Strong and Weak Secrecy in Wiretap Channels

Arunkumar Subramanian†, Ananda T. Suresh*, Safitha Raj*,
Andrew Thangaraj*, Matthieu Bloch† and Steven McLaughlin†
* Department of Electrical Engineering, Indian Institute of Technology, Madras, Email: andrew@iitm.ac.in
† School of Electrical and Computer Engineering, Georgia Institute of Technology, USA and GT-CNRS UMI 2958, France
Email: arunkumar@gatech.edu, matthieu.bloch@ece.gatech.edu, swm@ece.gatech.edu

***Abstract*—In the wiretap channel model, symbols transmitted through a main channel to a legitimate receiver are observed by an eavesdropper across a wiretapper's channel. The goal of coding for wiretap channels is to facilitate error-free decoding across the main channel, while ensuring zero information transfer across the wiretapper's channel. Strong secrecy requires the total information transfer to the eavesdropper to tend to zero, while weak secrecy requires the per-symbol information transfer to go to zero. In this paper, we will consider coding methods for binary wiretap channels with a noiseless main channel and a BEC or a BSC wiretapper's channel. We will provide conditions and codes that achieve strong and weak secrecy for the BEC case. For the BSC case, we will discuss some existing coding methods and develop additional criteria for secrecy.**

I. Introduction

Secrecy systems have been modeled using wiretap channels since Wyner introduced them in 1975 [1]. In the classic wiretap system, Alice tries to communicate with Bob through a main channel and Eve is listening to this communication via a wiretap channel. The security of such a system can be characterized using different metrics. One such metric is the mutual information between the transmitter and the eavesdropper. The metric based on mutual information itself can be defined in strong and weak sense as the message length becomes very large.

Let X^n be the n-length encoded version of a nR-bit message transmitted by Alice and let Z^n denote Eve's information. The message is said to be strongly secure as the message length n becomes very large, if $\lim_{n\to\infty} I(X^n, Z^n) = 0$, and weakly secure if $\lim_{n\to\infty} \frac{I(X^n,Z^n)}{n} = 0$. The *secrecy capacity* is the maximum rate R achievable over the main channel under the secrecy condition for the wiretapper's channel. Surprisingly, both strong and weak secrecy requirements result in the same secrecy capacity [2], [3].

Coding for wiretap channels has not attracted much research attention, except for a few efforts such as [4]–[9], which work with weak secrecy. Coding for strong secrecy has not received any attention at all, except for the multi-round method suggested and studied in [2], which relies on the equivalence of key-generation with one-way communication and coding for the wiretap channel.

In this work, we revisit the LDPC-based coset coding scheme of [6] for the binary erasure wiretap channel and the binary symmetric wiretap channel. It turns out that this scheme achieves strong secrecy on the erasure wiretap channel provided the block error probability for the sequence of LDPC codes decays faster than $\frac{1}{n}$ with the block length n in a binary erasure channel. A careful stopping set analysis of small-cycle-free LDPC ensembles (for a large enough girth and minimum left degree), using the method of [10], shows that the probability of block error under iterative decoding decays as $\mathcal{O}(\frac{1}{n^2})$, whenever the erasure probability is lower than a certain threshold.

For the binary symmetric wiretap channel, we derive conditions on the weight distributions of LDPC codes that result in strong and weak secrecy. The main method used here is the MacWilliams identity relating a code's weight distribution to its dual's weight distribution. We compute thresholds below which the codes achieve secrecy and compare with degraded erasure channel thresholds following [7]. In the process, we also show that dual of codes that have good performance over a binary symmetric channel can be used in coset coding for secrecy in a binary symmetric wiretap channel. This is a result similar to the coset coding result for an erasure wiretap channel.

