Journal of Universal Computer Science, vol. 27, no. 11 (2021), 1222-1239
submitted: 11/2/2021, accepted: 9/8/2021, appeared: 28/11/2021 CC BY-ND 4.0

E - Capacity - Equivocation Region of Wiretap Channel

Mariam Haroutunian
(Institute for Informatics and Automation Problems,
National Academy of Sciences of Armenia, Yerevan, Armenia
https://orcid.org/0000-0002-9262-4173, armar@sci.am)

Abstract: One of the problems of information - theoretic security concerns secure communication over a wiretap channel. The aim in the general wiretap channel model is to maximize the rate of the reliable communication from the source to the legitimate receiver, while keeping the confidential information as secret as possible from the wiretapper (eavesdropper).
We introduce and investigate the E - capacity - equivocation region and the E - secrecy capacity function for the wiretap channel, which are, correspondingly, the generalizations of the capacity - equivocation region and secrecy - capacity studied by Csiszár and Körner (1978). The E - capacity - equivocation region is the closure of the set of all achievable rate - reliability and equivocation pairs, where the rate - reliability function represents the optimal dependence of rate on the error probability exponent (reliability). By analogy with the notion of E - capacity, we consider the E - secrecy capacity function that for the given E is the maximum rate at which the message can be transmitted being kept perfectly secret from the wiretapper.

Keywords: Wiretap channel, information-theoretic security, equivocation rate, E-capacity, secrecy capacity
Categories: E.4
DOI: 10.3897/jucs.76605

1 Introduction

Security is an important topic in communications. The information - theoretic security is an approach that demonstrates the possibility of transmitting confidential messages without using an encryption key. The main idea of the information - theoretic security is to exploit the inherent noises and difference between the channels to the legitimate receiver and the eavesdropper. In addition, the transmitter intentionally adds randomness to prevent eavesdroppers from accepting useful information while guaranteeing the legitimate receiver to obtain the information. Such an approach to guarantee secrecy has the advantage of eliminating the key management issue, resulting in lower complexity and savings in resources. Such an approach was initiated by Wyner [Wyner 1975], who studied the most basic model called a wiretap channel. Later, Csiszár and Körner [Csiszár and Körner 1978] studied the broadcast channel with confidential messages, the special case of which is the more general model of the wiretap channel. It is called a generalized wiretap channel because the model from [Wyner 1975] is a special case of it, when the channel to the eavesdropper is a degraded version of the main channel.

In this paper, we consider the generalized model of **wiretap channel** (see Fig. 1), which is defined as follows. The source wishes to transmit a message m to the legitimate receiver while keeping it as secret as possible from the eavesdropper. The confidential message m is assumed to be randomly and uniformly distributed over the message set $\mathcal{M}$. The encoder f_N maps each message m to a codeword $\mathbf{x}(m) = (x_1, ..., x_N) \in \mathcal{X}^N$,

where $\mathcal{X}$ is the input alphabet, and N is the transmission length. The codeword $\mathbf{x}(m)$ is transmitted over a discrete memoryless channel (DMC) with transition probability $W(y,z|x)$. The noisy version $\mathbf{y} \in \mathcal{Y}^N$ is accepted by the legitimate receiver, and $\mathbf{z} \in \mathcal{Z}^N$ - by the eavesdropper, respectively. The decoder g_N at the receiver maps the received sequence $\mathbf{y}$ to an estimate $\hat{m}$ of the message.

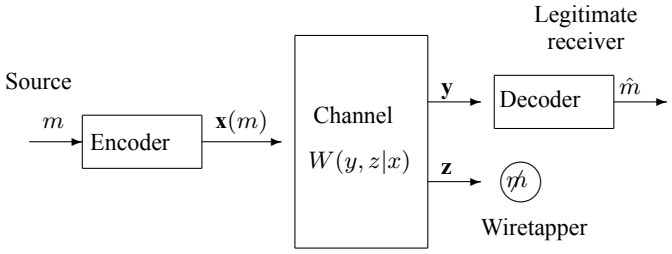

Figure 1: The model of generalized wiretap channel.

