Wiretap Channel II with a Noisy Main Channel

Mohamed Nafea and Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802.
msn139@psu.edu *yener@engr.psu.edu*

***Abstract*—In this paper, a wiretap channel where the transmitter and receiver communicate through a discrete memoryless channel, and the eavesdropper (Eve) has perfect access to a fixed fraction of transmitted symbols (of its choosing) is considered. An outer bound for the rate-equivocation region of the channel, for all such fractions, is derived. An achievable scheme, which provides an inner bound for the rate-equivocation region, is proposed. The achievability is established by defining a class of good codebooks for which there exists a good partition that achieves the required level of equivocation no matter what subset of symbols Eve chooses. It is shown that, for a uniform input distribution, the probability of this class of good codes approaches 1 as the block length increases. This generalizes the wiretap II model to one with a noisy main channel.**

I. Introduction

Wyner's wiretap channel (WTC) models a legitimate transmitter (Alice) and a receiver (Bob) communicating through a discrete memoryless channel (DMC), referred to as the main channel, and an external eavesdropper (Eve) overhearing the legitimate communication through a cascaded second DMC, referred to as the eavesdropper's channel [1]. Reference [2] has subsequently generalized this model to a not necessarily degraded memoryless wiretap channel.

Reference [3] introduced wiretap channel II (WTC-II), in which the legitimate communication takes place over a noiseless main channel, and Eve has a perfect access to μ bits (of its own choice) of the length-n binary codeword. Authors in [3] derived an outer bound for the rate-equivocation region of the WTC-II, and proved its tightness by considering the binary code $\mathcal{C}_0 = \{0,1\}^n$, and showing the existence of a good partition of $\mathcal{C}_0$ which results in the desired lower bound for equivocation at Eve. Besides deriving the capacity-equivocation region for the WTC-II model, reference [3] proposed a randomized coset coding scheme, where the partition of $\mathcal{C}_0$ corresponds to a group code and its cosets, and showed that it achieves the capacity-equivocation region. This result has spurred a considerable amount of research on practical coding design for secure communication, see for example [4]–[6]. In [6], the WTC with noiseless main channel and binary-input symmetric-output memoryless eavesdropper channel, is considered as type-II wiretap channel. Reference [7] studied a variation of the WTC-II model in [3], where Eve not only noiselessly overhears a subset of the transmitted bits, but also modifies (or corrupts) the bits, so that Bob receives a corrupted version of Alice's codeword.

In this paper, we consider a WTC with a finite input alphabet, a discrete memoryless main channel, and where Eve noiselessly observes μ symbols (of its choosing) of the length-n transmitted codeword, where $\mu = \alpha n$ and $0 \leq \alpha \leq 1$. We first derive an outer bound for the rate-equivocation region of the channel, for $0 \leq \alpha \leq 1$. Next, we propose an achievable scheme which extends the random partitioning argument in [3] constructed for the one codebook $\mathcal{C}_0$ that contains all possible codewords and has all of its components independently and identically distributed, to a random coding argument, which is exploited to guarantee reliable communication over the discrete memoryless main channel. Note that Eve's capability of choosing the positions of the symbols it observes results in an eavesdropper channel with memory, and hence the results of the original WTC [1] do not specialize to the performance of the model at hand. In the remainder of the paper, Sections II, III describe the channel model and main result. Sections IV and V provide outer and inner bounds for the rate-equivocation region of the channel. Section VI concludes the paper.

Notation: $|.|$ denotes the cardinality or the absolute value, when used for a set or a real number, respectively. Vectors are denoted by bold lower-case superscripted letters, and their components are denoted by lower-case subscripted letters. A similar convention, but with upper case letters, is used for random vectors and their components. The vector's superscript is dropped when its dimension is clear from the context.

II. Channel Model

We consider a wiretap channel II (WTC-II) with a discrete memoryless main channel, see Fig. 1. The transmitter (Alice) wishes to reliably transmit a message W to the receiver (Bob), and to keep it secret from the eavesdropper (Eve). The message W is uniformly drawn from $\mathcal{W} = \{1, 2, \cdots, 2^k\}$. The encoder at Alice $f_{(k,n)} : \mathcal{W} \mapsto \mathcal{X}^n$ maps the message $W \in \mathcal{W}$ to the transmitted codeword $\mathbf{X}^n \in \mathcal{X}^n$. The mapping $f_{(k,n)}$ is allowed to be stochastic. Alice-Bob channel is a discrete memoryless channel (DMC) with a finite input alphabet $\mathcal{X}$, finite output alphabet $\mathcal{Y}$, and probability distribution $p_{Y|X}(y|x)$ for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. The decoder at Bob, $g_{P_e} : \mathcal{Y}^n \mapsto \mathcal{W}$, which observes $\mathbf{Y}^n \in \mathcal{Y}^n$ and outputs an estimate $\hat{W}$ of the transmitted message, is parametrized by P_e, where

$$P_e = \Pr\{\hat{W} \neq W\} = \frac{1}{2^k} \sum_{w=1}^{2^k} \Pr\{\hat{W} \neq w | W = w\}. \quad (1)$$

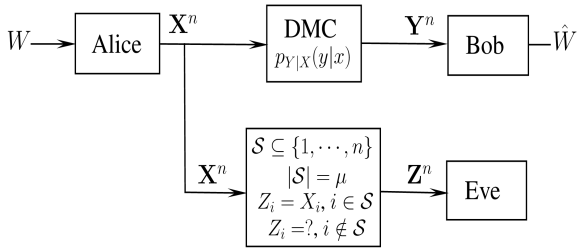

Fig. 1. Wiretap Channel II with a discrete memoryless main channel.

