Equivocation of Eve using Two Edge Type LDPC Codes for the Binary Erasure Wiretap Channel

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

***Abstract*—We consider transmission over a binary erasure wiretap channel using the code construction method introduced by Rathi et al. based on two edge type Low-Density Parity-Check (LDPC) codes and the coset encoding scheme.**

By generalizing the method of computing conditional entropy for standard LDPC ensembles introduced by Méasson, Montanari, and Urbanke to two edge type LDPC ensembles, we show how the equivocation for the wiretapper can be computed. We find that relatively simple constructions give very good secrecy performance and are close to the secrecy capacity.

I. Introduction

Wyner introduced the notion of a wiretap channel in [1] which is depicted in Figure 1. In general, the channel from Alice to Bob and the channel from Alice to Eve can be any two discrete memoryless channels. In this paper we will restrict ourselves to the setting where both channels are Binary Erasure Channels (BEC). We denote a BEC with erasure probability ϵ by BEC(ϵ). In a wiretap channel, Alice communicates a message $\underline{S}$, which is chosen uniformly at random from the message set $\mathcal{S}$, to Bob through the main channel which is a BEC(ϵ_m). Alice performs this task by encoding $\underline{S}$ as an n bit vector $\underline{X}$ and transmitting $\underline{X}$ across BEC(ϵ_m). Bob receives a noisy version of $\underline{X}$ denoted by $\underline{Y}$. Eve observes $\underline{X}$ via the wiretapper's channel BEC(ϵ_w) and receives a noisy version of $\underline{X}$ denoted by $\underline{Z}$. We denote such a wiretap channel by BEC-WT(ϵ_m, ϵ_w).

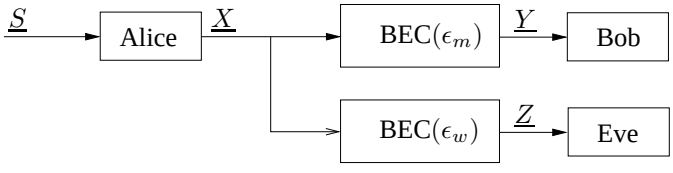

Fig. 1. Wiretap channel.

The encoding of a message $\underline{S}$ by Alice should be such that Bob is able to decode $\underline{S}$ reliably and $\underline{Z}$ provides as little information as possible to Eve about $\underline{S}$.

This work was funded in part by the Swedish Research Council and NSF grant CCF-0830666.

A code of rate R_{ab} with block length n for the wiretap channel is given by a message set $\mathcal{S}$ of cardinality $|\mathcal{S}| = 2^{nR_{ab}}$ and a set of disjoint sub-codes $\{\mathcal{C}(\underline{s}) \subset \mathcal{X}^n\}_{\underline{s}\in\mathcal{S}}$. To encode the message $\underline{s} \in \mathcal{S}$, Alice chooses one of the codewords in $\mathcal{C}(\underline{s})$ uniformly at random and transmits it. Bob uses a decoder $\phi : \mathcal{Y}^n \to \mathcal{S}$ to determine which message was sent.

A rate-equivocation pair (R_{ab}, R_e) is said to be achievable if $\forall \epsilon > 0$, there exists a sequence of codes of rate R_{ab} of length n and decoders ϕ_n such that the following reliability and secrecy criteria are satisfied:

$$\text{Reliability: } \lim_{n\to\infty} \quad P(\phi_n(\underline{Y}) \neq \underline{S}) < \epsilon, \tag{1}$$

$$\text{Secrecy: } \liminf_{n\to\infty} \frac{1}{n} H(\underline{S}|\underline{Z}) > R_e - \epsilon. \tag{2}$$

Note that we use the weak notion of secrecy as opposed to the strong notion [2]. With a slight abuse of terminology, when we say equivocation we mean the normalized equivocation as defined in the LHS of (2). As shown in [1], the set of achievable pairs (R_{ab}, R_e) for BEC-WT(ϵ_m, ϵ_w) is given by

$$R_e \leq R_{ab} \leq 1 - \epsilon_m, \quad 0 \leq R_e \leq \epsilon_w - \epsilon_m. \tag{3}$$

The points in the achievable region where $R_{ab} = R_e$ correspond to *perfect secrecy* i.e. for these points $I(\underline{Z}; \underline{S})/n \to 0$. The highest achievable rate R_{ab} at which we can achieve perfect secrecy is called the *secrecy capacity* [1] and we denote it by C_S. For the BEC-WT(ϵ_w, ϵ_m), we have $C_S = \epsilon_w - \epsilon_m$.