The rest of the paper is organized as follows. In Section II, we present results for the binary erasure wiretap channel establishing connections between strong secrecy and the decay of probability of block error with code length. A study of the secrecy thresholds for different LDPC ensembles and a comparison with secrecy capacity are also presented. In Section III, we present results for the binary symmetric wiretap channel. Some concluding remarks are made in Section IV

II. Binary Erasure Wiretap Channel

The binary erasure wiretap channel, denoted by BEWC(ϵ), is illustrated in Fig. 1. The channel between the legitimate parties is noiseless while the eavesdropper's channel is a binary erasure channel with erasure probability ϵ (denoted BEC(ϵ)). The secrecy capacity of this wiretap channel is $C_s = \epsilon$ [1].

The "coset coding" scheme to communicate secretly over this channel, proposed in [5], is the following. Prior to transmission, Alice and Bob agree on a $(n, n-k)$ code C with parity check matrix $\mathbf{H}$. The coset of C with syndrome s^k is denoted by $C(\mathsf{s}^k) = \{\mathsf{x}^n \in \{0,1\}^n : \mathsf{s}^k = \mathsf{x}^n\mathbf{H}^T\}$. To transmit a message M of k bits, Alice transmits a codeword

This work was supported in part by the Reliance TCOE at IIT Madras.

978-1-4244-6746-4/10/$26.00 ©2010 IEEE

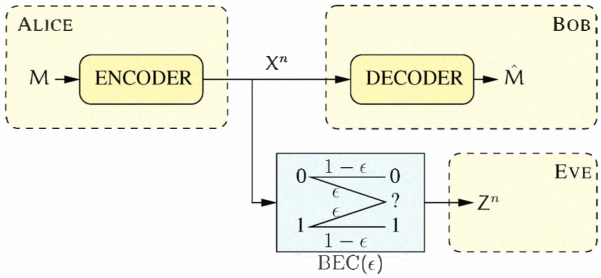

Fig. 1. Binary erasure wiretap channel.

X^n chosen uniformly at random in $C(M)$. Bob decodes his received codeword X^n by forming the syndrome $X^n\mathbf{H}^T$.

The following theorem due to Ozarow and Wyner connects the equivocation of the eavesdropper to algebraic properties of the generator matrix.

Theorem 1 ([5]). *Let C be a $(n, n-k)$ code with generator matrix $\mathbf{G} = [g_1, \ldots, g_n]$, where g_i represents the i-th column of $\mathbf{G}$. Let z^n be an observation of the eavesdropper with μ unerased position given by $\{i : z_i \neq ?\} = \{i_1, \ldots, i_\mu\}$. Let $\mathbf{G}_\mu = [g_{i_1} \ldots g_{i_\mu}]$. Then, $\mathbb{H}(M|z^n) = k$ iff $\mathbf{G}_\mu$ has full rank.*

Based on Theorem 1, we can now connect the rate of convergence of $\mathbb{I}(M; Z^n)$ to the probability that a submatrix of $\mathbf{G}$ has full rank.

Lemma 1. *Let G_μ be the submatrix of $\mathbf{G}$ corresponding to the unerased positions in Z^n. Let p_{nf} be the probability that G_μ is not full rank. Then, a coset coding scheme operates with strong secrecy if the probability p_{nf} is such that $p_{nf} = \mathcal{O}(\frac{1}{n^\alpha})$ for some $\alpha > 1$.*

Proof: We can lower bound $\mathbb{H}(M|Z^n)$ as

$$\begin{aligned}\mathbb{H}(M|Z^n) &\geq \mathbb{H}(M|Z^n, \mathrm{rank}(G_\mu)) \\ &\geq \mathbb{H}(M|Z^n, G_\mu \text{ is full rank})\, \mathbb{P}[G_\mu \text{ is full rank}] \\ &= k(1-p_{nf}) = k - R_s n p_{nf}\end{aligned}$$

If $p_{nf} = \mathcal{O}(\frac{1}{n^\alpha})$, then $\mathbb{I}(M; Z^n) = k - \mathbb{H}(M|Z^n) \leq \mathcal{O}(\frac{1}{n^{\alpha-1}})$, which can be made arbitrary small for n sufficiently large and $\alpha > 1$. ∎

Let $C^n(\lambda, \rho)$ be an LDPC ensemble with n variable nodes, left edge degree distributions $\lambda(x) = \sum_{i\geq 1} \lambda_i x^{i-1}$ and right node degree distribution $\rho(x) = \sum_{i\geq 1} \rho_i x^{i-1}$ [11, §3.4] with possibly some expurgations. The degree distributions $\lambda(x), \rho(x)$ are from an edge perspective, that is λ_i is the fraction of edges connected to a variable node of degree i and ρ_j is similarly defined.

