Two Edge Type LDPC Codes for the Wiretap Channel

Vishwambhar Rathi [*], Mattias Andersson[*], Ragnar Thobaben[*], Jörg Kliewer[†] and Mikael Skoglund[*]
[*]School of Electrical Engineering and the ACCESS Linnaeus Center,
Royal Institute of Technology (KTH),
Stockholm, Sweden
email: {vish, amattias, ragnar.thobaben, skoglund}@ee.kth.se
[†]Klipsch School of Electrical and Computer Engineering
New Mexico State University,
Las Cruces, NM 88003, USA
email: jkliewer@nmsu.edu

***Abstract*—We consider transmission over a wiretap channel where both the main channel and the wiretapper's channel are Binary Erasure Channels (BEC). We propose a code construction using two edge type LDPC codes based on the method of Thangaraj, Dihidar, Calderbank, McLaughlin and Merolla. The advantage of our construction is that we can easily calculate the threshold over the main channel. Using standard LDPC codes with a given threshold over the BEC we give a construction for a two edge type LDPC code with the same threshold. Since this construction gives a code for the main channel with threshold zero we also give numerical methods to find two edge type LDPC codes with non-zero threshold for the main channel.**

I. Introduction

Wyner introduced the notion of a wiretap channel in [1] whose non-degraded version is depicted in Figure 1. In general, the channel from Alice to Bob and the channel from Alice to Eve can be any discrete memoryless channels. In this paper we will restrict ourselves to the setting when both channels are Binary Erasure Channels (BEC). In a wiretap channel, Alice communicates a message W to Bob through the main channel denoted as C_m, by encoding W as an n bit vector $\underline{X}$, and transmitting $\underline{X}$ across C_m. Bob receives a noisy version of $\underline{X}$ which is denoted by $\underline{Y}$. In our setting C_m is a BEC with erasure probability ϵ_m. Eve observes $\underline{X}$ via the wiretapper's channel C_w and receives a noisy version of $\underline{X}$ denoted as $\underline{Z}$. In our setting, C_w is a BEC with erasure probability ϵ_w. The encoding of a message W by Alice should be such that Bob is able to decode W reliably and $\underline{Z}$ does not provide any information to Eve about W. More precisely, as in [2], the mutual information between W and Z goes to zero rate-wise as n goes to infinity. Assume that W is chosen from $\{1, \ldots, M\}$ with uniform probability. In [1] the codebook $\mathcal{C}$ used by Alice is partitioned into M subsets $\mathcal{C}_w$ of equal size, and to transmit message w Alice chooses a member of $\mathcal{C}_w$ uniformly at random. If $\mathcal{C}$ can be used to communicate reliably over the main channel Bob will be able to determine the subset $\mathcal{C}_w$ and thus the message W.

Previously in [2], [3] the authors have given code design methods based on sparse graph codes. The approach of [3] is based on nested codes [4]. It was shown in [2] that if the coarse code of the nested code is capacity achieving over BEC(ϵ_w) and the fine code has threshold greater than ϵ_m then perfectly secure and reliable communication is possible. However no construction method was given to find nested codes with these properties. In particular, no guarantee was given for the threshold over the main channel. In this paper, we give a code construction method based on two edge type LDPC codes. Our method has the advantage that its reliability performance on the main channel and secrecy performance on the wiretapper's channel can be easily computed. Our code construction is based on the code construction method of [2].

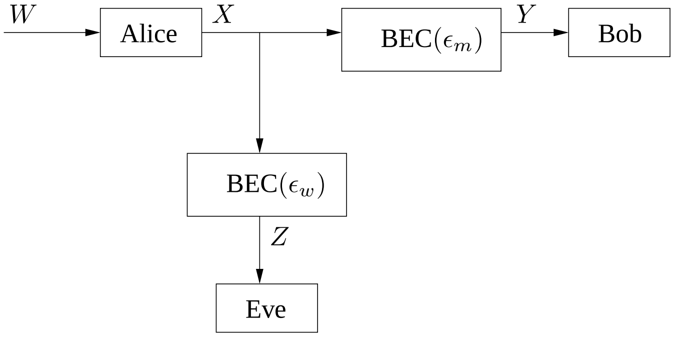

Fig. 1. Wiretap channel

II. Code Construction

We first describe the code construction method of [2]. Let H be an $n(1-r) \times n$ LDPC matrix. Let $\mathcal{C}$ be the code whose parity-check matrix is H. Let H_1 and H_2 be the submatrices of H such that