In [3], [4] the authors have given code design methods based on nested sparse graph codes and a coset encoding scheme. It was shown in [3] 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. In [5] we have given a code construction based on coset encoding and nested two edge type LDPC codes. This code construction was analyzed using density evolution, and numerical methods were found to optimize the thresholds for the coarse and the fine code.

Reliability, which corresponds to the probability of decoding error for the intended receiver, can be easily measured using density evolution recursion. However secrecy, which is given by the equivocation of the message conditioned on

the wiretapper's observation, can not be easily calculated. Méasson, Montanari, and Urbanke have derived a method to measure equivocation for a broad range of standard LDPC ensembles for point-to-point transmission over the BEC [6]. In the following we denote this approach the MMU method[1]. It was extended to non-binary LDPC codes for the BEC in [7]. By generalizing it to two edge type LDPC ensembles, we show how the equivocation for the wiretapper can be computed. We find that relatively simple constructions give very good secrecy performance and are close to the secrecy capacity.

II. Code Construction

We first describe the coset encoding and syndrome decoding method. 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 sub-matrices 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 $(\mathcal{C}_1, \mathcal{C})$. Also, $\mathcal{C}_1$ is partitioned into $2^{n(R_1-R)}$ disjoint subsets given by the cosets of $\mathcal{C}$. Alice uses the *coset encoding method* to communicate her message to Bob which we now describe.

Coset Encoding Method: Assume that Alice wants to transmit a message 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

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

Bob uses the following *syndrome decoding* approach to retrieve the message from Alice.

Syndrome Decoding: After observing $\underline{Y}$, Bob obtains an estimate $\hat{\underline{X}}$ for $\underline{X}$ using the parity check equations $H_1\underline{X} = 0$. Then he computes an estimate $\hat{\underline{S}}$ for $\underline{S}$ as $\hat{\underline{S}} = H_2\hat{\underline{X}}$.

A natural candidate for coset encoding is a two edge type LDPC code. A two edge type matrix H has the form

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

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 a two edge type LDPC ensemble. Let $\lambda^{(j)}_{l_1 l_2}$ denote the fraction of type j ($j = 1$ or 2) edges connected to variable nodes with l_1 outgoing type one edges and l_2 outgoing type two edges. The fraction $\lambda^{(j)}_{l_1 l_2}$ is calculated with respect to the total number of type j edges. Let $\Lambda_{l_1 l_2}$ be the fraction of variable nodes with l_1 outgoing edges of type one and l_2 outgoing edges of type two. $\Lambda_{l_1 l_2}$ is the degree distribution from the node perspective, and $\lambda^{(j)}_{l_1 l_2}$ is the degree distribution from the edge perspective. Similarly,

[1]We call it the MMU method in acknowledgment of the authors Méasson, Montanari, and Urbanke.

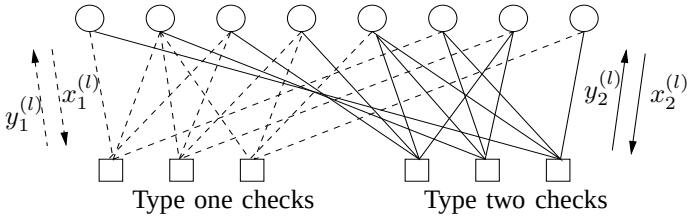

Fig. 2. Two edge type LDPC code.