Eve can noiselessly observe a subset, of her own choice, of the n transmitted symbols, $\mathbf{X}^n$. In particular, Eve chooses $\mathcal{S} \subseteq \{1, 2, \cdots, n\}$ with $|\mathcal{S}| = \mu \leq n$, and observes $\mathbf{Z}^n = [Z_1\ Z_2\ \cdots\ Z_n]$, where

$$Z_i = \begin{cases} X_i, & \text{if } i \in \mathcal{S} \\ ?, & \text{otherwise.} \end{cases} \tag{2}$$

Given Eve's choice of the subset $\mathcal{S}$, the equivocation at Eve is measured by $H(W|\mathbf{Z}^n)$. In order to assure the required level of secrecy at Eve, the encoding scheme has to be designed to maximize the equivocation

$$\Delta = \min_{\mathcal{S}:|\mathcal{S}|=\mu} H(W|\mathbf{Z}^n), \tag{3}$$

so that the equivocation at Eve is at least Δ, no matter what subset $\mathcal{S}$ Eve picks.

We study the tradeoff between the rate of reliable transmission ($R = \frac{\log|\mathcal{W}|}{n}$ such that $\lim_{n\to\infty} P_e = 0$), the fraction of the transmitted symbols tapped by Eve ($\alpha = \frac{\mu}{n}, 0 \leq \alpha \leq 1$), and the normalized equivocation at Eve ($\delta = \frac{\Delta}{H(W)}$).

Definition 1: The triple (R, α, δ) is said to be achievable if for every $\epsilon > 0$, there exists an encoder-decoder pair, $(f_{(k,n)}, g_{P_e})$, and $n_0 \geq 1$ such that $\frac{k}{n} \geq R - \epsilon$, $\frac{\mu}{n} \geq \alpha - \epsilon$, $\frac{\Delta}{k} \geq \delta - \epsilon$, and $P_e \leq \epsilon$, for all $n \geq n_0$.

Definition 2: For a fixed α, where $0 \leq \alpha \leq 1$, the secrecy rate R_s is achievable if the triple $(R_s, \alpha, 1)$ is achievable, i.e., the secrecy rate R_s, for some fixed α, is achievable if $P_e \to 0$, and $\frac{\Delta}{k} \to 1$ as $n \to \infty$.

III. Main Result

The following theorems provide outer and inner bounds for the set of achievable triples (R, α, δ), $\mathcal{R}$. Let C_M denote the capacity of the main channel $p_{Y|X}$, i.e., $C_M = \max_{p_X} I(X;Y)$. For the channel $p_{Y|X}$, let

$$C_u = I(X;Y) \text{ when } p_X(x) = 1/|\mathcal{X}| \text{ for all } x \in \mathcal{X}. \tag{4}$$

Theorem 1: The set $\mathcal{R} \subseteq \overline{\mathcal{R}}$, where

$$\overline{\mathcal{R}} = \Bigg((R, \alpha, \delta) : 0 \leq \alpha, \delta \leq 1,\ \ 0 \leq R \leq C_M, \text{ and } \delta \leq \begin{cases} 1, & \text{if } 0 \leq \alpha \leq 1 - \frac{R}{C_M} \\ (1-\alpha)\frac{C_M}{R}, & \text{if } 1 - \frac{R}{C_M} \leq \alpha \leq 1. \end{cases} \Bigg). \tag{5}$$

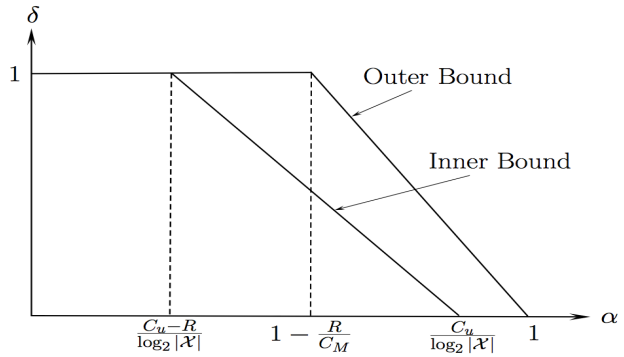

Fig. 2. Inner and outer bounds for (α, δ), for a fixed R.

Theorem 2: The set $\mathcal{R} \supseteq \underline{\mathcal{R}}$, where

$$\underline{\mathcal{R}} = \Bigg((R, \alpha, \delta) : 0 \leq \alpha, \delta \leq 1,\ \ 0 \leq R \leq C_u, \text{ and } \delta \leq \begin{cases} 1, & \text{if } 0 \leq \alpha \leq \frac{C_u - R}{\log|\mathcal{X}|} \\ \left[\frac{C_u - \alpha \log|\mathcal{X}|}{R}\right]^+, & \text{if } \frac{C_u - R}{\log|\mathcal{X}|} < \alpha \leq 1. \end{cases} \Bigg). \tag{6}$$

For a fixed rate R, the inner and outer bounds for the pair (α, δ) are shown in Fig. 2. As the achievable secrecy rate, R_s, for the model in question is of a particular interest, the following corollary, which directly follows from Theorems 1,2 by setting $\delta = 1$, gives lower and upper bounds for R_s.

