Diversity-Security Tradeoff for Compound Channels

Volkan Dedeoglu and Joseph J. Boutros
Texas A&M University, Electrical Engineering Dept.
23874 Doha, Qatar
Email:volkan.dedeoglu@tamu.edu, boutros@tamu.edu

***Abstract*—We propose new rate-flexible low-density parity-check (LDPC) coding schemes for secrecy over a compound channel with L parallel links. These codes, called *anti-root LDPC* codes, have good performance at both finite and asymptotic code length while all links are jointly encoded. Firstly, an algebraic security scheme is developed based on the anti-root LDPC ensemble and a source splitter. Secondly, an information theoretic security scheme is built from the same splitter with the adjunction of a random sequence. Then, we present a new diversity-security tradeoff for channels exhibiting block fading or block erasure. Finally, we describe anti-root LDPC ensembles with higher diversity or security orders to attain the aforementioned tradeoff.**

I. Introduction and Notations

The design of error-control codes was mainly dedicated in the past to source and channel coding [1][2][3] for single-user and multi-user systems. The era of physical-layer security brought the challenge of constructing new error-control codes that ensure secrecy while maintaining quality of service [4].

In [5], we introduced the anti-diversity concept for secure communications over compound channels. The idea of the anti-diversity concept is based on the fact that it is impossible to have perfect secrecy when the communication system has full diversity. Thus, by intentionally violating the conditions for full diversity, we assure that the system is diversity deficient. Then, we constructed anti-root LDPC coding schemes for both perfect algebraic and information theoretic security.

The coding scheme in [5] was designed for coding rates $R \geq 1/2$. Thus, in this paper we propose a new anti-root LDPC code ensemble that is rate-flexible, which allows for coding rates $0 < R < 1$. We show that the proposed anti-root LDPC ensemble has a good finite-length performance and good decoding thresholds at asymptotic length.

An important contribution of the paper is the study of diversity-security tradeoff, which has not been investigated in secure communications literature before. In [6], a new family of full-diversity LDPC codes was introduced. As full-diversity should be avoided for secure communications, we developed a new family of LDPC codes that achieves a diversity order allowed by the diversity-security tradeoff of the system by joint coding among the communication links.

The communication channels that we consider in this paper have L links. However, for simplicity of explanation, we start deriving the results for 2 links and then generalize the results for L links. Figure 1 depicts a compound communication system with two identical links defined by their transition probabilities $p_{Y|X}(y_1|v)$ and $p_{Y|X}(y_2|w)$. The links of the compound channel are any binary memoryless symmetric (BMS) channels with inputs $v, w \in \mathbb{F}_2^{N/2}$ and outputs $y_1, y_2 \in \mathcal{Y}^{N/2}$ for the output alphabet $\mathcal{Y}$. We assume that the source produces K uniform bits. Then, a rate-K/N binary encoder generates a length-N codeword, which is split into v and w of length $N/2$ to be transmitted on the parallel links. In the rest of the paper, for simplifying the notations, a unique letter is used to denote a random variable and any given value taken by that random variable depending on the context.

We assume the worst case scenario, where Eve has direct access to one of the two links without any noise, i.e. $z = v$ or $z = w$, where $z \in \mathbb{F}_2^{N/2}$ is the output of the channel between Alice and Eve. The aim of our work is two-folded: providing excellent performance for the legitimate listener Bob, and guaranteeing security against the eavesdropper Eve. For the source message $M = (a_1, a_2, \ldots, a_K) \in \mathbb{F}_2^K$, two types of security are considered:

- **Algebraic security**. Eve must not be able to solve any individual bit a_i, $\forall i = 1 \ldots K$. It is equivalent to absence of meaningful information, $I(a_i; z) = 0$ as in [7]. We guarantee algebraic security by the means of a non-stochastic LDPC encoder and a weight-2 splitter in Section II-A.
- **Information theoretic security**. Eve must not be able to determine any information derived from the source bits. Hence, the coding scheme must guarantee a zero information leakage, i.e. $I(M; z) = 0$ or equivalently $H(M|z) = H(M)$. We guarantee perfect secrecy by the means of a stochastic encoder in Section II-B.