$$H = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix},$$

where H_1 is an $n(1 - r_1) \times n$ matrix. Clearly, $r_1 > r$. Let $\mathcal{C}_1$ be the code with parity-check matrix H_1. $\mathcal{C}$ is the coarse code, and $\mathcal{C}_1$ is the fine code in the nested code $(\mathcal{C}_1, \mathcal{C})$, and $\mathcal{C}_1$ is partitioned into $2^{n(r_1-r)}$ disjoint subsets given by the cosets of $\mathcal{C}$. Assume that Alice wants to transmit a message W whose binary representation is given by an $n(r_1 - r)$-bit vector $\underline{S}$. To do this she transmits $\underline{X}$, which is a randomly chosen solution of

$$\begin{bmatrix} H_1 \\ H_2 \end{bmatrix} \underline{X} = [0 \cdots 0 \ \underline{S}]^T.$$

As shown in [2], the equivocation for Eve is

$$\Delta \equiv H(W|\underline{Z}) = n(\epsilon_w - (1 - r_1)). \tag{1}$$

If $\mathcal{C}$ is capacity achieving over the wiretapper's channel then $\epsilon_w = 1 - r$ and $\Delta = n(r_1 - r)$. This means that $\underline{S}$ is perfectly secure from Eve, since the rate from Alice to Bob is $r_1 - r$. Also, if the threshold of the code $\mathcal{C}_1$ is higher than the main channel erasure probability ϵ_m then Bob can recover $\underline{S}$ reliably.

The natural candidate for such a code construction is a two edge type LDPC code. A two edge type matrix H has form

$$H = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}. \tag{2}$$

The two types of edges are the edges connected to check nodes in H_1 and those connected to check nodes in H_2. An example of a two edge type LDPC code is shown in Figure 2. We now define the degree distribution of edges. Let $\omega^{(j)}_{i_1 i_2}$ denote the fraction of type j ($j = 1$ or 2) edges connected to variable nodes with i_1 outgoing type 1 edges and i_2 outgoing type 2 edges. The fraction $\omega^{(j)}_{i_1 i_2}$ is calculated with respect to the total number of type j edges. Let $\Omega_{i_1 i_2}$ be the fraction of variable nodes with i_1 outgoing edges of type 1 and i_2 outgoing edges of type 2. This gives the following relationships between $\Omega, \omega^{(1)}$, and $\omega^{(2)}$, which hold whenever the right hand side is defined,

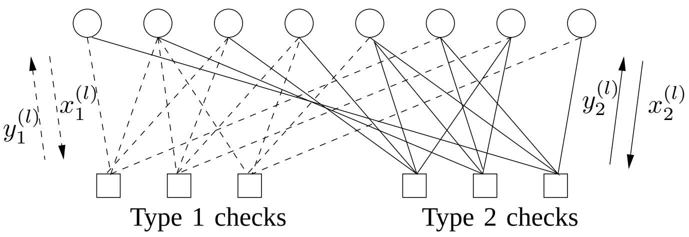

Fig. 2. Two edge type LDPC code

$$\omega^{(1)}_{i_1 i_2} = \frac{i_1 \Omega_{i_1 i_2}}{\sum_{i_1, i_2} i_1 \Omega_{i_1 i_2}} \tag{3}$$

$$\omega^{(2)}_{i_1 i_2} = \frac{i_2 \Omega_{i_1 i_2}}{\sum_{i_1, i_2} i_2 \Omega_{i_1 i_2}} \tag{4}$$

$$\Omega_{i_1 i_2} = \frac{\frac{\omega^{(1)}_{i_1 i_2}}{i_1}}{\sum_{i_1, i_2} \frac{\omega^{(1)}_{i_1 i_2}}{i_1}} = \frac{\frac{\omega^{(2)}_{i_1 i_2}}{i_2}}{\sum_{i_1, i_2} \frac{\omega^{(2)}_{i_1 i_2}}{i_2}}. \tag{5}$$