The capacity-equivocation region $\mathcal{C}(W)$, as well as the secrecy capacity $C_s(W)$ of this model, was obtained in [Csiszár and Körner 1978].

In recent years various extensions of this model has attracted attention and investigated in the literature. Some results are surveyed in [Liang et al. 2008], later publications, among others, include [Chen, Vinck 2008], [Liang et al. 2009], [Chia, Gamal 2012], [Nötzel et al. 2016], [Han et al. 2019], [Goldfeld et al. 2020] on state dependent wiretap channels, [Wang, Safavi-Naini 2016] on wiretap channels with active adversaries.

We are the first to investigate the E - capacity - equivocation region $\mathcal{C}(E,W)$, which is the closure of the set of all achievable rate - reliability - equivocation pairs $(R(E), R_e)$, where the function $R(E)$ represents the optimal dependence of the rate R on reliability (error probability exponent) E. It is the analogue of E - capacity (rate -reliabilty function) suggested by E. Haroutunian [Haroutunian 2007] and investigated for various channel models [Haroutunian et al. 2007].

The outer (sphere packing) bound of E - capacity - equivocation region was constructed in [Haroutunian 2019]. A version of the inner (random coding) bound was suggested in [Haroutunian 2020].

In this paper, we bring the improved inner bound with a full proof, introduce and analyze the concept of E - secrecy - capacity, as well as consider some special classes of wiretap channels.

The rest of the paper is structured as follows. In Section 2 notations, definitions and formulation of results are presented. The notion of E-secrecy capacity is introduced and discussed in Section 3. The particular cases of the generalized model are considered in Section 4. The proof of the constructed bound is given in Section 5. The paper is summarized in section 6.

2 Notations, Definitions and Formulation of Results

Consider the DMC $W(y,z|x)$ with finite input alphabet $\mathcal{X}$, finite output alphabets $\mathcal{Y}$ and $\mathcal{Z}$, where the memoryless property is expressed as

$$W^N(\mathbf{y},\mathbf{z}|\mathbf{x}) = \prod_{n=1}^{N} W(y,z|x).$$

Let us denote

$$W_1(y|x) = \sum_z W(y,z|x),$$

$$W_2(z|x) = \sum_y W(y,z|x).$$

To formulate the problem, consider auxiliary random variables U and Q with values in finite sets $\mathcal{U}$ and $\mathcal{Q}$, correspondingly, that satisfy the Markov chain relationship: $Q \to U \to X \to (Y,Z)$.

Let the probability distribution (PD) of random variables (RVs) Q and U be

$$P_0 = \{P_0(q,u), q \in \mathcal{Q}, u \in \mathcal{U}\}$$

and

$$P_1 = \{P_1(x|u), x \in \mathcal{X}, u \in \mathcal{U}\}$$

be conditional PD of RV X for a given value u. Joint PD of RVs U, X we denote by

$$P_{0,1} = \{P_{0,1}(u,x) = P_0(u)P_1(x|u), u \in \mathcal{U}, x \in \mathcal{X}\}$$

and the marginal PD of X is

$$P = \{P(x) = \sum_u P_{0,1}(u,x), u \in \mathcal{U}, x \in \mathcal{X}\}.$$

We denote

$$\begin{aligned} P_1W_1(y|u) &= \textstyle\sum_x P_1(x|u)W_1(y|x), \\ P_1W_2(z|u) &= \textstyle\sum_x P_1(x|u)W_2(z|x). \end{aligned} \tag{1}$$

We shall use also the PD $V = \{V(y|x), x \in \mathcal{X}, y \in \mathcal{Y}\}$.