let $\rho^{(j)}_r$ and $\Gamma^{(j)}_r$ denote the degree distribution of type j edges on the check node side from the edge and node perspective respectively. Note that only one type of edges is connected to a particular check node. An equivalent definition of the degree distribution is given by the following polynomials:

$$\begin{aligned}
\Lambda(x,y) &= \sum_{l_1,l_2} \Lambda_{l_1 l_2} x^{l_1} y^{l_2}, \\
\lambda^{(1)}(x,y) &= \sum_{l_1,l_2} \lambda^{(1)}_{l_1 l_2} x^{l_1-1} y^{l_2}, \\
\lambda^{(2)}(x,y) &= \sum_{l_1,l_2} \lambda^{(1)}_{l_1 l_2} x^{l_1} y^{l_2-1}, \\
\Gamma^{(j)}(x) &= \sum_r \Gamma^{(j)}_r x^r, \quad j = 1,2, \\
\rho^{(j)}(x) &= \sum_r \rho^{(j)}_r x^{r-1}, \quad j = 1,2.
\end{aligned}$$

Like the standard LDPC ensemble of [8], the two edge type LDPC ensemble with block length n and degree distribution $\{\Lambda, \Gamma^{(1)}, \Gamma^{(2)}\}$ is the collection of all bipartite graphs satisfying the degree distribution constraints, where we allow multiple edges between two nodes.

Consider the two edge type LDPC ensemble $\{\Lambda, \Gamma^{(1)}, \Gamma^{(2)}\}$. If we consider the ensemble of the subgraph induced by one particular type of edges then it is easy to see that the resulting ensemble is the standard LDPC ensemble and we can easily calculate its degree distribution. Let $\{\Lambda^{(j)}, \Gamma^{(j)}\}$ be the degree distribution of the ensemble induced by type j edges, $j = 1, 2$. Then $\Lambda^{(j)}$, for $j = 1, 2$, is given by

$$\Lambda^{(1)}_{l_1} = \sum_{l_2} \Lambda_{l_1 l_2}, \quad \Lambda^{(2)}_{l_2} = \sum_{l_1} \Lambda_{l_1 l_2}.$$

Assume that transmission takes place over BEC(ϵ) and 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. Then the density evolution recursion is

$$x^{(l+1)}_1 = \epsilon \lambda^{(1)}(y^{(l)}_1, y^{(l)}_2) \tag{4}$$

$$x^{(l+1)}_2 = \epsilon \lambda^{(2)}(y^{(l)}_1, y^{(l)}_2), \tag{5}$$

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

In the next section we show how to compute the equivocation of Eve when using a given two edge type LDPC ensemble.

III. Computation of Equivocation

In order to compute the average equivocation of Eve over the erasure pattern and ensemble of codes, we generalize

the MMU method of [6] to two edge type LDPC codes. In [6], the equivocation of standard LDPC ensemble for point-to-point communication over a BEC(ϵ) was computed. More precisely, let $\underline{\tilde{X}}$ be a randomly chosen codeword of a randomly chosen code G from the standard LDPC ensemble. Let $\underline{\tilde{X}}$ be transmitted over BEC(ϵ) and let $\underline{\tilde{Z}}$ be the channel output. Then the MMU method computes

$$\lim_{n\to\infty} \frac{\mathbb{E}\left(H_G(\underline{\tilde{X}}|\underline{\tilde{Z}})\right)}{n},$$

where $H_G(\underline{\tilde{X}}|\underline{\tilde{Z}})$ is the conditional entropy of the transmitted codeword given the channel observation for the code G and we perform the averaging over the ensemble. The MMU method is described below.

1) Consider decoding using the peeling decoder [9, pp. 115]. The peeling decoder gets stuck in the largest stopping set contained in the set of erased variable nodes. The subgraph induced by this stopping set is again a code whose codewords are compatible with the erasure set. We call this subgraph the *residual graph*. Thus the peeling decoder associates to every graph and erasure set a residual graph. If the erasure probability is above the BP threshold, then almost surely the residual graph has a degree distribution close to the *average residual degree distribution* [10]. The average residual degree distribution can be computed by the asymptotic analysis of the peeling decoder.
2) Conditioned on the residual degree distribution, the induced probability distribution is uniform over all the graphs with the given degree distribution. This implies that almost surely a residual graph is an element of the standard LDPC ensemble with degree distribution equal to the average residual degree distribution.
3) One can easily compute the design rate of the average residual degree distribution. However, the design rate is only a lower bound on the rate. A criterion was derived in [6], which, when satisfied, guarantees that the actual rate is equal to the design rate. If the actual rate is equal to the design rate, then the equivocation is given by the design rate of the standard LDPC ensemble with degree distribution equal to the average residual degree distribution.