Similarly, let $\rho^{(j)}_i$ denote the degree distribution of type j edges on the check node side. Note that only one type of edges is connected to a particular check node. Like the standard LDPC ensemble of [5], the two edge type LDPC ensemble with block length n and degree distribution $\left\{\omega^{(1)}, \omega^{(2)}, \rho^{(1)}, \rho^{(2)}\right\}$ is the collection of all the bipartite graphs satisfying the degree distribution constraints. To write the density evolution recursion, let $x^{(l)}_j$ denote the probability that a message from a variable node to a check node on an edge of type j in iteration l is erased. Clearly,

$$x^{(1)}_j = \epsilon.$$

In the same way let $y^{(l)}_j$ be the probability that a message from a check node to a variable node on an edge of type j in iteration l is erased. This probability is

$$y^{(l)}_j = 1 - \rho^{(j)}(1 - x^{(l)}_j), \quad j = 1, 2$$

where $\rho^{(j)}(x) = \sum_i \rho^{(j)}_i x^{i-1}$. Using this we can write down the following recursions for $x^{(l)}_j$:

$$x^{(l+1)}_1 = \epsilon \omega^{(1)}(y^{(l)}_1, y^{(l)}_2) \tag{6}$$

$$x^{(l+1)}_2 = \epsilon \omega^{(2)}(y^{(l)}_1, y^{(l)}_2), \tag{7}$$

where

$$\omega^{(1)}(x, y) = \sum_{i_1, i_2} \omega^{(1)}_{i_1 i_2} x^{i_1 - 1} y^{i_2}$$

$$\omega^{(2)}(x, y) = \sum_{i_1, i_2} \omega^{(2)}_{i_1 i_2} x^{i_1} y^{i_2 - 1}.$$

As the density evolution recursion is a two dimensional recursion, it is difficult to analyze. Thus we look for degree distributions which reduce the two dimensional recursion to a single dimension to be able to use the standard setting of density evolution recursion for the BEC. To do this, we impose the following constraints:

$$\rho^{(1)}(x) = \rho^{(2)}(x) = \rho(x) \tag{8}$$

$$\omega^{(1)}(x, x) = \omega^{(2)}(x, x) = \lambda(x). \tag{9}$$

Note that since

$$\omega^{(j)}(x, x) = \sum_{i_1, i_2} \omega^{(j)}_{i_1 i_2} x^{i_1 + i_2 - 1} = \sum_k \left(\sum_{i_1 + i_2 = k} \omega^{(j)}_{i_1 i_2} \right) x^{k-1},$$

(9) implies

$$\sum_{i_1 + i_2 = k} \omega^{(1)}_{i_1 i_2} = \sum_{i_1 + i_2 = k} \omega^{(2)}_{i_1 i_2} \quad \forall k. \tag{10}$$

Equation (8) ensures that $y^{(l)}_1 = y^{(l)}_2$ whenever $x^{(l)}_1 = x^{(l)}_2$, and (9) ensures $x^{(l+1)}_1 = x^{(l+1)}_2$ whenever $y^{(l)}_1 = y^{(l)}_2$. Thus, since $x^{(1)}_j = \epsilon$ we can skip the subscripts on $x^{(l)}_j$ and $y^{(l)}_j$ and end up with the usual one dimensional density evolution equation

$$x^{(l+1)} = \epsilon \lambda(1 - \rho(1 - x^{(l)})), \tag{11}$$

where $\lambda(x) = \sum_k \lambda_k x^{k-1}$ is given by

$$\lambda_k = \sum_{i_1 + i_2 = k} \omega^{(1)}_{i_1 i_2}. \tag{12}$$

Assume that we can find an assignment of $\omega^{(1)}, \omega^{(2)}, \rho^{(1)}, \rho^{(2)}$ which satisfies (5), (8), (9), (10), and (12). Now by choosing (λ, ρ) to be a degree distribution for the BEC with threshold $\epsilon^\star$, we obtain that the two edge type LDPC ensemble also has the same threshold $\epsilon^\star$. Thus it can guarantee an equivocation of $n(\epsilon^\star - (1-r_1))$, where r_1 is the rate of matrix H_1. To compute the threshold achievable on the main channel, we need to compute the threshold of $\mathcal{C}_1$. The ensemble of matrix H_1 is a standard LDPC ensemble, and its degree distribution can be easily calculated from the degree distribution of the two edge type ensemble. Hence we can easily compute its threshold. In the following theorem we present such an assignment of $\omega^{(1)}, \omega^{(2)}, \rho^{(1)}, \rho^{(2)}$.