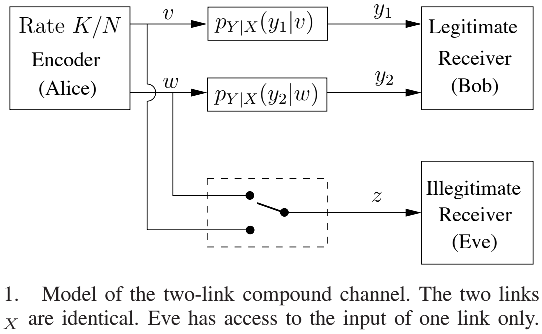

Figure 1. Model of the two-link compound channel. The two links defined by $p_{Y|X}$ are identical. Eve has access to the input of one link only.

The work of Joseph J. Boutros and Volkan Dedeoglu was supported by QNRF, a member of Qatar Foundation, NPRP project 5-603-2-243 at Texas A&M University.

The organization of the paper is as follows. First, a rate-flexible and finite-length-efficient LDPC ensemble and a splitter is proposed for algebraic and information theoretic security. The Bit Error Rate (BER) and Word Error Rate (WER) performances of the anti-root LDPC ensemble is given for different coding rates. Then, the density evolution (DE) equations are derived for the proposed anti-root LDPC ensemble and the belief propagation thresholds on the binary erasure channel are found for various coding rates. In Section IV, the diversity-security tradeoff and the upper bound for the coding rate is studied for block-fading links. Finally, the (s, d, L)-root LDPC ensemble is proposed for achieving the diversity-security tradeoff.

II. Anti-root LDPC for security

In [5], we constructed an anti-root LDPC code ensemble for secure communications over compound channels. In this section, a new rate-flexible anti-root LDPC code ensemble with good finite-length performance will be introduced. The anti-root LDPC code design is based on the anti-diversity concept, which refers to the code design principle where the fundamental diversity rules are violated intentionally to avoid full diversity. Further details can be found in [5].

A. Algebraic security

The algebraic security of our new code construction is proved based on the following lemmas.

Lemma 1: Let $x, y \in \mathbb{F}_2^n$ with Hamming weights $w_H(x)$, and $w_H(y)$ respectively. Assume that x and y have the same parity. Then, $w_H(x+y)$ is always even.

Proof. Let l be the number of indices where both x and y take the value of 1. Then, $w_H(x+y) = w_H(x) + w_H(y) - 2l$, which is always an even number when x and y have the same parity. □.

Lemma 2: Let $\{x_1, x_2, ..., x_L\}$ be L vectors in $\mathbb{F}_2^n$. Assume that the Hamming weights $w_H(x_i)$ is even, $\forall i$. Then, $w_H(\sum_{i=1}^{L} x_i)$ is always even.

Proof. Apply Lemma 1 $(L-1)$ times. □.

Lemma 3: Assume that the Hamming weights $w_H(x_i)$ is odd, $\forall i$. Then,$\forall L$ even, $w_H(\sum_{i=1}^{L} x_i)$ is even.

Proof. Apply Lemma 1 $(L/2)$ times. Then, apply Lemma 2 once. □.

Lemma 3 is not directly used in the rest of the code designs. However, the lemma gives us an important idea about the use of odd-weight rows in parity check matrices of the LDPC codes. To get an even-weight row as a combination of odd-weight rows, one needs an even number of rows, which is an impractical constraint on the design of codes for security.

Here, we briefly explain the general structure of the anti-root LDPC ensemble whose parity check matrix for two parallel links is shown in Figure 2. Let $\frac{K}{N}$ be the design rate (R is the effective rate), then $\frac{K}{N} \leq R < 1$. The N binary digits of a codeword are divided into four families. A family of $K/2$ information digits $1i$ and a family of $(N-K)/2$ parity digits $1p$ to be sent on the first link. Similarly, the two families $2i$ and $2p$ are to be sent on the second link. The submatrices A_1 and A_2 of size $(N-K) \times K/2$ correspond to the edges connecting bit nodes $1i$ and $2i$ to the check nodes, respectively. Whereas, the submatrix B of size $(N-K) \times (N-K)$ corresponds to the edges connecting the parity nodes $1p$ and $2p$ to the check nodes. To satisfy the rate constraint, we allocate the bit node and check node degrees as follows. The average check node degrees under A_1 and A_2 are d_i. Then, the bit node degrees under A_1 and A_2 are $2d_i(1/R-1)$. The bit node and check node degrees under B is d_p.