To use the MMU method to compute the equivocation $H(\underline{S}|\underline{Z})$, we use the chain rule to write $H(\underline{S},\underline{X}|\underline{Z})$ in two different ways and obtain

$$H(\underline{X}|\underline{Z}) \;+\; H(\underline{S}|\underline{X},\underline{Z}) \;\;=\;\; H(\underline{S}|\underline{Z}) \;+\; H(\underline{X}|\underline{S},\underline{Z}).$$

By noting that $H(\underline{S}|\underline{X},\underline{Z})=0$ we obtain

$$\frac{H(\underline{S}|\underline{Z})}{n} = \frac{H(\underline{X}|\underline{Z})}{n} - \frac{H(\underline{X}|\underline{S},\underline{Z})}{n}. \tag{6}$$

Note that $\underline{X}$ is a randomly chosen solution of $H_1\underline{X}=0$. These solutions are codewords of codes from the standard LDPC ensemble $\{\Lambda^{(1)},\Gamma^{(1)}\}$, and $\underline{Z}$ is the channel output from BEC(ϵ_w). Thus we can compute $\lim_{n\to\infty} H(\underline{X}|\underline{Z})/n$ by using [6, Thm. 10]. For more details we refer to [11].

In the following subsection we generalize the MMU method to two edge type LDPC ensembles in order to compute $\lim_{n\to\infty} H(\underline{X}|\underline{S},\underline{Z})/n$.

A. Computing Normalized $H(\underline{X}|\underline{S},\underline{Z})$

The proof of Step 1 and 2 of the MMU method for two edge type LDPC ensembles is the same as for standard LDPC ensembles. We state the following lemma to compute the average residual degree distribution which we will need later and refer to [11] for more details.

Lemma III.1. *Consider transmission over BEC(ϵ_w) using the two type LDPC ensemble $\{\Lambda,\Gamma^{(1)},\Gamma^{(2)}\}$ which is decoded by the peeling decoder. Let (x_1,x_2) be the fixed points of (4) and (5) when initialized with channel erasure probability ϵ_w. Let $y_j=1-\rho^{(j)}(1-x_j),\ j=1,2$, where $\rho^{(j)}$ is the degree distribution of check nodes of type j from the edge perspective. Then the average residual degree distribution $\{\Omega,\Phi^{(1)},\Phi^{(2)}\}$ is given by*

$$\begin{aligned}\Omega(z_1,z_2) &= \epsilon\Lambda(z_1y_1,z_2y_2),\\ \Phi^{(j)}(z) &= \Gamma^{(j)}(1-x_j+x_jz) - x_jz\Gamma'^{(j)}(1-x_j)\\ &\quad - \Gamma^{(j)}(1-x_j),\quad j=1,2,\end{aligned}$$

where $\Gamma'^{(j)}(x)$ is the derivative of $\Gamma^{(j)}(x)$. Note that the degree distributions are normalized with respect to the number of variable (check) nodes in the original graph.

Proof: The proof follows from the analysis for the standard LDPC case [12]. ∎

The key technical task when generalizing Step 3 of the MMU method to two edge type LDPC ensembles is to derive a criterion, which, when satisfied, guarantees that almost every code in the residual ensemble has its rate equal to the design rate. The rate is equal to the normalized logarithm of the total number of codewords. However, as the average of the logarithm of the total number of codewords is hard to compute, we instead compute the normalized logarithm of the average of the total number of codewords. By Jensen's inequality this is an upper bound on the average rate. If this upper bound is equal to the design rate, then by similar arguments as in [6, Lem. 7] we can show that almost every code in the ensemble has its rate equal to the design rate. To compute this upper bound we derive the average of the total number of codewords of a two edge type LDPC ensemble in the following lemma.