Theorem II.1. *Let (λ, ρ) be a standard LDPC degree distribution with design rate r and threshold $\epsilon^\star$ over the BEC. Then the following assignment*

$$\rho^{(1)}(x) = \rho^{(2)}(x) = \rho(x)$$

$$\omega^{(1)}_{ii} = \omega^{(2)}_{ii} = \lambda_{2i} \tag{13}$$

$$\omega^{(1)}_{ii+1} = \omega^{(2)}_{i+1i} = \frac{i}{2i+1}\lambda_{2i+1} \tag{14}$$

$$\omega^{(1)}_{i+1i} = \omega^{(2)}_{ii+1} = \frac{i+1}{2i+1}\lambda_{2i+1} \tag{15}$$

$$\omega^{(1)}_{i_1i_2} = \omega^{(2)}_{i_1i_2} = 0 \quad |i_1 - i_2| > 1, \tag{16}$$

ensures that the two edge type LDPC ensemble $\left\{\omega^{(1)}, \omega^{(2)}, \rho^{(1)}, \rho^{(2)}\right\}$ also has design rate r and threshold $\epsilon^\star$. Also, it guarantees an equivocation of $n(\epsilon^\star - (1-r)/2)$ to Eve.

Proof: Note that

$$\omega^{(1)}_{i_1i_2} = \omega^{(2)}_{i_2i_1} \ \forall i_1, i_2. \tag{17}$$

This ensures that (5) is fulfilled.

We now show that $\omega^{(1)}(x,x) = \omega^{(2)}(x,x) = \lambda(x)$. Then the two dimensional density evolution recursion becomes the one dimensional recursion in (11), and the two type edge ensemble will have the same threshold as the one edge type ensemble. We have

$$\begin{aligned}
\omega^{(1)}(x,x) &= \sum_{i_1,i_2} \omega^{(1)}_{i_1i_2} x^{i_1+i_2-1} \\
&\overset{(a)}{=} \sum_i \omega^{(1)}_{ii+1}x^{2i} + \omega^{(1)}_{ii}x^{2i-1} + \omega^{(1)}_{i+1i}x^{2i} \\
&\overset{(b)}{=} \sum_i \frac{i}{2i+1}\lambda_{2i+1}x^{2i} + \lambda_{2i}x^{2i-1} + \\
&\quad + \frac{i+1}{2i+1}\lambda_{2i+1}x^{2i} \\
&= \sum_i \lambda_{2i+1}x^{2i} + \lambda_{2i}x^{2i-1} \\
&= \lambda(x)
\end{aligned}$$

where (a) is due to (16) and (b) is due to (13) - (15). The proof for $\omega^{(2)}(x,x)$ is done in the same way.

The design rate of the two edge type ensemble is

$$r_{\text{des}} = 1 - (m_1 + m_2)/n$$

where m_j is the number of parity checks of type j and n is the number of variable nodes. If we let d_{avg} denote the average check node degree and count the number of type j edges in two different ways we get

$$n\sum_{i_1,i_2} i_j\Omega_{i_1i_2} = m_j d_{\text{avg}}$$

or

$$\begin{aligned}
\frac{m_j}{n} &= \frac{\sum_{i_1,i_2} i_j\Omega_{i_1i_2}}{d_{\text{avg}}} \\
&\overset{(a)}{=} \frac{1}{d_{\text{avg}}} \frac{\sum_{i_1,i_2} i_j \frac{\omega^{(j)}_{i_1i_2}}{i_j}}{\sum_{i_1,i_2} \frac{\omega^{(j)}_{i_1i_2}}{i_j}} \\
&\overset{(b)}{=} \frac{1}{d_{\text{avg}}} \frac{1}{\sum_{i_1,i_2} \frac{\omega^{(j)}_{i_1i_2}}{i_j}}
\end{aligned}$$

where (a) is due to (5) and (b) follows since the $\omega^{(1)}_{i_1i_2}$ sum to 1.