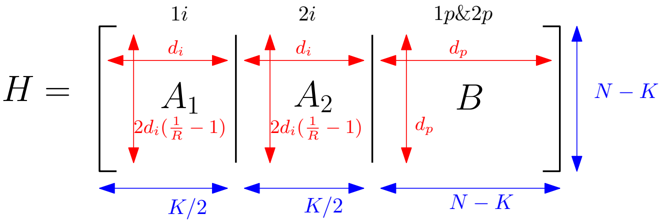

Figure 2. The general structure of the parity check matrix for the anti-root LDPC code ensemble.

As in [5], a source splitter is needed due to the systematic structure of the code ensemble. For security, we should not let Eve observe the information bits directly [8]. Therefore, a non-singular, and sparse source splitter S of size $K \times K$ is placed between the source and the LDPC encoder, such that $M = uS$, where $u = (u_1, u_2, \ldots, u_K) \in \mathbb{F}_2^K$ is the LDPC encoder input. When S is regular with degree d_s, i.e. the Hamming weight of all rows and columns is d_s, each source digit is split into d_s digits [9][10]. In this work, we consider a quasi-regular weight-2 non-singular splitter S with degree $d_s = 2$, except for one row and one column with degree 1.

Lemma 4: Any quasi-regular weight-2 non-singular splitter S can be decomposed as

$$S = \Pi \cdot S_0 \cdot \Pi^{'}, \qquad (1)$$

where S_0 is a double diagonal splitter, Π and $\Pi^{'}$ are $K \times K$ permutation matrices.

For simplicity, we assume that $S = S_0$. Then, each source bit a_i is split into two bits as follows

$$a_i = u_i + u_{i+1}, \qquad (2)$$

for $i = 1 \ldots K-1$ and $a_K = u_K$. We force the last source bit to be uniformly random, $a_K = Bern(1/2)$, and reduce the exact message entropy to $H(M) = K-1$ bits. As shown in Figure 3, the splitter outputs the K-bit sequence $u = (1i \ \& \ 2i)$, which is divided into two parts to be sent to the LDPC encoder such that the $K/2$ bits at odd positions go to $1i$ and the $K/2$ bits at even positions go to $2i$. In order to decode the source message M, Eve needs to know both bit families $1i$ and $2i$. When Eve observes $z = v$, all bits $1i$ are known, but all bits $2i$ are missing. The special structure of the anti-root LDPC code given in Figure 2 does not allow Eve to find any of the missing bits $2i$. Similarly, when Eve observes $z = w$, she cannot find the missing bits $1i$.

Theorem 5: When all rows of the submatrices A_1 and A_2 have even parity with $d_i > 0$ and $d_p \geq 2$, the anti-root code

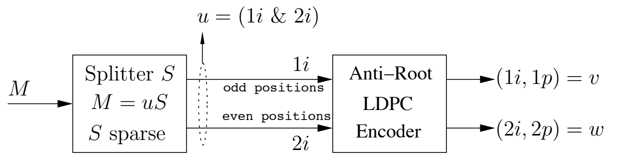

Figure 3. The non-stochastic encoder converts the source message M into half codewords v and w to be sent on each link. $M \in \mathbb{F}_2^K$, $v, w \in \mathbb{F}_2^{N/2}$.

ensemble is algebraically secure.

Proof. Note that, to solve an information bit from $1i$, a combination of rows in A_1 should produce a weight 1 sequence. As stated by Lemma 2, the sum of rows with even parities would always produce a sequence with an even parity. Thus, when all rows of the A_1 matrix have an even parity, none of the information bits in $1i$ can be solved. Similarly, all rows of the A_2 matrix should have even parity by symmetry. However, the submatrix B may have even or odd parity rows as the parity bits do not need to be protected for algebraic security. □.

The algebraic security of the anti-root code ensemble can be generalized to L-links in a straightforward manner by introducing the information nodes $(1i, 2i, ..., Li)$ with the corresponding parity nodes $(1p, 2p, ..., Lp)$ and the submatrices $(A_1, A_2, ..., A_L, B)$ with appropriate sizes when Eve is observing only one of the L links.

B. Information Theoretic Security

As shown in the previous section, the algebraic security is realized by using a non-stochastic encoder. In this section, we show that the information theoretic security can be realized by replacing the non-stochastic encoder with a stochastic encoder. Hence, this section introduces the stochastic encoder structure for perfect secrecy.

For the algebraic security, the conditional entropy of the message is given by

$$H(M|z = v) = H(1i|z = v) + H(2i|z = v, 1i) = H(2i|v).$$

where the message entropy is $H(M) = K$ (we omit $a_K = Bern(1/2)$ for simplification).