For N **length code** (f_N, g_N), where $f_N : \mathcal{M}_N \to \mathcal{X}^N$ is **encoding** and $g_N : \mathcal{Y}_N \to \mathcal{M}_N$ **decoding**, **code rate** is

$$R(f_N, g_N) = \frac{1}{N} \log |\mathcal{M}_N|$$

(log and exp are taken to the base 2). **Average error probability** is defined as

$$e(f_N, g_N, W_1) = \frac{1}{|\mathcal{M}_N|} \sum_{m \in \mathcal{M}_N} W_1^N\{\mathcal{Y}^N - g_N^{-1}(m) | f_N(m)\},$$

where $g^{-1}(m) = \{\mathbf{y} : g(\mathbf{y}) = m\}$ and '–' is the operation between sets.

The secrecy level of a confidential message m at the wiretapper is measured by the **equivocation rate**, defined as

$$R_e^N = \frac{1}{N} H_{P_{01},W_2}(M|Z^N),$$

where $H_{P_{01},W_2}(M|Z^N)$ is the conditional entropy [Cover and Thomas 2006] with distributions P_{01}, W_2. In other words, the equivocation rate indicates the eavesdropper's uncertainty about the message m given the channel outputs Z^N. Hence, the larger the equivocation rate, the higher the level of secrecy.

The rate – equivocation pair (R, R_e) is **achievable** if there exists a sequence of message sets $\mathcal{M}_N$ with $|\mathcal{M}_N| = \exp NR$ and encoder – decoder (f_N, g_N) such that the average error probability tends to zero as N goes to infinity, and the equivocation rate R_e satisfies

$$R_e \leq \lim_{N\to\infty} \inf R_e^N.$$

The rate – equivocation pair (R, R_e) indicates the confidential rate R achieved at a certain secrecy level R_e.

The **capacity - equivocation region** $\mathcal{C}(W)$ is defined to be the closure of the set that consists of all achievable rate – equivocation pairs (R, R_e).

The following result was obtained in [Csiszár and Körner 1978] as a special case of a more general result for the broadcast channel with confidential messages.

Theorem 1. *The capacity - equivocation region of wiretap channel is given by*

$$\mathcal{C}(W) = \bigcup_{P_{0,1}} \left\{ \begin{array}{l} (R, R_e) : Q \to U \to X \to (Y, Z), \\ R \leq I_{P_{0,1},W_1}(U;Y), \\ 0 \leq R_e \leq R, \\ R_e \leq I_{P_{0,1},W_1}(U;Y|Q) - I_{P_{0,1},W_2}(U;Z|Q) \end{array} \right\}, \tag{2}$$

where for generic random variables X and Y, $I(X;Y)$ denotes the mutual information between RVs X and Y [Cover and Thomas 2006] . The auxiliary random variables Q and U are bounded in cardinality by $|\mathcal{Q}| \leq |\mathcal{X}| + 3$ and $|\mathcal{U}| \leq |\mathcal{X}|^2 + 4|\mathcal{X}| + 3$, respectively.

From this theorem the following corollary was obtained on **secrecy capacity** ([Csiszár and Körner 1978]), which is defined as the maximum rate at which the message m can be transmitted while being kept perfectly secret from the eavesdropper. Here **perfect secrecy** means that observing **z** will not add information about m to the eavesdropper.

Corollary 1. The secrecy capacity of the wiretap channel is given by

$$C_s(W) = \max_{P_{0,1}} [I_{P_{0,1},W_1}(U;Y) - I_{P_{0,1},W_2}(U;Z)],$$

where the auxiliary random variable U satisfies the Markov chain relationship: $U \to X \to (Y, Z)$ and is bounded in cardinality by $|\mathcal{U}| \leq |\mathcal{X}| + 1$.

We investigate the E **- capacity - equivocation region** $\mathcal{C}(E, W)$, which is defined as the closure of the set that consists of all E - achievable rate – equivocation pairs

$(R(E), R_e), E > 0$ with the average error probability satifying $e(f_N, g_N, W_1) \leq \exp\{-NE\}$.