The design rate then becomes

$$\begin{aligned}
r_{\text{des}} &= 1 - (m_1 + m_2)/n \\
&= 1 - \frac{1}{d_{\text{avg}}}\left(\frac{1}{\sum_{i_1,i_2}\frac{\omega^{(1)}_{i_1i_2}}{i_1}} + \frac{1}{\sum_{i_1,i_2}\frac{\omega^{(2)}_{i_1i_2}}{i_2}}\right) \\
&\overset{(a)}{=} 1 - \frac{2}{d_{\text{avg}}}\left(\frac{1}{\sum_{i_1,i_2}\frac{\omega^{(1)}_{i_1i_2}}{i_1}}\right) \\
&\overset{(b)}{=} 1 - \frac{2}{d_{\text{avg}}}\left(\frac{1}{\sum_i \frac{\lambda_{2i+1}}{2i+1} + \frac{\lambda_{2i}}{i} + \frac{\lambda_{2i+1}}{2i+1}}\right) \\
&= 1 - \frac{1}{d_{\text{avg}}}\frac{1}{\sum_i \frac{\lambda_{2i+1}}{2i+1} + \frac{\lambda_{2i}}{2i}} \\
&= 1 - \frac{1}{d_{\text{avg}}}\frac{1}{\sum_i \frac{\lambda_i}{i}}
\end{aligned}$$

where (a) is due to (17) and (b) follows using (13) - (16). Since this expression is the same as the design rate of the standard LDPC ensemble (λ, ρ) we have shown that $\mathcal{C}$ has design rate r. Thus if the one edge type ensemble achieves capacity over the BEC(ϵ_w), so does the two edge type ensemble.

To show that the equivocation to Eve is $n(\epsilon^\star - (1-r)/2)$ we show that the design rate of $\mathcal{C}_1$ is $(1+r)/2$ and use (1). The fraction of type 1 edges connected to a variable node with i_1 outgoing type 1 edges is given by $\sum_{i_2}\omega^{(1)}_{i_1i_2}$, so the variable degree distribution for H_1 is given by

$$\begin{aligned}
\lambda^{(1)}_i &= \sum_{i_2}\omega^{(1)}_{ii_2} \\
&= \omega^{(1)}_{ii-1} + \omega^{(1)}_{ii} + \omega^{(1)}_{ii+1} \\
&= \frac{i}{2i-1}\lambda_{2i-1} + \lambda_{2i} + \frac{i}{2i+1}\lambda_{2i+1}
\end{aligned}$$

again using (13) - (16). Thus the design rate for $\mathcal{C}_1$ becomes

$$\begin{aligned} r_1 &= 1 - \frac{1}{d_{\text{avg}}} \frac{1}{\sum_i \frac{\lambda_i^{(1)}}{i}} \\ &= 1 - \frac{1}{d_{\text{avg}}} \frac{1}{\sum_i \frac{\lambda_{2i-1}}{2i-1} + \frac{2\lambda_{2i}}{2i} + \frac{\lambda_{2i+1}}{2i+1}} \\ &= 1 - \frac{1}{2} \frac{1}{d_{\text{avg}}} \frac{1}{\sum_i \frac{\lambda_i}{i}} \\ &= 1 - \frac{1}{2}(1-r) \\ &= \frac{1+r}{2}. \end{aligned}$$

■

Since all capacity approaching sequences of degree distributions have some degree two variable nodes we see that our construction will have some degree one variable nodes in the code for the main channel. This means that the threshold over the main channel will be zero. To get around this problem we use linear programming methods to find good degree distributions satisfying the two dimensional density evolution equations.

III. Numerical Optimization

Since the construction in Theorem II.1 gives a code over the main channel with threshold zero we try to find a good two edge type ensemble using numerical methods. First we optimize $\mathcal{C}_1$ for the main channel using the methods described in [6] and obtain a good ensemble $(\Lambda^{(1)}, R^{(1)})$ for the main channel. $\Lambda^{(1)}$ and $R^{(1)}$ are degree distributions from the node perspective.