Corollary 1: For a fixed α, where $0 \leq \alpha \leq 1$, the achievable secrecy rate R_s satisfies

$$[C_u - \alpha \log|\mathcal{X}|]^+ \leq R_s \leq (1-\alpha) C_M. \tag{7}$$

Remark: The lower bound for R_s in (7), computed for a binary main channel whose capacity is achieved by a uniform input distribution, is equal to the secrecy capacity of a WTC with the same binary main channel and an erasure eavesdropper channel with erasure probability $1 - \alpha$.

IV. Outer Bound

In order to prove Theorem 1, we show that any achievable triple, $(R, \alpha, \delta) \in \mathcal{R}$, satisfies $(R, \alpha, \delta) \in \overline{\mathcal{R}}$, where $\overline{\mathcal{R}}$ is given in (5). That $R \leq C_M$ follows from the regular converse to the channel coding theorem [8]. That $\alpha \leq 1$ follows since $\alpha \leq \frac{\mu}{n} + \epsilon \leq 1 + \epsilon$ for every $\epsilon > 0$. That $\delta \leq 1$ follows since, for any $\epsilon > 0$, $\delta \leq \frac{\Delta}{k} + \epsilon = \frac{\min_{\mathcal{S}} H(W|\mathbf{Z}^n)}{H(W)} + \epsilon \leq 1 + \epsilon$. Thus, it remains to show the last inequality in (5).

Consider an arbitrary encoder-decoder pair, $(f_{(k,n)}, g_{P_e})$, and a fixed selection of $\mathcal{S}$ at Eve. Let $W, \mathbf{X}, \mathbf{Y}, \mathbf{Z}, \hat{W}$ correspond to the pair $(f_{(k,n)}, g_{P_e})$ and the selection of $\mathcal{S}$. Thus,

$$\begin{aligned} \Delta = H(W|\mathbf{Z}) &\leq H(W|\mathbf{Z}) - H(W|\mathbf{Y}) + n\eta(P_e) && (8) \\ &= I(W;\mathbf{Y}) - I(W;\mathbf{Z}) + n\eta(P_e) && (9) \\ &\leq I(W;\mathbf{YZ}) - I(W;\mathbf{Z}) + n\eta(P_e) && (10) \\ &= I(W;\mathbf{Y}|\mathbf{Z}) + n\eta(Pe), && (11) \end{aligned}$$

where (8) follows from Fano's inequality, $\lim_{P_e \to 0} \eta(P_e) = 0$. Let $\mathcal{S}^{\mathrm{C}} = \{1, 2, \cdots, n\} \backslash \mathcal{S}$. Define $\mathbf{X}_{\mathcal{S}} = \{X_i\}_{i \in \mathcal{S}}$, and

$\mathbf{X}_{\mathcal{S}^{\mathrm{C}}} = \{X_i\}_{i\in\mathcal{S}^{\mathrm{C}}}$, and let $\mathbf{Y}_{\mathcal{S}}$ and $\mathbf{Y}_{\mathcal{S}^{\mathrm{C}}}$ be defined similarly. Due to the Markov Chain $W - \mathbf{XZ} - \mathbf{Y}$, (11) is bounded as

$$\begin{aligned}
\Delta &\le I(\mathbf{X};\mathbf{Y}|\mathbf{Z}) + n\eta(P_e) && (12)\\
&= H(\mathbf{X}_{\mathcal{S}^{\mathrm{C}}}|\mathbf{X}_{\mathcal{S}}) - H(\mathbf{X}_{\mathcal{S}^{\mathrm{C}}}|\mathbf{Y}_{\mathcal{S}}\mathbf{Y}_{\mathcal{S}^{\mathrm{C}}}\mathbf{X}_{\mathcal{S}}) + n\eta(P_e) && (13)\\
&= H(\mathbf{X}_{\mathcal{S}^{\mathrm{C}}}|\mathbf{X}_{\mathcal{S}}) - H(\mathbf{X}_{\mathcal{S}^{\mathrm{C}}}|\mathbf{Y}_{\mathcal{S}^{\mathrm{C}}}\mathbf{X}_{\mathcal{S}}) + n\eta(P_e) && (14)\\
&= I(\mathbf{X}_{\mathcal{S}^{\mathrm{C}}};\mathbf{Y}_{\mathcal{S}^{\mathrm{C}}}|\mathbf{X}_{\mathcal{S}}) + n\eta(P_e) && (15)\\
&\le I(\mathbf{X}_{\mathcal{S}^{\mathrm{C}}};\mathbf{Y}_{\mathcal{S}^{\mathrm{C}}}) + n\eta(P_e) && (16)\\
&\le \sum_{i\in\mathcal{S}^{\mathrm{C}}} I(X_i;Y_i) + n\eta(Pe) && (17)\\
&\le (n-\mu)\max_{p_X} I(X;Y) + n\eta(P_e) && (18)\\
&= (n-\mu)C_M + n\eta(P_e), && (19)
\end{aligned}$$

where (14) follows from the Markov chain $\mathbf{X}_{\mathcal{S}^{\mathrm{C}}} - \mathbf{X}_{\mathcal{S}}\mathbf{Y}_{\mathcal{S}^{\mathrm{C}}} - \mathbf{Y}_{\mathcal{S}}$, (16) follows from the Markov chain $\mathbf{X}_{\mathcal{S}} - \mathbf{X}_{\mathcal{S}^{\mathrm{C}}} - \mathbf{Y}_{\mathcal{S}^{\mathrm{C}}}$, and (17) follows from the memoryless channel assumption.