To study this region, a general approach includes two stages: finding

- the achievability region or the inner bound, that is: any rate pair in the region can be achieved by a certain code,

- the converse region or the outer bound, that is: no rate pairs outside the region can be achieved.

The outer bound or the so-called sphere packing bound of E - capacity - equivocation region was obtained in [Haroutunian 2019], where the following theorem was proved.

Theorem 2. *For $E > 0$, the outer bound for E - capacity - equivocation region of generalized wiretap channel is given by*

$$\mathcal{C}(E, W) \leq \mathcal{R}_{sp}(E, W)$$

with

$$\mathcal{R}_{sp}(E, W) = \bigcup_{P_{0,1}} \left\{ \begin{array}{l} (R(E), R_e) : Q \to U \to X \to (Y, Z), \\ R(E) \leq \min\limits_{P_1 V : D(P_1 V || P_1 W_1 | P_0) \leq E} I_{P_{0,1},V}(U; Y), \\ 0 \leq R_e \leq R(E), \\ R_e \leq I_{P_{0,1},W_1}(U; Y|Q) - I_{P_{0,1},W_2}(U; Z|Q) \end{array} \right\}, \quad (3)$$

where $D(P_1 V || P_1 W_1 | P_0)$ denotes the divergence between conditional distributions $P_1 V$ and $P_1 W_1$ given PD P_0 (for definition see [Cover and Thomas 2006]).

For the achievability part, a message splitting approach is used, when the source message m is split into two parts $m_0 \in \mathcal{M}_0, m_1 \in \mathcal{M}_1$ with the corresponding rates

$$R_0 = \frac{1}{N} \log |\mathcal{M}_{0,N}| \text{ and } R_1 = \frac{1}{N} \log |\mathcal{M}_{1,N}|.$$

The first part can be decoded by both the receiver and the wiretapper, while the remaining part is only for the legitimate receiver to decode and needs to be kept as secret as possible from the eavesdropper. This rate splitting technique is useful only for the channel models with secrecy constraint.

The inner bound, which is also called a random coding bound as per method of the proof, is given in the following theorem.

Theorem 3. *For $E > 0$, the inner bound for E - capacity - equivocation region of generalized wiretap channel is given by*

$$\mathcal{R}_r(E, W) \leq \mathcal{C}(E, W)$$

with

$$\mathcal{R}_r(E,W)=\bigcup_{P_{0,1}}\left\{\begin{array}{l}(R_0(E),R_1(E),R_e(E)):Q\to U\to X\to(Y,Z),\\ R_0(E)\le\min\{I_{P_{0,1},W_2}(Q;Z),\\ \min\limits_{P_1V:D(P_1V||P_1W_1|P_0)\le E}|I_{P_{0,1},V}(Q;Y)+\\ D(P_1V||P_1W_1|P_0)-E|^+\},\\ R_1(E)\le\min\limits_{P_1V:D(P_1V||P_1W_1|P_0)\le E}|I_{P_{0,1},V}(U;Y|Q)+\\ D(P_1V||P_1W_1|P_0)-E|^+,\\ 0\le R_e(E)\le R_0(E)+R_1(E),\\ R_e(E)\le\min\limits_{P_1V:D(P_1V||P_1W_1|P_0)\le E}|I_{P_{0,1},V}(U;Y|Q)+\\ D(P_1V||P_1W_1|P_0)-E|^+-I_{P_{0,1},W_2}(U;Z|Q)\end{array}\right\},\quad(4)$$

where $|a|^+=\max(a,0)$.

The full proof of this theorem is given in the appendix (Section 5).

The proofs are using the **method of types** [Csiszár 1998], the idea of which is to partition the set of all N-length sequences into classes according to their empirical distributions (types). Then useful properties are derived which include;

- the number of types is at most polynomial in N, whereas the number of sequences is exponential in N,
- if all sequences are drawn i.i.d. according to the same distribution then the sequences with the same type have the same probability that depends only on that type,
- number of sequences of a particular type class is also strongly bounded depending on that type.