Let $P_e^{(n)}(\epsilon)$ denote the probability of block error for codes from $C^n(\lambda, \rho)$ over BEC(ϵ) under iterative decoding. An important interpretation of $P_e^{(n)}(\epsilon)$ is the following: for a parity-check matrix H with degree distribution (λ, ρ), $1 - P_e^{(n)}(\epsilon)$ is a lower bound on the probability that erased columns of H (over a BEC(ϵ)) form a full-rank submatrix. Using this interpretation and results from [6], we have the following immediate corollary of Lemma 1.

Corollary 1. *If there exists $\epsilon^* > 0$ such that $P_e^{(n)}(\epsilon) = \mathcal{O}(\frac{1}{n^\alpha})$, $(\alpha > 1)$ for $\epsilon < \epsilon^*$, then the dual of a code from $C^n(\lambda, \rho)$ used in a coset coding scheme provides strong secrecy over a* BEWC(ϵ) *for $\epsilon > 1 - \epsilon^*$.*

It is immediately clear that we will have $\epsilon^* \leq \epsilon_{\text{th}}$, where ϵ_{th} is the erasure threshold for the ensemble over LDPC codes [11]. As noted in [6], when $\epsilon \leq \epsilon_{\text{th}}$ we have weak secrecy.

Next, we define the sub-ensemble of Tanner graphs [11] whose girth is at least $2k$ for some integer $k \geq 2$ which does not change with the block length n. We denote the ensemble of all Tanner graphs by $\mathcal{G}(n, \lambda, \rho)$ and the sub-ensemble of girth $\geq g$ graphs by $\mathcal{G}_g(n, \lambda, \rho)$. We associate i *sockets* to each node of degree i. An edge in a Tanner graph is an unordered pair containing one bit node socket and one check node socket. A Tanner graph with $|E|$ edges has $|E|$ sockets on each side. Therefore, the size of the ensemble equal to the number of permutation of the check node sockets, which is $|E|!$.

Let $P_B^{\text{IT}}(C, \epsilon)$ be the probability of block error when the code C is transmitted over BEC(ϵ) and iteratively decoded. We define [10]

$$\epsilon_{\text{ef}} \triangleq \sup\left\{\epsilon : \max_{\alpha\in[0,\epsilon]} \left(\gamma(\alpha) + (1-\alpha)h(\tfrac{\epsilon-\alpha}{1-\alpha}) - h(\epsilon)\right) \leq 0\right\}$$

where $h(x)$ is the binary entropy function calculated using natural logarithms and $\gamma(\alpha)$ is the normalized stopping set distribution computed as shown in [10]. Note that $\gamma(\alpha)$ and ϵ_{ef} are calculated over the entire ensemble $\mathcal{G}(n, \lambda, \rho)$ instead of the girth-restricted ensemble. The following theorem, proved in [12], shows the rate of decay for the block error probability averaged over the girth restricted ensemble.

Theorem 2. *For a randomly chosen $C \in \mathcal{G}_{2k}(n, \lambda, \rho)$, with minimum variable node degree $l_{\min}$, we have*

$$\mathbb{E}(P_B^{\text{IT}}(C, \epsilon)) = \mathcal{O}\left(\frac{1}{n^{\lceil \frac{l_{\min}}{2} k\rceil - k}}\right)$$

for $\epsilon < \epsilon_{\text{ef}}$. In the limits of small ϵ and large n

$$\mathbb{E}(P_B^{\text{IT}}(C, \epsilon)) = \mathcal{O}\left(\frac{\epsilon^k}{n^{\lceil \frac{l_{\min}}{2} k\rceil - k}}\right)$$

From the above theorem, the average block error probability in the girth-$2k$ ensemble decays faster than $\frac{1}{n^2}$ for $l_{\min} > 2$ and $k > 2$. This corresponds to LDPC ensembles with a minimum bit node degree of at least 3 and girth at least 6. By corollary 1, the duals of these LDPC codes achieve strong secrecy over a BEWC of erasure probability $1 - \epsilon_{\text{ef}}$.