Thus, we have, for any selection of $\mathcal{S}$, $\Delta \le (n-\mu)C_M + n\eta(P_e)$. But, Δ is also upper bounded as $\Delta = \min_{\mathcal{S}} H(W|\mathbf{Z}) \le H(W) = k$, and hence, we have, for every encoder-decoder pair,

$$\Delta \le \min\left\{k, (n-\mu)C_M + n\eta(P_e)\right\}. \tag{20}$$

Since $(R,\alpha,\delta) \in \mathcal{R}$, then for every $\epsilon > 0$, there exists an encoder-decoder pair with $\frac{k}{n} \ge R-\epsilon$, $\frac{\mu}{n} \ge \alpha-\epsilon$, $\frac{\Delta}{k} \ge \delta-\epsilon$, and $P_e \le \epsilon$. Thus, for every $\epsilon > 0$, by applying (20) to this encoder-decoder pair, we obtain

$$\delta \le \begin{cases} 1+\epsilon, & 0 \le \alpha \le 1 - \frac{R}{C_M} + O(\epsilon) \\ \frac{(1-\alpha)C_M}{R-\epsilon} + O(\epsilon), & 1 - \frac{R}{C_M} \le \alpha + O(\epsilon) \le 1. \end{cases} \tag{21}$$

Taking $\epsilon \to 0$, the last inequality in (5) is proved, which completes the proof for Theorem 1.

V. Inner Bound

The enabler for the achievability result in [3] is the assumption of a noiseless main channel over which a codebook $\mathcal{C}_0$, that contains all possible codewords, can be reliably communicated. The enabling property, satisfied by $\mathcal{C}_0$, is that for every possible observation at Eve, $\mathbf{z}^n$ (which results from a transmitted codeword, $\mathbf{x}^n$, and a selection of $\mathcal{S}$), the number of codewords in $\mathcal{C}_0$ that can generate $\mathbf{z}^n$ is the same. Relying on this property, the existence of a good partition of $\mathcal{C}_0$ (of equal size subsets) that distributes the codewords among the subsets of the partition in a harmony that asymptotically (with the codeword length, n) achieves the secrecy constraint for every possible selection of $\mathcal{S}$, is evident by [3]. When the main channel is a DMC, our achievability scheme relies on defining a class of good codebooks which possess a similar property to that of $\mathcal{C}_0$. We restrict the input distribution to be uniform, and α to be such that $\alpha < \frac{C_u}{\log|\mathcal{X}|}$, in order to show, using a random coding argument, that the probability of the class of good codes approaches 1 as $n \to \infty$. Thus, the existence of a codebook, that achieves the reliability constraint, within the class of good codes follows. In the following, the achievable scheme is described in detail.

Codebook Generation: Let p_X be a uniform distribution over $\mathcal{X}$, i.e., $p_X(x) = 1/|\mathcal{X}|$ for all $x \in \mathcal{X}$, and for the main channel $p_{Y|X}$, let $C_u = I(X;Y)$. Generate 2^{nC_u} length-n codewords randomly and independently, each with independent and identically distributed (i.i.d.) components according to p_X. Let $\mathcal{C}$ denote the random variable which represents the generated codebook. For the generated codebook $\mathcal{C} = C$, let $\{\mathcal{A}_w\}_{w=1}^{2^k}$ be a partition of C into 2^k disjoint subsets, $\mathcal{A}_w$s, each containing 2^{nC_u-k} codewords.

Encoder at Alice: In order to send the message W, the encoder randomly selects a codeword, $\mathbf{X}^n$, from $\mathcal{A}_W$, and transmits $\mathbf{X}^n$. For this encoder, let $k = Rn$, and $\mu = \alpha n$.

Decoder at Bob: Since the rate of the codebook C, $(1/n)\log 2^{nC_u} = I(X;Y)$, it can be shown [8], using a typical set decoder at Bob, that for every $\epsilon > 0$, there exists a sufficiently large n_1 such that $\mathrm{E}_{\mathcal{C}}(P_e) \le \frac{\epsilon}{3}$ for all $n \ge n_1$.

Equivocation Analysis: For an arbitrary codebook C, an encoder defined as above, an arbitrary selection of $\mathcal{S}$, and $\mathbf{Z}^n$ which corresponds to $\mathcal{S}$ (as defined in (2)), we have

$$\begin{aligned}
\Delta &= H(W|\mathbf{Z}) = H(W,\mathbf{Z}) - H(\mathbf{Z}) && (22)\\
&= H(W,\mathbf{X},\mathbf{Z}) - H(\mathbf{X}|W,\mathbf{Z}) - H(\mathbf{Z}) && (23)\\
&= H(\mathbf{X}|\mathbf{Z}) + H(W|\mathbf{X},\mathbf{Z}) - H(\mathbf{X}|W,\mathbf{Z}). && (24)
\end{aligned}$$

By the construction of the encoding scheme, for every selection of the set $\mathcal{S}$, we have

$$H(W|\mathbf{X},\mathbf{Z}) = 0. \tag{25}$$

Definition 3*:* The codeword $\mathbf{x}^n$ is said to be consistent with Eve's observation $\mathbf{z}^n$ if $\mathbf{z}^n$ can be obtained from $\mathbf{x}^n$ by switching $(n-\mu)$ components of $\mathbf{x}^n$ to $'?'$.