For a given two edge type ensemble we can find the corresponding one edge type ensemble for $\mathcal{C}_1$ by summing over the second index, since the fraction of variable nodes with i_1 outgoing type 1 edges is given by $\sum_{i_2} \Omega_{i_1 i_2}$. To fix the degree distribution of H_1 we then impose the constraint

$$\sum_{i_2} \Omega_{i_1 i_2} = \Lambda_{i_1}^{(1)} \text{ for all } i_1.$$

For succesful decoding we impose the two constraints $x_1^{(l+1)} \leq x_1^{(l)}$ and $x_2^{(l+1)} \leq x_2^{(l)}$ which can be written as

$$\begin{aligned} x_1 &\geq \epsilon \omega^{(1)}(y_1, y_2) \\ &= \epsilon \sum_{i_1, i_2} \omega_{i_1 i_2}^{(1)} y_1^{i_1 - 1} y_2^{i_2} \\ &= \epsilon \sum_{i_1, i_2} \frac{i_1 \Omega_{i_1, i_2}}{\sum_{k_1, k_2} k_1 \Omega_{k_1, k_2}} y_1^{i_1 - 1} y_2^{i_2}. \end{aligned}$$

where we have used (3) in the last step, and y_1, y_2 are given by

$$y_j = 1 - \rho_j(1 - x_j).$$

This simplifies to the linear constraint

$$0 \leq \sum_{i_1, i_2} i_1 (x_1 - \epsilon y_1^{i_1 - 1} y_2^{i_2}) \Omega_{i_1 i_2}.$$

The corresponding constraint for x_2 is

$$0 \leq \sum_{i_1, i_2} i_1 (x_2 - \epsilon y_1^{i_1} y_2^{i_2 - 1}) \Omega_{i_1 i_2}.$$

The design rate can be written as

$$r_{\text{des}} = 1 - \frac{\sum_{i_1, i_2} i_1 \Omega_{i_1 i_2}}{\sum_i i R_i^{(1)}} - \frac{\sum_{i_1, i_2} i_2 \Omega_{i_1 i_2}}{\sum_i i R_i^{(2)}},$$

where the term $\frac{\sum_{i_1, i_2} i_1 \Omega_{i_1 i_2}}{\sum_i i R_i^{(1)}}$ is constant because of the fixed degree distribution of H_1. If $R^{(2)}$ is fixed we see that maximizing the design rate is the same as minimizing $\sum_{i_1, i_2} i_2 \Omega_{i_1 i_2}$. Thus we end up with the following linear program:

$$\text{minimize } \sum_{i_1, i_2} i_2 \Omega_{i_1 i_2}$$

subject to

$$\begin{aligned} &\sum_{i_2} \Omega_{i_1 i_2} = \Lambda_{i_1}^{(1)}, \; i_1 = 2, \ldots, I \\ &\sum_{i_1, i_2} i_1 (x_1(k) - \epsilon y_1(k)^{i_1 - 1} y_2(k)^{i_2}) \Omega_{i_1 i_2} \geq 0, \; k = 1, \ldots, K \\ &\sum_{i_1, i_2} i_1 (x_2(k) - \epsilon y_1(k)^{i_1} y_2(k)^{i_2 - 1}) \Omega_{i_1 i_2} \geq 0, \; k = 1, \ldots, K, \end{aligned}$$

where I is the largest degree in $\Lambda^{(1)}(x)$. The points $\{x_1(k), x_2(k)\}_{k=1}^K$ are chosen by generating a distribution Ω and then running the density evolution recursion

$$\begin{aligned} x_1^{(1)} &= x_2^{(1)} = \epsilon \\ x_1^{(l+1)} &= \epsilon \omega^{(1)}(y_1^{(l)}, y_2^{(l)}) \\ x_2^{(l+1)} &= \epsilon \omega^{(2)}(y_1^{(l)}, y_2^{(l)}) \end{aligned}$$

K times. The program is then solved repeatedly, each time updating $\{x_1(k), x_2(k)\}_{k=1}^K$. This process is repeated several times for different check node degree distributions $R^{(2)}$.