Note that, the information leakage $H(2i|v)$ depends on the particular construction of the parity check matrix H and unknown. However, the conditional entropy is always bounded as $0 < H(2i|v) \leq K/2$. Similarly, for $z = w$, $0 < H(1i|w) \leq K/2$. Then, due to the information leakage caused by the non-stochastic encoding scheme, the conditional entropy of the message satisfies

$$H(M|z) \leq \frac{K}{2} < K = H(M). \tag{3}$$

In summary, although the non-stochastic encoding scheme achieves algebraic security, it does not guarantee information-theoretic security.

Next we introduce our stochastic scheme, which guarantees perfect secrecy in the information theoretic sense. In order to achieve perfect secrecy, the stochastic encoding scheme sacrifices $K/2$ bits in the message, i.e. $H(M) = K/2$. We show that the conditional entropy satisfies $H(M|z) = H(M) = K/2$ using the proposed stochastic encoder.

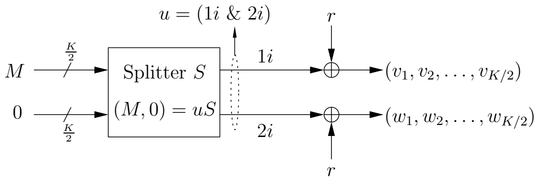

Figure 4. The $K \times K$ splitter in the stochastic scheme reads a message M of $K/2$ bits and a zero sequence of $K/2$ bits. A random sequence of $K/2$ bits is applied at the splitter output before channel transmission.

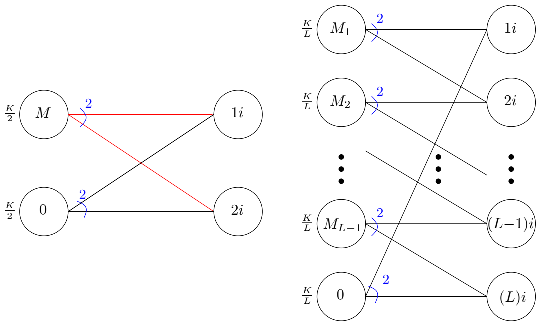

Figure 5. Splitter structures for stochastic encoding for two links (left) and L links (right). The graphs have a 2-regular degree on the left (S is sparse) and a high degree on the right (S^{-1} is dense).

The encoding scheme is modified as shown in Figure 4. The $K/2$ bits of the splitter input comes from the message $M = (a_1, a_2, \ldots, a_{K/2})$ and the rest of the input bits are filled with a zero sequence of length $K/2$. Furthermore, a random sequence $r = (r_1, r_2, \ldots, r_{K/2})$ of $K/2$ independent uniform bits is added to the splitter outputs. Hence, the $K/2$ bits of the codewords v and w are filled by the splitter outputs. The parity bits of an LDPC encoder fill the remaining $N - K$ bits in both codewords v and w. The analysis is valid for joint encoding by a two-link anti-root LDPC, as well as for two separate length-$N/2$ LDPC codes. The splitter structures for two links and its extension to L links are illustrated in Figure 5. In a straightforward manner, the following Theorem 6 can be generalized to an eavesdropper reading one link out of L links, for any $L \geq 2$.

Theorem 6: The stochastic coding scheme achieves $H(M|z) = \frac{K}{2} = H(M)$ on a two-link compound channel, i.e. it guarantees perfect security in the information-theoretic sense.

Notice that the coding scheme uses the same splitter structure as in [5] but a different LDPC code ensemble. Thus, the proof is similar to the proof of the Theorem 4 in [5].

III. The Performance for the Legitimate User

In this section, the performance of the anti-root LDPC code ensemble will be studied. First, the finite-length performance will be examined by comparing the bit and word error rates of the anti-root LDPC ensemble with a fully random LDPC code for various coding rates. Then, the asymptotic performance of the anti-root LDPC ensemble will be analyzed over a binary

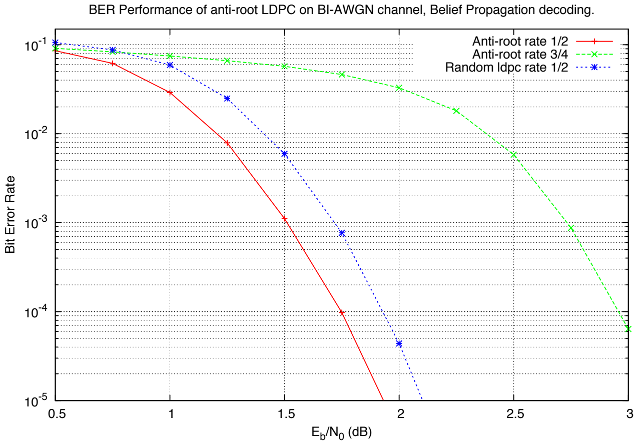

Figure 6. The bit error rate performance of the anti-root LDPC code on BI-AWGN channel under belief propagation decoding.