For an arbitrary codebook C, $j = 1,2,\cdots,2^{nC_u}$, and $\mathcal{S} \subseteq \{1,2,\cdots,n\}$ with $|\mathcal{S}| = \mu$, let $\mathbf{x}(j) = [x_1(j)\ \cdots\ x_n(j)]$ denote the jth codeword in C, and $\mathbf{z}(j,\mathcal{S})$ denote the length-n vector with $x_i(j)$ in the positions $i \in \mathcal{S}$, and $'?'$ in the remaining positions, and define $\mathcal{Q}_C(j,\mathcal{S})$, $m_C(j,\mathcal{S})$ as

$$\begin{aligned}
\mathcal{Q}_C(j,\mathcal{S}) = \Big\{ &\mathbf{x}(i) \in C :\ \text{for } \mathbf{x}(j) \in C,\ \mathbf{x}(i) \text{ is consistent} \\
&\text{with } \mathbf{z}(j,\mathcal{S}),\ i = 1,2,\cdots,2^{nC_u}, i \ne j \Big\}, && (26)\\
m_C(j,\mathcal{S}) = &\left|\mathcal{Q}_C(j,\mathcal{S})\right|. && (27)
\end{aligned}$$

Now, let us define a set of good codebooks, $\mathcal{C}^*$, as

$$\begin{aligned}
\mathcal{C}^* = \Big\{ &C : \forall j = 1,2,\cdots,2^{nC_u},\ \text{and } \forall \mathcal{S} \subseteq \{1,2,\cdots,n\}, \\
&\text{with } |\mathcal{S}| = \mu,\ \ |m_C(j,\mathcal{S}) - m| \le t \Big\}, && (28)
\end{aligned}$$

where[1] $m = 2^{n(C_u - \alpha\log|\mathcal{X}|)}$, $t = \beta\sqrt{n}2^{\frac{n}{2}(C_u-\alpha\log|\mathcal{X}|)} + |\mathcal{X}|^{-\alpha n}$, and β is a constant which does not depend on n.

Now, we consider a good codebook, $C \in \mathcal{C}^*$. Since the message W is uniformly distributed, and the encoder randomly selects a codeword from $\mathcal{A}_W$, we have $\mathbf{X}^n$ is uniformly distributed over C. Thus, given Eve's observation, $\mathbf{Z}^n = \mathbf{z}^n$, $\mathbf{X}^n$ is uniformly distributed over the codewords in C consistent

[1]We assume that 2^{nC_u}, and all such quantities, are integers. If not, a straight forward modification of the sequel is necessary.

with $\mathbf{z}^n$. Using (28), we have, for all $\mathcal{S}$, that

$$H(\mathbf{X}|\mathbf{Z}) \geq \log(m-t). \tag{29}$$

Next, we show the existence of a partition $\{\mathcal{A}_w\}_{w=1}^{2^k}$ of the good codebook C, which satisfies that, for all $\mathcal{S}$, $H(\mathbf{X}|W,\mathbf{Z})$ is upper bounded by a constant which does not depend on n.

Definition 4: A partition $\{\mathcal{A}_w\}_{w=1}^{2^k}$ of the codebook C is said to be good, if there exists an integer $L \geq 1$ such that for all $w = 1, \cdots, 2^k$, $j = 1, \cdots, 2^{nC_u}$, and $\mathcal{S} \subseteq \{1, 2, \cdots, n\}$ with $|\mathcal{S}| = \mu$, we have

$$\left| \{\mathbf{x} \in \mathcal{A}_w : \mathbf{x} \text{ is consistent with } \mathbf{z}(j, \mathcal{S})\} \right| < L. \tag{30}$$

If a partition $\{\mathcal{A}_w\}$ of $C \in \mathcal{C}^*$ is good, we have, for all $\mathcal{S}$,

$$H(\mathbf{X}|W,\mathbf{Z}) < \log L. \tag{31}$$

We now choose the partition $\{\mathcal{A}_w\}$ of $C \in \mathcal{C}^*$ uniformly at random from the set of all partitions of C into 2^k equal size subsets. Define the functions $\psi(\{\mathcal{A}_w\})$, $\phi(\mathcal{A}_w, \mathbf{z}(j,\mathcal{S}))$ as

$$\psi(\{\mathcal{A}_w\}) = \begin{cases} 0, & \text{if the partition } \{\mathcal{A}_w\} \text{ is good} \\ 1, & \text{otherwise.} \end{cases} \tag{32}$$

$$\phi(\mathcal{A}_w, \mathbf{z}) = \begin{cases} 0, & \text{if } \left|\{\mathbf{x} \in \mathcal{A}_w : \mathbf{x} \text{ is consistent with } \mathbf{z}\}\right| < L \\ 1, & \text{otherwise.} \end{cases} \tag{33}$$

Note that, we have $\psi(\{\mathcal{A}_w\}) \leq \sum_{w=1}^{2^k} \sum_{j,\mathcal{S}} \phi(\mathcal{A}_w, \mathbf{z}(j,\mathcal{S}))$, and hence, by linearity and monotonicity of expectation,

$$\mathrm{E}\{\psi(\{\mathcal{A}_w\})\} \leq \sum_{w=1}^{2^k} \sum_{j,\mathcal{S}} \mathrm{E}\{\phi(\mathcal{A}_w, \mathbf{z}(j,\mathcal{S}))\}. \tag{34}$$