Lemma III.2. *Let N be the total number of codewords of a randomly chosen code from the two edge type LDPC ensemble $(\Lambda,\Gamma^{(1)},\Gamma^{(2)})$. Then the average of N over the ensemble is given by*

$$\begin{aligned}\mathbb{E}(N) &= \mathbb{E}\left(\sum_{E_1=0,E_2=0}^{n\Lambda'_1(1,1),n\Lambda'_2(1,1)} N(E_1,E_2)\right)\\ &= \sum_{E_1=0,E_2=0}^{n\Lambda'_1(1,1),n\Lambda'_2(1,1)} \operatorname{coef}\left\{\prod_{l_1,l_2}(1+u_1^{l_1}u_2^{l_2})^{n\Lambda_{l_1,l_2}}, u_1^{E_1}u_2^{E_2}\right\}\times\end{aligned}$$

$$\frac{\text{coef}\left\{\prod_{r_1,r_2} q_{r_1}(v_1)^{\frac{n\Lambda'_1(1,1)}{\Gamma'^{(1)}(1)}\Gamma^{(1)}_{r_1}} q_{r_2}(v_2)^{\frac{n\Lambda'_2(1,1)}{\Gamma'^{(2)}(1)}\Gamma^{(2)}_{r_2}}, v_1^{E_1} v_2^{E_2}\right\}}{\binom{n\Lambda'_1(1,1)}{E_1}\binom{n\Lambda'_2(1,1)}{E_2}},$$

where $\Lambda'_j(1,1) = \sum_{l_1,l_2} l_j \Lambda_{l_1,l_2}$, $\Gamma'^{(j)}(1) = \sum_{r_j} r_j \Gamma^{(j)}_{r_j}$, $j \in \{1,2\}$. *The polynomial* $q_r(v)$ *is defined as*

$$q_r(v) = \frac{(1+v)^r + (1-v)^r}{2}$$

and coef$\{\sum_i F_i D^i, D^j\}$ *is the coefficient of* D^j *in* $\sum_i F_i D^i$.

Proof: The proof can be found in [11]. ∎

Before stating our next result we need the following definition. For a two edge type LDPC ensemble $\{\Lambda, \Gamma^{(1)}, \Gamma^{(2)}\}$ with design rate R_{des} we define the function $\theta(e_1, e_2)$ for $(e_1, e_2) \in \mathcal{E}$ as

$$\begin{aligned}\theta(e_1,e_2) &\triangleq \sum_{l_1,l_2} \Lambda_{l_1,l_2} \log_2(1+u_1^{l_2}u_2^{l_2}) \\ &- \Lambda'_1(1,1)e_1\log_2 u_1 - \Lambda'_2(1,1)e_2\log_2 u_2 \\ &+ \frac{\Lambda'_1(1,1)}{\Gamma'^{(1)}(1)}\sum_{r_1}\Gamma^{(1)}_{r_1}\log_2 q_{r_1}(v_1) - \Lambda'_1(1,1)e_1\log_2 v_1 \\ &+ \frac{\Lambda'_2(1,1)}{\Gamma'^{(2)}(1)}\sum_{r_2}\Gamma^{(2)}_{r_2}\log_2 q_{r_2}(v_2) - \Lambda'_2(1,1)e_2\log_2 v_2 \\ &- \Lambda'_1(1,1)h(e_1) - \Lambda'_2(1,1)h(e_2) - R_{\text{des}}, \end{aligned} \tag{7}$$

where u_1, u_2, v_1, and v_2 are positive solutions to the following equations

$$\frac{v_1}{\Gamma^{(1)\prime}(1)}\sum_{r_1} r_1\Gamma^{(1)}_{r_1}\frac{(1+v_1)^{r_1-1}-(1-v_1)^{r_1-1}}{(1+v_1)^{r_1}+(1-v_1)^{r_1}} = e_1, \tag{8}$$

$$\frac{v_2}{\Gamma^{(2)\prime}(1)}\sum_{r_2} r_2\Gamma^{(2)}_{r_2}\frac{(1+v_2)^{r_2-1}-(1-v_2)^{r_2-1}}{(1+v_2)^{r_2}+(1-v_2)^{r_2}} = e_2, \tag{9}$$