For LDPC degree distributions with minimum degree ≥ 3 and a given rate, we examine the values of ϵ for which weak secrecy according to [6] and strong secrecy using girth restricted ensembles according to Theorem 2 are achieved. The thresholds ϵ_{th} and ϵ_{ef} are shown in Fig. 2 for various regular and irregular codes of rate-1/2 taken from [13].

Fig. 2 reveals that codes that are optimized to achieve large erasure thresholds ϵ_{th} result in a low ϵ_{ef} i.e. achieve strong secrecy only for large values of ϵ. For example, the (3, 6) regular distribution with $\epsilon_{\text{th}} = 0.429$ and $\epsilon_{\text{ef}} = 0.366$ achieves

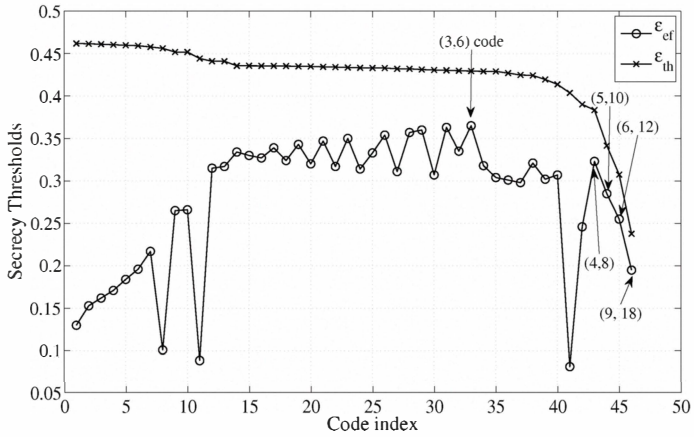

Fig. 2. Erasure thresholds (ϵ_{th} and ϵ_{ef}) for various regular and irregular rate-1/2 codes.

a secret communication rate of 0.5 with weak secrecy when $\epsilon \in (0.571, 0.634]$ and with strong secrecy when $\epsilon > 0.634$. On the other hand, the threshold-optimized [13] distribution pair $\lambda(x) = 0.5473x^2 + 0.2950x^{18} + 0.0632x^{69} + 0.0945x^{82}$, $\rho(x) = x^9$ with $\epsilon_{\text{th}} = 0.460$ and $\epsilon_{\text{ef}} = 0.171$ achieves weak secrecy for $\epsilon = (0.54, 0.829]$ and strong secrecy for $\epsilon > 0.829$.

III. Binary Symmetric Wiretap Channel

We define the binary symmetric wiretap channel, denoted BSWC(p), to be the wiretap channel where the main channel is a noiseless link and the wiretapper's channel is a Binary Symmetric Channel (BSC) with transition probability p. Alice codes her messages using cosets of an $(n, n-k)$ linear block code $\mathcal{C}$. Alice can send 2^k messages, where each message corresponds to a particular coset of $\mathcal{C}$.

Let S^k denote the secret message, X^n the transmitted word and Z^n the received word of Eve. Since the wiretapper's channel is a BSC, we have $Z^n = X^n + E^n$, where $E^n = [E_1\ E_2 \cdots E_n]$ and $E_i \in \{0,1\}$ are *iid* with $\text{Prob}\{E_i = 1\} = p$. Let the cosets of C be $C_{w_i} = w_i + C$, where w_i ($i \in \{1, 2, \cdots, 2^k\}$) denote the coset leaders with w_1 being the all-zero vector and $C = C_{w_1}$.