Two degree distributions found in this way are given in Tables II and III. The same distribution was used for H_1, a rate .498836 code with threshold .5 and multiplicative gap to capacity $(1 - \epsilon - r_{\text{des}})/(1 - \epsilon) = 0.00232857$. The degree distribution for this code is given in Table I.

The code in Table II has rate 0.39893 and threshold 0.6. The multiplicative gap to capacity of this code is 0.00267632. The rate from Alice to Bob is 0.099906 and the equivocation for Eve is $0.098836n$.

The code in Table III has rate 0.248705 and threshold 0.75. The multiplicative gap to capacity is 0.00518359. The rate from Alice to Bob is 0.250131 and the equivocation for Eve is $0.248836n$.

IV. Conclusion

We have constructed a capacity achieving sequence of two edge type LDPC ensembles based on standard LDPC ensembles. The reliability and security performance of our construction can easily be computed from the performance of the standard LDPC ensemble over the BEC. Note that

TABLE I
DEGREE DISTRIBUTION FOR H_1

i	Λ_i
2	0.5572098
3	0.1651436
4	0.07567923
5	0.0571348
7	0.043603
8	0.02679802
13	0.013885518
14	0.0294308
31	0.02225301
100	0.00886105

i	$R_i^{(1)}$
9	0.25
10	0.75

TABLE II
DEGREE DISTRIBUTIONS FOR A CODE OPTIMIZED FOR $\epsilon_m = 0.5$ AND $\epsilon_w = 0.6$.

i_1	i_2	$\Omega_{i_1 i_2}$
2	0	0.463846
2	1	0.0814943
2	2	0.0118691
3	0	0.14239
3	1	0.0201658
3	2	0.00258812
4	0	0.0292241
4	1	0.0464551
5	0	0.0564162
5	1	0.000718585
7	1	0.0436039
8	1	0.0258926
8	2	0.000905503
13	2	0.00631474
13	5	0.00757076
14	1	0.011051
14	2	0.0173718
14	5	0.00100807
31	0	0.00240762
31	4	0.0012626
31	5	0.0185828
100	4	0.000326117
100	17	0.00383319
100	18	0.00470174

i	$R_i^{(1)}$
9	0.25
10	0.75

i	$R_i^{(2)}$
6	1.0

if we choose the standard LDPC ensemble to be capacity achieving, we achieve perfect secrecy as the two edge type LDPC ensemble is then also capacity achieving. However, as there are degree two variable nodes in a capacity achieving degree distribution, we obtain some degree one variable nodes in the upper submatrix H_1. This reduces its threshold to zero, requiring an error free main channel.

TABLE III
DEGREE DISTRIBUTIONS FOR A CODE OPTIMIZED FOR $\epsilon_m = 0.5$ AND $\epsilon_w = 0.75$.

i_1	i_2	$\Omega_{i_1 i_2}$
2	0	0.367823
2	1	0.166244
2	2	0.0231428
3	0	0.125727
3	1	0.0394166
4	0	0.00286773
4	1	0.0728115
5	1	0.0571348
7	2	0.0300989
7	3	0.013505
8	3	0.0196622
8	4	0.00713582
13	2	0.000565918
13	5	0.0133196
14	2	0.0149732
14	5	0.0132215
14	6	0.0012361
31	8	0.00490831
31	9	0.0173447
100	17	0.00130606
100	30	0.00498932
100	31	0.00256567

i	$R_i^{(1)}$
9	0.25
10	0.75

i	$R_i^{(2)}$
4	0.25
5	0.75

To alleviate this problem we use numerical methods to find codes with rates close to the secrecy capacity and high equivocation over the wiretapper's channel.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *Information Theory, IEEE Transactions on*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[3] R. Liu, H. Poor, P. Spasojevic, and Y. Liang, "Nested codes for secure transmission," in *Proc. Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, Sept. 2008, pp. 1–5.

[4] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *Information Theory, IEEE Transactions on*, vol. 48, no. 6, pp. 1250–1276, Jun 2002.

[5] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *Information Theory, IEEE Transactions on*, vol. 47, no. 2, pp. 619–637, Feb. 2001.

[6] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge University Press, 2008. [Online]. Available: http://www.cambridge.org/catalogue/catalogue.asp?isbn=9780521852296