The set of all $\mathbf{u}\in\mathcal{U}^N$ of the type P_0^N is denoted by $\mathcal{T}^N_{P_0}(U)$, and $\mathcal{T}^N_{P_{0,1}}(X|\mathbf{u})$ is the set of all vectors $\mathbf{x}\in\mathcal{X}^N$ with the conditional type $P_1^N(x|u)$ given $\mathbf{u}\in\mathcal{T}^N_{P_0}(U)$. For further notations and properties we refer to [Haroutunian et al. 2007] section 1.4, or [Cover and Thomas 2006] section 12.1.

Corollary 2. When $E\to 0$, the inner and outer bounds coincide and are equal to the capacity - equivocation region (2) obtained in [Csiszár and Körner 1978].

Indeed, the statement of the corollary 2 for the outer bound is obvious. To establish the statement for the inner bound that is

$$\mathcal{C}(W)=\lim_{E\to 0}\mathcal{R}_r(E,W),$$

notice that

$$\lim_{E\to 0}\mathcal{R}_r(E,W)=\bigcup_{P_{0,1}}\left\{\begin{array}{l}(R_0,R_1,R_e):Q\to U\to X\to(Y,Z),\\ R_0\le\min\{I_{P_{0,1},W_1}(Q;Y),I_{P_{0,1},W_2}(Q;Z)\}\\ R_1\le I_{P_{0,1},W_1}(U;Y|Q),\\ 0\le R_e\le R_0+R_1,\\ R_e\le I_{P_{0,1},W_1}(U;Y|Q)-I_{P_{0,1},W_2}(U;Z|Q)\end{array}\right\}=$$

$$\bigcup_{P_{0,1}}\left\{\begin{array}{l}(R,R_e):Q\to U\to X\to(Y,Z),\\ R\le\min\{I_{P_{0,1},W_1}(Q;Y),I_{P_{0,1},W_2}(Q;Z)\}+I_{P_{0,1},W_1}(U;Y|Q),\\ 0\le R_e\le R\\ R_e\le I_{P_{0,1},W_1}(U;Y|Q)-I_{P_{0,1},W_2}(U;Z|Q)\end{array}\right\}.$$

It is clear that $\lim_{E\to 0}\mathcal{R}_r(E,W)\subset\mathcal{C}(W)$. To show the opposite, consider two cases: for any $(R,R_e)\in\mathcal{C}(W)$ if

- $I_{P_{0,1},W_1}(Q;Y)\le I_{P_{0,1},W_2}(Q;Z)$, then $(R,R_e)\in\lim_{E\to 0}\mathcal{R}_r(E,W)$,
- $I_{P_{0,1},W_1}(Q;Y)>I_{P_{0,1},W_2}(Q;Z)$, then

$$R_e\le I_{P_{0,1},W_1}(U;Y|Q)-I_{P_{0,1},W_2}(U;Z|Q)$$

$$=I_{P_{0,1},W_1}(U;Y)-I_{P_{0,1},W_1}(Q;Y)-I_{P_{0,1},W_2}(U;Z)+I_{P_{0,1},W_2}(Q;Z)$$

$$<I_{P_{0,1},W_1}(U;Y)-I_{P_{0,1},W_2}(U;Z).$$

The required result is achieved by setting $Q=\emptyset$.

3 E - Secrecy - Capacity

Since the case of perfect secrecy, when $R_1=R_e$, is of particular interest, it is also logical to consider the function of perfect secrecy depending on the reliability E.