We now upper bound $\mathrm{E}\{\phi(\mathcal{A}_w, \mathbf{z}(j,\mathcal{S}))\}$. For fixed w, j, and $\mathcal{S}$, let L_r denote a random variable which represents the number of codewords $\mathbf{x} \in \mathcal{A}_w$, that are consistent with $\mathbf{z}(j,\mathcal{S})$. Let $n_C = |C| = 2^{nC_u}$, $m_C = |\mathcal{Q}_C(j,\mathcal{S})|$, and $n_r = |\mathcal{A}_w| = 2^{n(C_u - R)}$. Using a similar analysis as in [3], we have

$$\Pr\{L_r = l\} \leq \left(\frac{m_C n_r}{n_C}\right)^l \frac{2^l}{l!}. \tag{35}$$

Since we consider a good codebook $C \in \mathcal{C}^*$, we have $m_C \leq m + t = 2^{n(C_u - \alpha\log|\mathcal{X}|)}(1 + \frac{t}{m})$. For $\alpha < \frac{C_u}{\log|\mathcal{X}|}$, $\lim_{n\to\infty} \frac{t}{m} = 0$, i.e., $\frac{t}{m} \in o(n)$. Thus, using (35), we have

$$\Pr\{L_r = l\} \leq 2^{n(C_u - \alpha\log|\mathcal{X}| - R)l} \frac{\left(2(1+\frac{t}{m})\right)^l}{l!}. \tag{36}$$

Thus, whenever $R > C_u - \alpha\log|\mathcal{X}|$, we have

$$\mathrm{E}\{\phi(\mathcal{A}_w, \mathbf{z}(j,\mathcal{S}))\} = \Pr\{\phi(\mathcal{A}_w, \mathbf{z}(j,\mathcal{S})) = 1\} \tag{37}$$

$$\leq \sum_{l=L}^{n_r} 2^{n(C_u - \alpha\log|\mathcal{X}| - R)l} \frac{\left(2(1+\frac{t}{m})\right)^l}{l!} \tag{38}$$

$$\leq 2^{n(C_u - \alpha\log|\mathcal{X}| - R)L + 2(1+\frac{t}{m})\log e}, \tag{39}$$

and hence, using (34), we have

$$\mathrm{E}\{\psi(\{\mathcal{A}_w\})\} \leq 2^k 2^{nC_u} \binom{n}{\alpha n} \times 2^{n(C_u - \alpha\log|\mathcal{X}| - R)L + 2(1+\frac{t}{m})\log e} \tag{40}$$

$$\leq 2^{n(R + C_u + H(\alpha) + o(n)) + 2(1+\frac{t}{m})\log e + n(C_u - \alpha\log|\mathcal{X}| - R)L}, \tag{41}$$

where (41) follows from Stirling's approximation. Thus, for

$$L > \frac{R + C_u + H(\alpha) + o(n) + \frac{2(1+\frac{t}{m})\log e}{n}}{R - C_u + \alpha\log|\mathcal{X}|}, \tag{42}$$

we have $\mathrm{E}\{\psi(\{\mathcal{A}_w\})\} < 1$, and hence there must exist a good partition $\{\mathcal{A}_w\}$ of the codebook $C \in \mathcal{C}^*$. Since $\frac{t}{m} \in o(n)$, we have, for sufficiently large n_2, $o(n) \leq \epsilon_1$ and $\frac{t}{m} \leq \epsilon_2$, for all $n \geq n_2$. Thus, whenever $\frac{C_u - R}{\log|\mathcal{X}|} < \alpha < \frac{C_u}{\log|\mathcal{X}|}$, by setting

$$L = \frac{R + C_u + H(\alpha) + \epsilon_1 + \frac{2(1+\epsilon_2)\log e}{n_2}}{R - C_u + \alpha\log|\mathcal{X}|} + 1 = B, \tag{43}$$

the existence of a good partition $\{\mathcal{A}_w\}$ is guaranteed. This is the partition chosen by the encoder at Alice.

Using (24), (25), (29), (31), and (43), we have, for $C \in \mathcal{C}^*$, $\frac{C_u - R}{\log|\mathcal{X}|} < \alpha < \frac{C_u}{\log|\mathcal{X}|}$, and sufficiently large n,

$$\frac{\Delta}{k} = \min_{\mathcal{S}:|\mathcal{S}|=\mu} \frac{H(W|\mathbf{Z})}{k} \geq \frac{1}{k}(\log(m-t) - \log B) \tag{44}$$

$$= \frac{\log m}{k} - o(n) \geq \frac{C_u - \alpha\log|\mathcal{X}|}{R} - \epsilon_3, \tag{45}$$

where, for sufficiently large n_3, $o(n) \leq \epsilon_3$ for all $n \geq n_3$.