It can be shown that

$$I(Z^n; S^k) = H(Z^n) - H(Z^n|S^k), \tag{1}$$
$$= k - H_{\text{code}}(p), \tag{2}$$

where $H_{\text{code}}(p) = -\sum_{i=1:2^k} P(E^n \in C_{w_i}) \log_2 P(E^n \in C_{w_i})$. The condition of security, viz $I(Z^n, S^k) \to 0$, translates as $H_{\text{code}}(p) \to k$ or $P(C_{w_i}) \to 2^{-k}$.

Let A_j and A'_j denote the number of words of weight j in the code C and the dual $C^\perp$, respectively. Using the arguments in [6] using MacWilliams identities, for $p = (1-\beta)/2$, we can show that

$$P(C_{w_i}) = 2^{-k}\left(1 + \delta_i(n)\right), \tag{3}$$

where $\delta_1(n) = \sum_{j=1:n} A'_j \beta^j$ and $\delta_1(n) \geq |\delta_i(n)|$ for all i. So, we have

$$H_{\text{code}}\left(\frac{1-\beta}{2}\right) = -\sum_{i=1:2^k} 2^{-k}\left(1+\delta_i(n)\right)\log\left(2^{-k}\left(1+\delta_i(n)\right)\right),$$
$$\geq k\left(1+\delta_1(n)\right) - \left(1+\delta_1(n)\right)\log\left(1+\delta_1(n)\right). \tag{4}$$

This implies

$$\lim_{n\to\infty} I(Z^n; S^k) \leq R \lim_{n\to\infty} n\delta_1(n) + \lim_{n\to\infty}\left(1+\delta_1(n)\right)\log\left(1+\delta_1(n)\right), \tag{5}$$

where the secrecy rate $R = k/n$ is assumed to be constant as $n \to \infty$. For strong secrecy, mutual information $I(Z^n; S^k)$ should go to zero. This condition translates in terms of $\delta_1(n)$ (from (5)) as, $\lim_{n\to\infty} n\delta_1(n) \to 0$. The condition for weak secrecy in terms of $\delta_1(n)$ is therefore, $\lim_{n\to\infty} \delta_1(n) \to 0$.

In particular, we have weak secrecy in a BSWC(p) for $p > (1-\beta^*)/2$, if for $\beta < \beta^*$,

$$\lim_{n\to\infty} \sum_{j=1:n} A'_j \beta^j \to 0. \tag{6}$$

We have strong secrecy for $p > (1-\beta^*)/2$, if $\sum_{j=1:n} A'_j \beta^j = \mathcal{O}(1/n^2)$ for $\beta < \beta^*$.

A. Secrecy Threshold for Regular LDPC Codes

We consider the specific case of regular LDPC ensembles, and use results from the literature on average weight distributions to estimate a suitable β^*. Let the ensemble $\mathcal{C}(n, x^{c-1}, x^{d-1})$ be a regular LDPC ensemble with variable node degree c and check node degree d. The average weight distribution of $\mathcal{C}(n, x^{c-1}, x^{d-1})$ is given by ([14] and references therein),

$$\overline{A}_i = \binom{n}{i} \frac{\text{coef}\left(\left(\sum_{l=0:\lfloor \frac{d}{2} \rfloor} \binom{d}{2j} x^{2j}\right)^{n\frac{c}{d}}, x^{ic}\right)}{\binom{nc}{ic}} \tag{7}$$

where $\overline{A}_i$ is the average number of codewords of weight i in $\mathcal{C}(n, x^{c-1}, x^{d-1})$. The asymptotic average weight spectrum of $\mathcal{C}(n, x^{c-1}, x^{d-1})$ is defined as

$$r(\alpha) = \lim_{n\to\infty} r_n(\alpha) = \frac{\log \overline{A}_{\lfloor \alpha n \rfloor}}{n}. \tag{8}$$

For the regular LDPC ensemble, $r(\alpha)$ is derived in [14] to be

$$r(\alpha) = h(\alpha) + c\left(-h(\alpha) + \frac{1}{d}\log \inf_{x>0} \frac{\sum_{j=0:\lfloor \frac{d}{2} \rfloor} \binom{d}{2j} x^{2j}}{x^{\alpha d}}\right). \tag{9}$$