$$\frac{1}{\Lambda'_1(1,1)}\sum_{l_1,l_2}\Lambda_{l_1,l_2} l_1 \frac{u_1^{l_1}u_2^{l_2}}{1+u_1^{l_1}u_2^{l_2}} = e_1, \tag{10}$$

$$\frac{1}{\Lambda'_2(1,1)}\sum_{l_1,l_2}\Lambda_{l_1,l_2} l_2 \frac{u_1^{l_1}u_2^{l_2}}{1+u_1^{l_1}u_2^{l_2}} = e_2, \tag{11}$$

and $h(x)$ is the binary entropy function. The set $\mathcal{E}$ is the set of (e_1, e_2) such that

$$\text{coef}\left\{\prod_{l_1,l_2}(1+u_1^{l_1}u_2^{l_2})^{n\Lambda_{l_1,l_2}}, u_1^{e_1 n\Lambda'_1(1,1)} u_2^{e_2 n\Lambda'_2(1,1)}\right\} \neq 0. \tag{12}$$

In the following theorem, we present a criterion for two edge type LDPC ensembles, which, when satisfied, guarantees that the actual rate is equal to the design rate.

Theorem III.3. *Consider the two edge type LDPC ensemble* $(\Lambda, \Gamma^{(1)}, \Gamma^{(2)})$ *with design rate* R_{des}. *Let* N *be the total number of codewords of a randomly chosen code* G *from this ensemble and let* R_G *be the actual rate of the code* G. *Then*

$$\lim_{n\to\infty}\frac{\log_2(\mathbb{E}[N])}{n} = \sup_{(e_1,e_2)\in\mathcal{E}}\theta(e_1,e_2) + R_{\text{des}},$$

where $\theta(e_1, e_2)$ *and* $\mathcal{E}$ *are defined in (7) and (12). Also, if* $\sup_{(e_1,e_2)\in\mathcal{E}}\theta(e_1,e_2) = 0$, *then for any* $\delta > 0$

$$\lim_{n\to\infty} P\left(R_G \geq R_{\text{des}} + \delta\right) = 0.$$

Proof: By Lemma III.2 and since the number of different E_1, E_2 grows only linearly with n, we have

$$\lim_{n\to\infty}\frac{\log_2(\mathbb{E}[N])}{n} = \sup_{(e_1,e_2)\in\mathcal{E}}\lim_{n\to\infty}\frac{\log_2(\mathbb{E}[N(e_1 n\Lambda'_1(1,1), e_2 n\Lambda'_2(1,1))])}{n},$$

where $e_1 = E_1/(n\Lambda'_1(1,1))$, $e_2 = E_2/(n\Lambda'_2(1,1))$. Using Stirling's approximation for the binomial coefficients and [9, Appendix D] for the coefficient growths in Lemma III.2 we know that

$$\lim_{n\to\infty}\frac{\log_2(\mathbb{E}[N(e_1 n\Lambda'_1(1,1), e_2 n\Lambda'_2(1,1))])}{n} = \inf_{u_1,u_2,v_1,v_2>0}\psi(e_1,e_2,u_1,u_2,v_1,v_2)$$

where $\psi(e_1, e_2, u_1, u_2, v_1, v_2)$ is given by

$$\begin{aligned}&\sum_{l_1,l_2}\Lambda_{l_1,l_2}\log_2(1+u_1^{l_2}u_2^{l_2}) - \Lambda'_1(1,1)e_1\log_2 u_1 \\ &-\Lambda'_2(1,1)e_2\log_2 u_2 + \frac{\Lambda'_1(1,1)}{\Gamma'^{(1)}(1)}\sum_{r_1}\Gamma^{(1)}_{r_1}\log_2 q_{r_1}(v_1) \\ &-\Lambda'_1(1,1)e_1\log_2 v_1 + \frac{\Lambda'_2(1,1)}{\Gamma'^{(2)}(1)}\sum_{r_2}\Gamma^{(2)}_{r_2}\log_2 q_{r_2}(v_2) \\ &-\Lambda'_2(1,1)e_2\log_2 v_2 - \Lambda'_1(1,1)h(e_1) - \Lambda'_2(1,1)h(e_2).\end{aligned}$$

Further, the infimum of ψ with respect to u_1, u_2, v_1, and v_2 is given by solving the following saddle point equations

$$\frac{\partial\psi}{\partial u_1} = \frac{\partial\psi}{\partial u_2} = \frac{\partial\psi}{\partial v_1} = \frac{\partial\psi}{\partial v_2} = 0,$$

which are equivalent to (8) - (11). The second claim of the theorem follows from [6, Lem. 7]. ∎

In the following theorem we state how we can compute the quantity $H(\underline{X}|\underline{S}, \underline{Z})$ appearing in (6).