Thus, we introduce the concept of E **- secrecy - capacity** $C_s(E,W)$, which for each E is the largest rate achievable with perfect secrecy and, hence, can be expressed as

$$C_s(E,W)=\max_{R_1(E)=R_e(E)}R_1(E).$$

From this definition and taking into account that $R(E)$ is a decreasing function, we derive the upper and lower bounds of this function. The **upper bound** will be

$$C_s(E,W)\le\left\{\begin{array}{l}\max\limits_{P_{0,1}}[I_{P_{0,1},W_1}(U;Y)-I_{P_{0,1},W_2}(U;Z)],\ for E\le E^*_{sp},\\ \max\limits_{P_{0,1}}\min\limits_{P_1V:D(P_1V||P_1W_1|P_0)\le E}I_{P_{0,1},V}(U;Y),\ for E\ge E^*_{sp}\end{array}\right\},$$

where E_{sp}^* is the value of E, for which

$$\max_{P_{0,1}}[I_{P_{0,1},W_1}(U;Y) - I_{P_{0,1},W_2}(U;Z)] = \max_{P_{0,1}\,P_1V:D(P_1V||P_1W_1|P_0)\le E} \min I_{P_{0,1},V}(U;Y).$$

Actually, for small E the situation is similar to the case with secrecy capacity, because

$$\max_{P_{0,1}}[I_{P_{0,1},W_1}(U;Y) - I_{P_{0,1},W_2}(U;Z)] \le \max_{P_{0,1}\,P_1V:D(P_1V||P_1W_1|P_0)\le E} \min I_{P_{0,1},V}(U;Y)$$

and $\max_{P_{0,1}}[I_{P_{0,1},W_1}(U;Y) - I_{P_{0,1},W_2}(U;Z)]$ is the maximal value of $R(E)$ for which $R(E) = R_e(E)$. As $R(E)$ is decreasing on E, for E greater than E_{sp}^* it becomes

$$\max_{P_{0,1}}[I_{P_{0,1},W_1}(U;Y) - I_{P_{0,1},W_2}(U;Z)] \ge \max_{P_{0,1}\,P_1V:D(P_1V||P_1W_1|P_0)\le E} \min I_{P_{0,1},V}(U;Y).$$

Hence for $E \ge E_{sp}^*$ E-secrecy capacity can not be greater than

$$\max_{P_{0,1}\,P_1V:D(P_1V||P_1W_1|P_0)\le E} \min I_{P_{0,1},V}(U;Y).$$

The **lower bound** of E-secrecy capacity will be

$$C_s(E,W) \ge \max_{P_{0,1}} \Bigg[\min_{P_1V:D(P_1V||P_1W_1|P_0)\le E} |I_{P_{0,1},V}(U;Y|Q)$$

$$+D(P_1V||P_1W_1|P_0) - E|^+ - I_{P_{0,1},W_2}(U;Z|Q)\Big] .$$

When $E \to 0$ bounds coincide and are equal to $C_s(W)$.

4 Some Special Classes of Wiretap Channels

The E-capacity-equivocation region similar to capacity - equivocation region has simpler form for special cases of considered model. We discuss here some of them.

4.1 The channel to the legitimate receiver is less noisy than the channel to the wiretapper

It means that

$$I_{P_{0,1},W_2}(U;Z) \le I_{P_{0,1},W_1}(U;Y),$$

for every $U \to X \to (Y,Z)$.

It is clear that the secrecy capacity is always positive unless W_2 is less noisy than W_1.

The capacity - equivocation region and the secrecy capacity for this class were obtained in [Csiszár and Körner 1978]:

$$\mathcal{C}(W) = \bigcup_P \left\{ \begin{array}{l} (R,R_e) : R \le I_{P,W_1}(X;Y), \\ 0 \le R_e \le R, \\ R_e \le I_{P,W_1}(X;Y) - I_{P,W_2}(X;Z), \end{array} \right\} \tag{5}$$

and

$$C_s(W) = \max_P [I_{P,W_1}(X;Y) - I_{P,W_2}(X;Z)]. \tag{6}$$

4.2 The channel to the legitimate receiver is more capable than the channel to the wiretapper

It means that

$$I_{P,W_2}(X;Z) \le I_{P,W_2}(X;Y),$$

for every input distribution P. This condition is weaker than the less noisy condition.