Suppose a code C randomly chosen from $\mathcal{C}(n, x^{c-1}, x^{d-1})$ is used as the code $C^\perp$ in the coset coding scheme over a

BSWC(p). Secrecy will depend on the limit of the following average of $\delta_1(n)$, defined as

$$\overline{\delta}_1 = \lim_{n\to\infty} \sum_{j=1:n} \overline{A}_j \beta^j, \tag{10}$$

$$= \lim_{n\to\infty} \left(\sum_{j=1:w} \overline{A}_j \beta^j + \sum_{j=(w+1):n} \overline{A}_j \beta^j \right), \tag{11}$$

where $w = (\lfloor \alpha_0 n \rfloor - 1)$ and α_0 is the smallest fraction for which $r(\alpha_0) > 0$ and $r(\alpha) < 0$ for $0 < \alpha < \alpha_0$. Substituting (8) in (11), we get

$$\overline{\delta}_1 = \lim_{n\to\infty} \sum_{j=1:(\lfloor \alpha_0 n \rfloor - 1)} e^{n r_n(\frac{j}{n})} \beta^j + \sum_{j=\lfloor \alpha_0 n \rfloor : n} e^{-j\left(-\frac{r_n(\frac{j}{n})}{\frac{j}{n}} - \log\beta\right)}. \tag{12}$$

Let T_1 and T_2 be the first and second terms in the RHS above. We have

$$T_1 = \sum_{j=1:(\lfloor \alpha_0 n \rfloor - 1)} e^{n r_n(\frac{j}{n})} \beta^j, \tag{13}$$

$$= \sum_{j=1:(\lfloor \delta n \rfloor - 1)} \overline{A}_j \beta^j + \sum_{j=\lfloor \delta n \rfloor : (\lfloor \alpha_0 n \rfloor - 1)} e^{n r_n(\frac{j}{n})} \beta^j, \tag{14}$$

$$\leq \sum_{j=1:(\lfloor \delta n \rfloor - 1)} \overline{A}_j + \sum_{j=\lfloor \delta n \rfloor : (\lfloor \alpha_0 n \rfloor - 1)} e^{n r_n(\frac{j}{n})}, \tag{15}$$

$$= \sum_{j=1:(\lfloor \delta n \rfloor - 1)} \overline{A}_j + O\left(n e^{n(\max_{\alpha\in[\delta,\alpha_0]} r(\alpha) + \epsilon)} \right). \tag{16}$$

In order to approximate the first term in T_1, we bound the expression for $\overline{A}_j$. The average number of codewords of weight i in the LDPC regular ensemble $\mathcal{C}(n, x^{c-1}, x^{d-1})$ can be viewed in terms of selection of check node sockets. Each check node has d sockets and there are $m = nc/d$ check nodes. The term in the numerator of (7), $S_{ic} = \text{coef}\left(\left(\sum_{j=0:\lfloor \frac{d}{2} \rfloor} \binom{d}{2j} x^{2j} \right)^{n\frac{c}{d}}, x^{ic} \right)$ is the number of ways of choosing $n_i = ic$ check node sockets out of all check node sockets such that an even number of sockets are picked from each check node. In [10], an upper bound is derived for the term $S'_{ic} = \text{coef}\left(\left((1+x)^d - dx \right)^{n\frac{c}{d}}, x^{ic} \right)$ which is the number of ways of choosing n_i check node sockets out of all check node sockets such that no check node is selected exactly once. The bound on S'_{ic} is applicable to S_{ic} as well, since $S_{ic} \leq S'_{ic}$. As n increases, the highest order term in S'_{ic} will correspond to the situation when the sockets are distributed among $\lfloor n_i/2 \rfloor$ check nodes (where we will have the term $\binom{m}{\lfloor \frac{n_i}{2} \rfloor}$). Looking at S_{ic}, we observe that the highest order term is identical. Thus, the difference between S_{ic} and S'_{ic} is only in lower order terms, and as n tends to ∞ the order of decrease in n of both S_{ic} and S'_{ic} is equal. Thus from [10],

$$\sum_{j=1:(\lfloor \delta n \rfloor - 1)} \overline{A}_j = O\left(\frac{1}{n^{\lceil \frac{c}{2} \rceil - 1}} \right) \tag{17}$$

for $c > 2$ and sufficiently small δ.