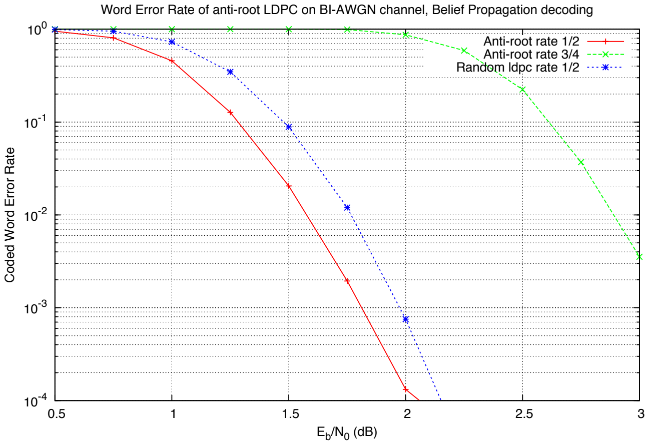

Figure 7. The coded word error rate performance of the anti-root LDPC code on BI-AWGN channel under belief propagation decoding.

erasure channel by comparing the density evolution thresholds with the fully random LDPC ensemble for various rates.

A. BER and WER Performance of the Anti-root LDPC

In this section, the BER and the WER performance of the anti-root LDPC code ensemble on BI-AWGN channels under belief propagation decoding is compared with the performance of the fully random LDPC ensemble for a finite block length of $N = 2000$. The performance of the proposed code ensembles depends on the construction of the parity check matrix given in Figure 2. The Monte Carlo simulations are presented for rates $R = 1/2$ with $d_i = 2$ and $d_p = 2$ and $R = 3/4$ with $d_i = 9/2$ and $d_p = 3$ in Figure 6 and Figure 7.

The proposed code constructions are almost regular. Thus, the performance of the proposed code constructions is compared with fully random regular LDPC codes. The aim is to check if the proposed anti-diversity codes perform similar to fully random LDPC codes. The results in Figure 6 and Figure 7 show that our constructions perform slightly better than a rate $1/2$ regular $(3, 6)$ LDPC code. In terms of BER and WER, the anti-root LDPC code ensembles show good performance such that for the rate $1/2$ anti-root code, the BER is less than 10^-5 and WER is less than 10^-4 on information bits at 2 dB. The BER performance of the rate $3/4$ anti-root code is 1.5 dB away from the Shannon limit similar to the performance of the rate $1/2$ anti-root code.

Note that the error rate is calculated over the information bits as Bob is interested in decoding the information bits only. Also, this performance simulation does not include the performance of the splitter. After applying the splitter, the error rate would be roughly multiplied by 2 for the source bits (refer to the splitter structure in (2)).

B. DE threshold on BEC

This section studies the DE equations [3] for the asymptotic performance of Bob under iterative decoding for sufficiently large codeword length. The performance of the legitimate user Bob depends on the construction of the anti-root LDPC ensemble, which is composed of the submatrices A_1, A_2, and B. The graph defined by the parity check matrix of the anti-root LDPC code in Figure 2 has multiple edge types. Since, we are only interested in the performance on the information bits, different polynomials are needed to be defined for the density evolution of the information and parity messages[6][11].

For algebraic security, the degree distributions of A_1 and A_2 from an edge perspective, at bit nodes and check nodes respectively, are defined as:

$$\lambda_I(x) = \lambda_k^I x^{k-1} + (1 - \lambda_k^I)x^k \tag{4}$$

and

$$\rho_I(x) = \rho_j^I x^{j-1} + (1 - \rho_j^I)x^{j+1} \tag{5}$$

where

$$j \leq d_i < j + 2 \text{ , } j \text{ even}$$
$$k = \lfloor 2d_i(1/R - 1) \rfloor$$

and

$$\lambda_k^I = \frac{(k + 1 - (2d_i(1/R - 1)))k}{2d_i(1/R - 1)} \tag{6}$$

$$\rho_j^I = \frac{(j + 2 - d_i)j}{2d_i} \tag{7}$$

The degree distribution for the submatrix B at bit nodes and check nodes is given by