Theorem III.4. *Consider transmission over BEC-WT(*ϵ_m, ϵ_w*) using a random code* G *from the two edge type LDPC ensemble* $\{\Lambda, \Gamma^{(1)}, \Gamma^{(2)}\}$ *and the coset encoding method.*

Also consider point-to-point communication over a BEC(ϵ_w*) using the two edge type LDPC ensemble* $\{\Lambda, \Gamma^{(1)}, \Gamma^{(2)}\}$. *Assume that the erasure probability* ϵ_w *is above the BP threshold of the ensemble. Let* $\{\Omega, \Phi^{(1)}, \Phi^{(2)}\}$ *be the residual ensemble from the peeling decoder and let* R^r_{des} *be its design rate. If* $\{\Omega, \Phi^{(1)}, \Phi^{(2)}\}$ *satisfies the condition of Theorem III.3, i.e. if the design rate is equal to the rate then*

$$\lim_{n\to\infty}\frac{\mathbb{E}(H_G(\underline{X}|\underline{S}, \underline{Z}))}{n} = \epsilon_w\Lambda(y_1, y_2)R^r_{\text{des}}, \tag{13}$$

where x_1, x_2, y_1, *and* y_2 *are the fixed points of the density evolution equations* (4) *and* (5) *obtained when initializing them with* $x_1^{(1)} = x_2^{(2)} = \epsilon_w$.

Proof: It is easy to show that the conditional entropy in the point-to-point set-up is identical to $H(\underline{X}|\underline{S},\underline{Z})$. The conditional entropy in the point-to-point case is equal to the RHS of (13). This follows from the same arguments as in [6, Thm. 10]. The quantity $\epsilon_w \Lambda(y_1, y_2)$ on the RHS of (13) is the ratio of the number of variable nodes in the residual ensemble to that in the initial ensemble. ■

This gives us the following method to calculate the equivocation of Eve when using two edge type LDPC ensembles for the BEC-WT(ϵ_m, ϵ_w) based on the coset encoding method.

1) If the threshold of the two edge type LDPC ensemble is lower than ϵ_w, calculate the residual degree distribution for the two edge type LDPC ensemble for transmission over the BEC(ϵ_w). Check that the rate of this residual ensemble is equal to the design rate using Theorem III.3 and calculate $H(\underline{X}|\underline{S},\underline{Z})$ using Theorem III.4. If the threshold is higher than ϵ_w, $H(\underline{X}|\underline{S},\underline{Z})$ is trivially zero.
2) If the threshold of the standard LDPC ensemble induced by type one edges is higher than ϵ_w, calculate the residual degree distribution of this ensemble for transmission over the BEC(ϵ_w). Check that its rate is equal to the design rate using [6, Lemma 7] and calculate $H(\underline{X}|\underline{Z})$ using [6, Theorem 10]. If the threshold is higher than ϵ_w, $H(\underline{X}|\underline{Z})$ is trivially zero.
3) Finally calculate $H(\underline{S}|\underline{Z})$ using (6).

IV. Example

Consider the two edge type ensemble

$$\begin{aligned}\Lambda(x,y) =& 0.5572098x^2y^3 + 0.1651436x^3y^3 + \\ & 0.07567923x^4y^3 + 0.0571348x^5y^3 + \\ & 0.043603x^7y^3 + 0.02679802x^8y^3 + \\ & 0.013885518x^{13}y^3 + 0.0294308x^{14}y^3 + \\ & 0.02225301x^{31}y^3 + 0.00886105x^{100}y^3, \\ \Gamma^{(1)}(x) =& \ 0.25x^9 + 0.75x^{10}, \\ \Gamma^{(2)}(x) =& \ x^{12}\end{aligned}$$

for transmission over the BEC-WT($0.5, 0.751164$). The graph induced by type one edges is optimized for the BEC(0.5) using methods from [9], and the graph induced by type two edges is $(3, 12)$ regular. The rate from Alice to Bob is $R_{ab} = 0.25$.