The first term in T_1 can be approximated as in (17), and it converges to zero if $c > 2$. The second term in T_1 also converges to zero as n tends to ∞ since $r(\alpha) < 0 \ \forall \ \alpha \in [\delta, \alpha_0]$. Thus the term T_1 converges to zero as n tends to ∞.

$$T_2 = \sum_{j=\lfloor \alpha_0 n \rfloor : n} e^{-j\left(-\frac{r_n(\frac{j}{n})}{\frac{j}{n}} - \log\beta\right)}, \tag{18}$$

$$\leq \sum_{j=\lfloor \alpha_0 n \rfloor : n} e^{-j(-\gamma_t - \log\beta)} \quad \text{with} \quad \gamma_t = \max_{\alpha} \left(\frac{r(\alpha)}{\alpha} \right), \tag{19}$$

$$\leq \sum_{j=\lfloor \alpha_0 n \rfloor : n} e^{-j(\epsilon)}, \tag{20}$$

$$\leq \frac{1}{1 - e^{-\epsilon}} e^{-\lfloor \alpha_0 n \rfloor \epsilon}. \tag{21}$$

As n tends to ∞, $\lfloor \alpha_0 n \rfloor$ also tends to ∞. Thus, the term T_2 will also converge to 0 as n tends to ∞ for $\epsilon > 0$ and $\beta < \beta^* = e^{-\gamma_t}$. This means that dual of regular LDPC codes with $c > 2$ will be weakly secure over a BSWC(p), whenever $p > p^* = (1 - e^{-\gamma_t})/2$.

In fact, if $c > 4$ both nT_1 and nT_2 also converge to zero as n tends to ∞ and $\beta < \beta^* = e^{-\gamma_t}$. Thus, dual of regular LDPC codes with $c > 4$ are strongly secure over a BSWC(p), whenever $p > p^* = (1 - e^{-\gamma_t})/2$.

B. Thresholds and Comparisons

In Fig. 3, we compare the secrecy thresholds of regular LDPC codes over a BSWC(p) and compare with using codes that are secure over a BEWC. Since the BSC with cross-over probability $p < 1/2$ is physically degraded with respect to a BEC with erasure probability $2p$, a code which is secure over a BEWC(ϵ) for $\epsilon > \epsilon_0$ will be secure over a BSWC(p) with $p > p_0 = \epsilon_0/2$.

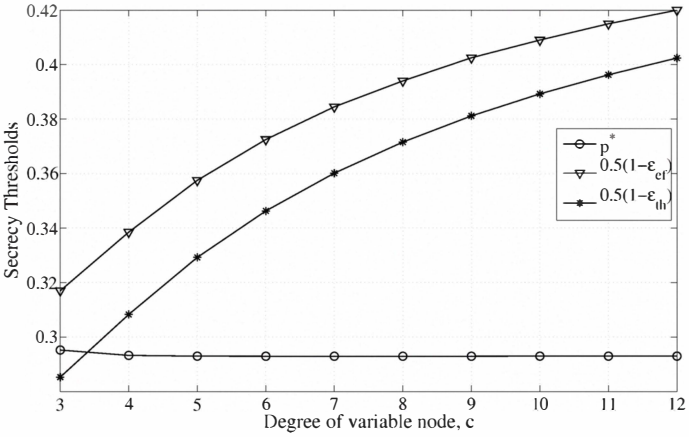

Fig. 3. Secrecy thresholds for regular, rate-1/2 LDPC codes.

We see that the direct BSWC secrecy threshold is better than the BEC-degraded threshold for all cases, except $c = 3$. The difference is significantly higher for larger c.