$$\lambda_P(x) = \rho_P(x) = \lambda_l^P x^{l-1} + (1 - \lambda_l^P)x^l \tag{8}$$

where

$$l = \lfloor d_p \rfloor \tag{9}$$

and

$$\lambda_l^P = \frac{(l + 1 - d_p)l}{d_p} \tag{10}$$

We introduce the node-perspective polynomials $\tilde{\rho_I}(x)$ and $\tilde{\rho_P}(x)$ as

$$\tilde{\rho_I}(x) = (\frac{j + 2 - d_i}{2})x^j + (\frac{d_i - j}{2})x^{j+2} \tag{11}$$

$$\tilde{\rho_P}(x) = (l + 1 - d_p)x^l + (d_p - l)x^{l+1} \tag{12}$$

The symmetric structure of the proposed anti-root LDPC code and the identical communication links result in two message densities to be used in DE equations:

- f is the probability density function of log-ratio messages from bit node $1i$ to check node c, and $2i$ to c.
- q is the probability density function of log-ratio messages from bit nodes $1p$ and $2p$ to check node c.

The evolution of the two message densities f^m and q^m can be found by the tree representations drawn if Figure 8 and Figure 9, respectively. After drawing the local neighborhood of each type of bit nodes, we find the following DE equations for BEC at decoding iteration $m+1$:

$$f^{m+1} = \epsilon\lambda_I\left(1-\rho_I\left(1-f^m\right)\tilde{\rho_I}\left(1-f^m\right)\tilde{\rho_P}\left(1-q^m\right)\right) \quad (13)$$

$$q^{m+1} = \epsilon\lambda_P\left(1-\tilde{\rho_I}\left(1-f^m\right)\tilde{\rho_I}\left(1-f^m\right)\rho_P\left(1-q^m\right)\right) \quad (14)$$

where ϵ is the erasure probability of the BEC. Note that, the DE equations for the Gaussian channel can be derived in a similar way.

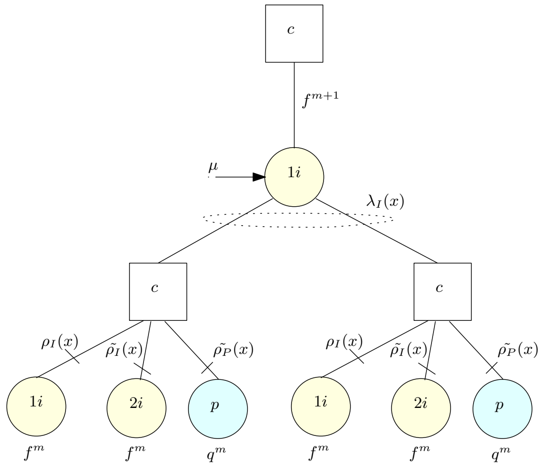

Figure 8. Tree representation of the local neighborhood of information bit node 1i showing the outgoing message f^m.

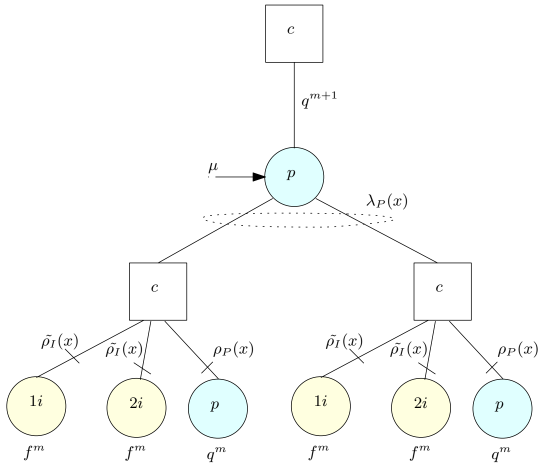

Figure 9. Tree representation of the local neighborhood of parity bit node p showing the outgoing message q^m.

The density evolution thresholds are compared in Table I.