We now show that with high probability, $C \in \mathcal{C}^*$, i.e., $\lim_{n\to\infty} \Pr\{C \in \mathcal{C}^*\} = 1$. Let $\mathbf{X}(j)$, $j = 1, \cdots, 2^{nC_u}$, represent the jth codeword of the random code $\mathcal{C}$, and let $\mathbf{Z}_{\mathcal{S}}(\mathbf{X}(j))$ represent the codeword $\mathbf{X}(j)$ with '?' for $i \notin \mathcal{S}$. For $j = 1, \cdots, 2^{nC_u}$, and all $\mathcal{S}$, define the event $\mathcal{E}(j,\mathcal{S})$ as

$$\mathcal{E}(j,\mathcal{S}) = \Big\{\Big|\mathrm{card}\big\{i : \mathbf{X}(i) \text{ is consistent with } \mathbf{Z}_{\mathcal{S}}(\mathbf{X}(j)), \text{ where } i = 1, 2, \cdots, 2^{nC_u}, i \neq j\big\} - m\Big| \leq t\Big\}, \tag{46}$$

and let $\mathcal{E}^{\mathrm{C}}(j,\mathcal{S})$ denote the complement of (46). Using the definition of $\mathcal{C}^*$ in (28), we have

$$\Pr\{\mathcal{C}^*\} = \Pr\big\{\mathcal{E}(j,\mathcal{S}), \forall j = 1, 2, \cdots, 2^{nC_u} \text{ and } \forall \mathcal{S} \subseteq \{1, 2, \cdots, n\} \text{ with } |\mathcal{S}| = \mu\big\} \tag{47}$$

$$= 1 - \Pr\big\{\mathcal{E}^{\mathrm{C}}(j,\mathcal{S}) \text{ for some } j, \text{ or some } \mathcal{S}\big\} \tag{48}$$

$$\geq 1 - \sum_{j=1}^{2^{nC_u}} \sum_{\mathcal{S}} \Pr\{\mathcal{E}^{\mathrm{C}}(j,\mathcal{S})\} \tag{49}$$

$$= 1 - 2^{nC_u} \binom{n}{\alpha n} \Pr\big\{\mathcal{E}^{\mathrm{C}}(1,\mathcal{S}^*)\big\}, \tag{50}$$

where $\mathcal{S}^*$ is some set such that $\mathcal{S}^* \subseteq \{1, 2, \cdots, n\}$ with $|\mathcal{S}^*| = \mu$, (49) follows from the union bound, and (50) follows because of the symmetry in the codebook, $\mathcal{C}$, construction; $\Pr\{\mathcal{E}^{\mathrm{C}}(j,\mathcal{S})\}$ is the same for all j and all $\mathcal{S}$.

Let $\mathcal{E}_{\mathbf{x}(1)}(1,\mathcal{S}^*)$, and $\mathbf{z}_{\mathcal{S}^*}(\mathbf{x}(1))$ denote the event $\mathcal{E}(1,\mathcal{S}^*)$,

and the random vector $\mathbf{Z}_{\mathcal{S}^*}(\mathbf{X}(1))$ when $\mathbf{X}(1) = \mathbf{x}(1)$, respectively. Using (46), we have,

$$\Pr\{\mathcal{E}_{\mathbf{x}(1)}(1,\mathcal{S}^*)\} = \Pr\left\{\left|\mathrm{card}\Big\{i : \mathbf{X}(i) \text{ is consistent with } \mathbf{z}_{\mathcal{S}^*}(\mathbf{x}(1)), i = 2,3,\cdots,2^{nC_u}\Big\} - m\right| \le t\right\}. \quad (51)$$

For $i = 2,3,\cdots,2^{nC_u}$, define the random variable V_i as

$$V_i = \begin{cases} 1, & \text{if } \mathbf{X}(i) \text{ is consistent with } \mathbf{z}_{\mathcal{S}^*}(\mathbf{x}(1)) \\ 0, & \text{otherwise.} \end{cases} \quad (52)$$

Note that the random variables $\{V_i\}_{i=2}^{2^{nC_u}}$ are i.i.d. In addition, we have, for each value of $\mathbf{x}(1)$, and for $i = 2,\cdots,2^{nC_u}$,

$$\mathrm{E}\{V_i\} = \Pr\{V_i = 1\} = |\mathcal{X}|^{-\alpha n}. \quad (53)$$

Let $V = \sum_{i=2}^{2^{nC_u}} V_i$. We can rewrite $\Pr\{\mathcal{E}_{\mathbf{x}(1)}(1,\mathcal{S}^*)\}$ as

$$\Pr\{\mathcal{E}_{\mathbf{x}(1)}(1,\mathcal{S}^*)\} = \Pr\{|V - m| \le t\}. \quad (54)$$

Since $\mathrm{E}(V) = (2^{nC_u} - 1)|\mathcal{X}|^{-\alpha n} = m - |\mathcal{X}|^{-\alpha n}$, by setting $t' = t - |\mathcal{X}|^{-\alpha n}$, we have

$$\Pr\{\mathcal{E}_{\mathbf{x}(1)}(1,\mathcal{S}^*)\} \ge \Pr\{|V - \mathrm{E}(V)| \le t'\}. \quad (55)$$

By applying the multiplicative version of Chernoff-Hoeffding bound [9], [10] to (55), we obtain

$$\Pr\{\mathcal{E}_{\mathbf{x}(1)}(1,\mathcal{S}^*)\} \ge 1 - 2e^{\frac{-t'^2}{(2+\tau)\mathrm{E}(V)}}, \quad (56)$$

where $\tau = \frac{t'}{\mathrm{E}(V)}$. Using (56), we have

$$\Pr\{\mathcal{E}(1,\mathcal{S}^*)\} = \sum_{\mathbf{x}(1)} \Pr\{\mathbf{X}(1) = \mathbf{x}(1)\} \Pr\left\{\mathcal{E}_{\mathbf{x}(1)}(1,\mathcal{S}^*)\right\} \ge 1 - 2e^{\frac{-t'^2}{(2+\tau)\mathrm{E}(V)}}. \quad (57)$$