In Fig. 4, the same comparison is done for LDPC ensembles with different rates and fixed c value, $c = 5$. The BSWC threshold is found to be better than BEC-degraded threshold for all rates considered.

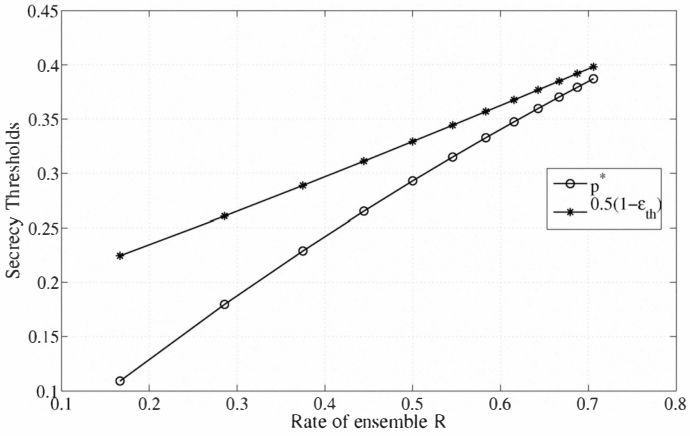

Fig. 4. Secrecy thresholds for regular LDPC ensembles with c = 5.

IV. Conclusion and future directions

In this work, we have shown that duals of LDPC codes with girth greater than 4 and minimum left degree at least 3 achieve strong secrecy on the binary erasure wiretap channel. For the binary symmetric wiretap channel, we derive secrecy thresholds for LDPC codes and show that duals of regular LDPC codes with left degree greater than 4 achieve strong secrecy. The constraint on the dual code is in the form of a union bound for ML probability of error for the code over a BSC. This indicates that the dual of a code which is 'good' in the conventional sense (probability of ML decoding error tends to zero at high block length), is secure over a BSWC. This fact has been observed before for the BEC wiretap channel.

References

[1] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, October 1975.

[2] U. M. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," in *Advances in Cryptology - Eurocrypt 2000*, Lecture Notes in Computer Science. B. Preneel, 2000, p. 351.

[3] I. Csiszár, "Almost Independence and Secrecy Capacity," *Problems of Information Transmission*, vol. 32, no. 1, pp. 40–47, January-March 1996.

[4] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized Privacy Amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, November 1995.

[5] L. H. Ozarow and A. D. Wyner, "Wire Tap Channel II," *AT&T Bell Laboratories Technical Journal*, vol. 63, no. 10, pp. 2135–2157, December 1984.

[6] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC Codes to the Wiretap Channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[7] R. Liu, Y. Liang, H. V. Poor, and P. Spasojević, "Secure Nested Codes for Type II Wiretap Channels," in *Proceedings of IEEE Information Theory Workshop*, Lake Tahoe, California, USA, September 2007, pp. 337–342.

[8] G. Cohen and G. Zemor, "Syndrome-Coding for the Wiretap Channel Revisited," in *Proc. IEEE Information Theory Workshop*, Chengdu, China, October 2006, pp. 33–36.

[9] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using Polar codes," in *Proc. IEEE ISIT2010*, Austin, Texas, USA, June 2010.

[10] A. Orlitsky, K. Viswanathan, and J. Zhang, "Stopping set distribution of LDPC code ensembles," *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 929 –953, march 2005.

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

[12] A. T. Suresh, A. Subramanian, A. Thangaraj, M. Bloch, and S. McLaughlin, "Strong Secrecy for Erasure Wiretap Channels," *'to be presented at the IEEE Information Theory Workship (ITW) 2010, Dublin, Ireland.*

[13] R. Urbanke and A. Amraoui. (2010, Jun.) LDPCOPT. [Online]. Available: http://ipgdemos.epfl.ch/ldpcopt/

[14] D. Burshtein and G. Miller, "Asymptotic Enumeration Methods for Analyzing LDPC Codes," *IEEE Transactions on Information Theory*, vol. 50, pp. 1115–1131, 2004.