Table I
BELIEF PROPAGATION THRESHOLDS ON THE BINARY ERASURE CHANNEL

Rate	(d_b, d_c)	Fully Random	Anti-Root	d_i	d_p
3/4	(3,12)	0.21047	0.21594	4	4
3/4	(3,12)	0.21047	0.21469	5	2
2/3	(3,9)	0.28283	0.28113	3	3
1/2	(3,6)	0.42944	0.44511	2	2
1/3	(4,6)	0.50613	0.56131	2	2
1/3	(4,6)	0.50613	0.58211	1.5	2
1/4	(3,4)	0.64742	0.66126	0.5	3
1/4	(3,4)	0.64742	0.66160	1	2

IV. Diversity-Security Tradeoff

In this section, we examine the maximal achievable diversity order d and the security order s when each link is undergoing a quasi-static fading. For a system with L links, the maximal achievable diversity order d, and the security order s, Eve is missing $L-s$ links. For security, the code should not recover more than $L-s-1$ links. To achieve secrecy, the number of missing links for Eve should satisfy:

$$L - s \geq d \quad (15)$$

Whereas, the code should recover $d-1$ missing links so that Bob can decode the secret message when the diversity order is d. Hence, we can state the diversity-security tradeoff as

$$d + s = L \quad (16)$$

Note that, the diversity-security tradeoff cannot be achieved by coding the L links separately. In the following sections, an (s,d,L)-root LDPC ensemble will be proposed based on the joint coding on L links.

The upper bound on the coding rate R should satisfy the block-fading Singleton bound, which is stated as

$$d \leq \lfloor L(1-R) \rfloor + 1 \quad (17)$$

When d and s are achieved, by using (16) and (17), the coding rate should not exceed

$$R \leq \frac{s+1}{L} \quad (18)$$

V. (s,d,L)-root LDPC Ensemble

When there are only two links $L=2$, and Eve is listening to one of the links $s=1$, the maximum achievable diversity order is $d=1$. This diversity-security tradeoff is achieved by the stochastic splitter structure and the anti-root LDPC code ensemble proposed in Section II. To achieve a higher diversity order with security constraint, more links are needed between Alice and Bob, i.e. $L>2$.

In this section, we present an (s,d,L)-root LDPC ensemble and splitter structures for $L=3$ links. When Eve cannot intercept any of the links, the security order is $s=0$. In this case, the maximal diversity order is $d=3$, and the coding rate should not exceed $R \leq \frac{1}{3}$.

When Eve can intercept one of the links, the security order is $s=1$. The anti-root LDPC code proposed in Section II achieves the diversity order $d=1$. However, by using the diversity-security tradeoff, the maximal diversity order is $d = 2$. Using the Singleton bound (17), the coding rate is upper bounded by $R \leq \frac{2}{3}$. Next, we propose an (1,2,3)-root LDPC ensemble that achieves the coding rate upper bound $R = \frac{2}{3}$.

The structure of the parity check matrix for the proposed (1,2,3)-root LDPC ensemble is shown in Figure 10, where Π represents the class of random permutation matrices, and 0 represents the zero matrix. The parity check matrix is also composed of random matrices of class B_i and B_p, and three random matrices with row weights w_2.

Theorem 7: When the row weights of the matrices of class B_i is even and w_2 is odd, the (1,2,3)-root LDPC ensemble constructed by the parity check matrix in by Figure 10 is algebraically secure for $s = 1$ and achieves the diversity order $d = 2$.

Proof. The proof is based on Lemma 2. Eve is listening to one link. The row weight of any row under two of the three remaining information bit families is even. By Lemma 2, any combination of the rows under two of the three information bit families is also even. Hence, Eve can not solve any information bits from the two remaining information bit families. Thus, algebraic security is guaranteed. Bob, who has access to two links, can solve the remaining information bits in the third link. Hence, the diversity order is $d = 2$. □.

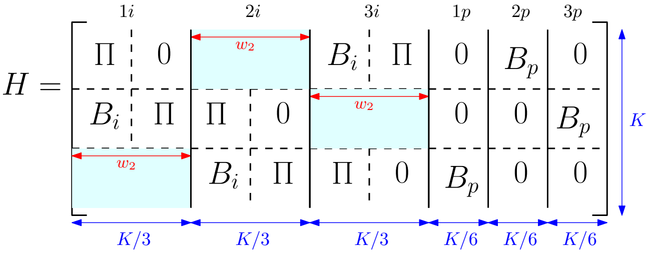

Figure 10. The structure of the parity check matrix for the $(s = 1, d = 2, L = 3)$-root LDPC ensemble.

The information theoretic security is guaranteed by using the source splitter in addition to a random sequence as discussed in Section II-B.