Substituting $\Pr\{\mathcal{E}^{\mathrm{C}}(1,\mathcal{S}^*)\} \le 2e^{\frac{-t'^2}{(2+\tau)\mathrm{E}(V)}}$ in (50), and choosing t' as $t' = \beta\sqrt{n}2^{\frac{n}{2}(C_u - \alpha\log|\mathcal{X}|)}$, gives

$$\Pr\{\mathcal{C}^*\} \ge 1 - 2^{nC_u}\binom{n}{\alpha n} 2e^{\frac{-t'^2}{(2+\tau)\mathrm{E}(V)}} \quad (58)$$

$$\ge 1 - 2^{n(C_u + H(\alpha) + o(n) - \frac{\beta^2}{(2+\tau)}\log e)}. \quad (59)$$

For sufficiently large n_4, we have $o(n) \le \epsilon_4$ and $\tau \le \epsilon_5$ for all $n \ge n_4$, where $\tau = \frac{t'}{\mathrm{E}(V)} \in o(n)$. By setting $\beta \ge \sqrt{\frac{(\gamma + C_u + H(\alpha) + \epsilon_4)(2+\epsilon_5)}{\log e}}$, where $\gamma > 0$, we have, for $n \ge n_4$,

$$\Pr\{\mathcal{C}^*\} \ge 1 - 2^{-\gamma n}. \quad (60)$$

Using (45) and (60), we have, for $\frac{C_u - R}{\log|\mathcal{X}|} < \alpha < \frac{C_u}{\log|\mathcal{X}|}$, and sufficiently large n,

$$\mathrm{E}_{\mathcal{C}}\left(\frac{\Delta}{k}\right) \ge \left(\frac{C_u - \alpha\log|\mathcal{X}|}{R} - \epsilon_3\right)(1 - 2^{-\gamma n}) \quad (61)$$

$$\ge \frac{C_u - \alpha\log|\mathcal{X}|}{R} - \frac{\epsilon}{3}, \quad (62)$$

where, for sufficiently large n_5, $3(\epsilon_3 + \frac{2^{-\gamma n}(C_u - \alpha\log|\mathcal{X}|)}{R}) \le \epsilon$ for all $n \ge n_5$. Let $n_0 = \max_{i=1:5} n_i$. For $n \ge n_0$ and $\frac{C_u - R}{\log|\mathcal{X}|} < \alpha < \frac{C_u}{\log|\mathcal{X}|}$, using (62) and that $\mathrm{E}_{\mathcal{C}}(P_e) \le \frac{\epsilon}{3}$, we have

$$\Pr\left\{P_e \le \epsilon, \frac{\Delta}{k} \ge \frac{C_u - \alpha\log|\mathcal{X}|}{R} - \epsilon\right\} \ge 1 - \Pr\{P_e \ge \epsilon\} - \Pr\left\{\frac{\Delta}{k} \le \frac{C_u - \alpha\log|\mathcal{X}|}{R} - \epsilon\right\} \ge \frac{1}{3}, \quad (63)$$

where (63) follows from the union bound and Markov inequality. Thus, for a fixed R, $0 \le R \le C_u$, a fixed α, $\frac{C_u - R}{\log|\mathcal{X}|} < \alpha \le 1$, and for every $\epsilon > 0$, there exists a sufficiently large n_0, and an encoder-decoder pair with $k = Rn$, $\mu = \alpha n$, $\frac{\Delta}{k} \ge \frac{[C_u - \alpha\log|\mathcal{X}|]^+}{R} - \epsilon$, and $P_e \le \epsilon$, for all $n \ge n_0$. This completes the proof for Theorem 2.

VI. Conclusion

In this work, we have derived outer and inner bounds for the rate-equivocation region of a wiretap channel with a discrete memoryless main channel, and an eavesdropper (Eve) which has a noiseless access to μ symbols (of its own choice) of the n transmitted symbols. The characterization of the derived inner and outer bounds has provided a trade-off between the rate of reliable transmission, R, the level of equivocation at Eve, δ, and the ratio of the tapped symbols by Eve, $\alpha = \frac{\mu}{n}$. The achievability has been established by random coding and random partitioning arguments, where, for a uniform input distribution and a certain range of α, the existence of a good codebook which achieves the reliability constraint, and for which there exists a good partition that achieves the required level of equivocation no matter what subset of μ symbols Eve chooses, is guaranteed. Although the capacity-equivocation region of the model in question is still open, the inner and outer bounds proposed in this work provide insights for understanding the fundamental limits of the model, and count as a step towards characterizing its capacity-equivocation region, as well as towards understanding the impact of more powerful eavesdroppers than passive observers.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. 24, no. 3, pp. 339–3487, 1978.

[3] L. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell System Technical Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[4] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Info. Theory*, vol. 37, no. 5, pp. 1412–1418, 1991.

[5] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Info. Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[6] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," in *IEEE Information Theory Workshop*, September 2007.

[7] V. Aggarwal, L. Lai, A. R. Calderbank, and H. V. Poor, "Wiretap channel type II with an active eavesdropper," in *IEEE International Symposium on Information Theory*, July 2009.

[8] T. M. Cover and J. A. Thomas, *Elements of information theory 2nd edition*. New York, NY, USA: Wiley, 2006.

[9] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American statistical association*, vol. 58, no. 301, pp. 13–30, 1963.

[10] D. Angluin and L. G. Valiant, "Fast probabilistic algorithms for Hamiltonian circuits and matchings," in *the ninth annual ACM symposium on Theory of computing*, May 1977.