory. **57**(9), 6052–6067 (2011)
23. SJ Johnson, SR Weller, A family of irregular LDPC codes with low encoding complexity. IEEE Commun. Lett. **7**(2), 79–81 (2003)
24. M Baldi, G Cancellieri, A Carassai, F Chiaraluce, LDPC codes based on serially concatenated multiple parity-check codes. IEEE Commun. Lett. **13**(2), 142–144 (2009)
25. JSK Tee, DP Taylor, PA Martin, Multiple serial and parallel concatenated single parity-check codes. IEEE Trans. Commun. **51**(10), 1666–1675 (2003)
26. M Baldi, G Cancellieri, F Chiaraluce, *Proc. International Conference on Advances in Satellite and Space Communications (SPACOMM 2009)*. A class of low-density parity-check product codes, (Colmar, France, 2009), pp. 107–112
27. Z Qi, NC Sum, *Proc. International Conference on Communications Systems (ICCS, 2004)*. LDPC product codes, (Krakow, Poland, 2004), pp. 481–483
28. M Baldi, G Cancellieri, F Chiaraluce, Interleaved product LDPC codes. IEEE Trans. Commun. **60**(4), 895–901 (2012)
29. O Gazi, AO Yilmaz, Turbo product codes based on convolutional codes. ETRI J. **28**(4), 453–460 (2006)
30. RM Tanner, D Sridhara, A Sridharan, TE Fuja, DJ Costello, LDPC block and convolutional codes based on circulant matrices. IEEE Trans. Inform. Theory. **50**(12), 2966–2984 (2004)
31. M Baldi, M Bianchi, G Cancellieri, F Chiaraluce, Progressive differences convolutional low-density parity-check codes. IEEE Commun. Lett. **16**(11), 1848–1851 (2012)
32. M Baldi, F Chiaraluce, *Proc. IEEE International Symposium on Information Theory (ISIT 2007)*. Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes, (Nice, France, 2007), pp. 2591–2595
33. M Baldi, G Cancellieri, F Chiaraluce, Finite-precision analysis of demappers and decoders for LDPC-coded M-QAM systems. IEEE Trans. Broadcast. **55**(2), 239–250 (2009)
34. CE Shannon, Probability of error for optimal codes in a Gaussian channel. Bell Syst. Tech. J. **38**(3), 611–656 (1959)
35. M Baldi, F Chiaraluce, N Laurenti, S Tomasin, F Renna, Secrecy transmission on parallel channels: theoretical limits and performance of practical codes. IEEE Trans. Inf. Forensics Secur. **11**(9), 1765–1779 (2014)
36. M Baldi, M Bianchi, N Maturo, F Chiaraluce, *Proc. IEEE Symposium on Computers and Communications (ISCC, 2013)*. A practical viewpoint on the performance of LDPC codes over the fast Rayleigh fading wire-tap channel, (Split, Croatia, 2013)