We calculate the residual ensemble $\{\Omega^{(1)}, \Phi^{(1)}\}$ induced by type one edges and the residual two edge type ensemble $\{\Omega, \Phi^{(1)}, \Phi^{(2)}\}$ when transmitting over BEC(ϵ_w). We check using [6, Lemma 7] that the rate is equal to the design rate for $\{\Omega^{(1)}, \Phi^{(1)}\}$.

In Figure 3 we plot $\theta(e_1, e_2)$ for $(\Omega, \Phi^{(1)}, \Phi^{(2)})$. Since the maximum of $\theta(e_1, e_2)$ over $\mathcal{E}$ is zero, we obtain by Theorem III.3 that the rate is equal to the design rate. In this case we can calculate the equivocation of Eve and find it to be 0.24999999, which is very close to the rate from Alice to Bob. Thus this ensemble achieves the point $(R_{ab}, R_e) = (0.25, 0.24999999)$ in the rate equivocation region. The secrecy capacity is 0.251164, so this code has rate close to the secrecy capacity, and it is very close to achieving perfect secrecy.

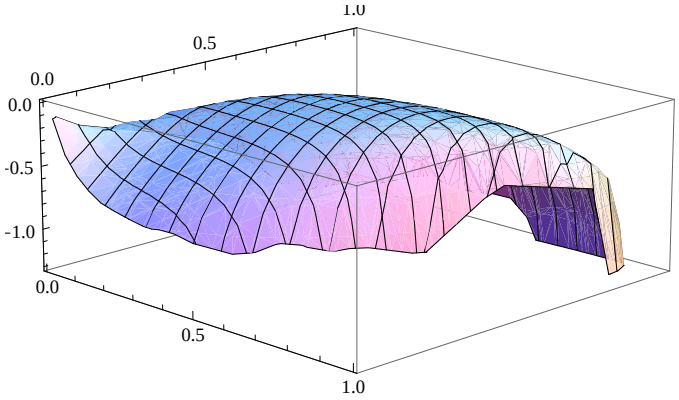

Fig. 3. Plot of $\theta(e_1, e_2)$ for the residual ensemble $(\Omega, \Phi^{(1)}, \Phi^{(2)})$.

This example demonstrates that there are simple ensembles with very good secrecy performance.

V. Conclusions

We generalize the method of [6] to two edge type LDPC codes in order to measure the security performance when using two edge type LDPC codes for the binary erasure wiretap channel. We find that relatively simple ensembles have very good secrecy performance.

References

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

[2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[3] 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.

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

[5] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Two edge type LDPC codes for the wiretap channel," in *Signals, Systems and Computers, 2009 Conference Record of the Forty-Third Asilomar Conference on*, 2009, pp. 834 –838.

[6] C. Méasson, A. Montanari, and R. Urbanke, "Maxwell Construction: The Hidden Bridge Between Iterativew and Maximum a Posteriori Decoding," *Information Theory, IEEE Transactions on*, vol. 54, no. 12, pp. 5277–5307, 2008.

[7] V. Rathi and I. Andriyanova, "Some Results on MAP Decoding of Non-Binary LDPC Codes over the BEC," *Accepted to IEEE Transactions on Information Theory*, 2010.

[8] 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.

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

[10] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. A. Spielman, "Efficient erasure correcting codes," *Information Theory, IEEE Transactions on*, vol. 47, no. 2, pp. 569–584, Feb. 2001.

[11] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance Analysis and Design of Two Edge Type LDPC Codes for the BEC Wiretap Channel," *ArXiv e-prints*, Sept. 2010.

[12] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman, "Improved low-density parity-check codes using irregular graphs," *Information Theory, IEEE Transactions on*, vol. 47, no. 2, pp. 585 –598, Feb. 2001.