The diversity-security tradeoff tells us that it is possible to communicate securely even if Eve intercepts any two of the three links. In this case, the security order is $s = 2$, and the diversity is $d = 1$. To achieve the security order $s = 2$, we propose a new splitter structure in conjunction with some randomness. The new stochastic scheme will sacrifice $2K/3$ bits in the message by reducing the message entropy to $H(M) = K/3$ to achieve the security order of $s = 2$. The splitter input is modified to include $M = (a_1, a_2, \ldots, a_{K/3})$ and two zero sequences of length $K/3$. Let r_1 and r_2 be two random sequences of $K/3$ independent uniform binary digits. Then, the random sequences r_1, r_2, and $r_1 + r_2$ is added to three splitter outputs. The stochastic structure is shown in Figure 11 where the splitter output fills $K/3$ bits in v_1, v_2, and v_3. The remaining $N - K$ bits in v_1, v_2, and v_3 will be equal to parity bits of an anti-root LDPC encoder whose structure is given in Figure 2.

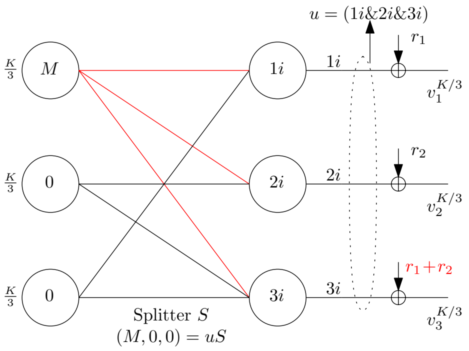

Figure 11. Splitter composition for stochastic encoding over three links for $s = 2$ and $d = 1$.

VI. Conclusions

We proposed a new anti-root LDPC ensemble that is rate-flexible and has a good finite-length performance for secure communications over compound channels. Algebraic security and information theoretic security are guaranteed for the proposed coding schemes. The finite length and asymptotic performance of the anti-root LDPC ensemble are compared with the fully random LDPC ensemble. The joint coding structure between links results in a longer code. Joint coding between the links also allows for a higher diversity order. In fact, there is no diversity without joint coding. We studied the diversity-security tradeoff over compound channels and constructed the (s, d, L)-root LDPC ensemble to achieve the diversity-security tradeoff.

References

[1] T.M. Cover and J.A. Thomas, *Elements of Information Theory*, Wiley, 2nd edition, 2006.

[2] R.E. Blahut, *Algebraic codes for data transmission*, Cambridge University Press, 2003.

[3] T.J. Richardson and R.L. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008.

[4] W.K. Harrison, J. Almeida, M.R. Bloch, S.W. McLaughlin, and J. Barros, "Coding for Secrecy: An Overview of Error-Control Coding Techniques for Physical-Layer Security," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 41-50, 2013.

[5] J. Boutros, V. Dedeoglu, and M. Bloch, "The Anti-Diversity Concept for Secure Communication on a Two-Link Compound Channel," *in Proc. International Zurich Seminar on Communications*, pp. 116-119, Feb. 2014.

[6] J.J. Boutros, A. Guillén i Fàbregas, E. Biglieri, and G. Zémor, "Low-Density Parity-Check Codes for Nonergodic Block-Fading Channels," *IEEE Trans. Inform. Theory*, vol. 56, no. 9, pp. 4286-4300, Sept. 2010.

[7] K. Bhattad and K.R. Narayanan, "Weakly secure network coding," *First Workshop on Network Coding, NetCod 2005*, vol. 104, April 2005.

[8] M. Baldi, M. Bianchi, and Franco Chiaraluce, "Non-Systematic Codes for Physical Layer Security," *in Proc. IEEE Information Theory Workshop (ITW 2010)*, pp. 1-5, Dublin, Ireland, Aug. 30 - Sept. 3, 2010.

[9] G. Shamir and J. Boutros, "Non-systematic low-density parity-check codes for nonuniform sources," *in Proc. International Symp. on Information Theory (ISIT 2005)*, Adelaide, Australia, pp. 18981902, Sept. 2005.

[10] A. Alloum, J. Boutros, G. Shamir, and L. Wang, "Non-systematic LDPC codes via scrambling and splitting," *in Proc. Allertons Conference on Comm. and Control*, Monticello, Illinois, pp. 1879-1888, Sept. 2005.

[11] J.J. Boutros, "Diversity and coding gain evolution in graph codes," *in Proc. Information Theory and Appl. (ITA'2009)*, pp. 34-43, UCSD, San Diego, Feb. 2009.