In [Csiszár and Körner 1978] it was shown that (6) is also true for this case.

4.3 Physically degraded wiretap channel

The wiretap channel is called physically degraded if X and Z are conditionally independent for a given Y, or $X \to Y \to Z$, in other words, the channel distribution satisfies

$$W(y,z|x) = W_1(y|x)W_2(z|x).$$

4.4 Stochastically degraded wiretap channel

The wiretap channel is called stochastically degraded if there exists a distribution $W(z|y)$ such that

$$W_2(z|x) = \sum_x W_1(y|x)W(z|y),$$

in other words, if the conditional marginal distribution of the wiretap channel is the same as that of a physically degraded one.

It is obvious that the degradedness condition is stronger than the less noisy condition, and, hence, both (5) and (6) hold for the degraded wiretap channel. That is why it is enough to consider only the "less noisy" case, as the result will be true also for other mentioned cases.

By the analogy of the proof of (5), we can obtain the upper and lower bounds of E - capacity equivocation region. The **upper bound** will be

$$\mathcal{R}_{sp}(E,W) = \bigcup_P \left\{ \begin{array}{l} (R(E), R_e) : U \to X \to (Y,Z), \\ R(E) \le \min\limits_{V: D(V||W_1|P) \le E} I_{P,V}(X;Y), \\ 0 \le R_e \le R(E), \\ R_e \le I_{P,W_1}(X;Y) - I_{P,W_2}(X;Z) \end{array} \right\}.$$

To prove this we must show that every bound in (3) is less than or equal to the corresponding bound here. It is obvious that for any V

$$I_{P_{0,1},V}(U;Y) \le I_{P,V}(X;Y),$$

as $U \to X \to Y$, hence

$$\min_{P_1 V: D(P_1 V||P_1 W_1|P_0) \le E} I_{P_{0,1},V}(U;Y) \le \min_{V: D(V||W_1|P) \le E} I_{P,V}(X;Y).$$

The second inequality is the same as in (5).

The **lower bounds** of E - capacity equivocation region for "less noisy" case will be

$$\mathcal{R}_r(E,W)=\bigcup_{P}\left\{\begin{array}{l}(R(E),R_e(E)):U\to X\to(Y,Z),\\ R(E)\le \min\limits_{V:D(V||W_1|P)\le E}|I_{P,V}(X;Y)+\\ D(V||W_1|P_0)-E|^+,\\ 0\le R_e(E)\le R(E)\\ R_e(E)\le \min\limits_{V:D(V||W_1|P)\le E}|I_{P,V}(X;Y)+\\ D(V||W_1|P)-E|^+-I_{P,W_2}(X;Z)\end{array}\right\}.$$

This bound follows from theorem 3 by setting $Q=\emptyset$ and $U=X$.

These upper and lower bounds coincide for small E and when $E\to 0$ coincide with (5).

5 Appendix: Proof of Theorem 3

To prove Theorem 4, we must show that the rate region specified in (4) is E - achievable for $E>0$. This is done by constructing a code of length N with certain properties based on the random coding technique.

The proof consists of 2 steps. In step 1, the existence of a code with the required properties is proved. In step 2, the estimation of the equivocation rate is given.

5.1 Step 1: Code construction

We must prove that for any $\delta>0$, $E>0$ and sufficiently large N there exists a code of length N with

$$|\mathcal{M}_{0,N}|=\exp\{N\min\{I_{P_{0,1},W_2}(Q;Z), \tag{7}$$

$$\min_{P_1V:D(P_1V||P_1W_1|P_0)\le E}|I_{P_{0,1},V}(Q;Y)+D(P_1V||P_1W_1|P_0)-E-\delta|^+\},$$

$$|\mathcal{M}_{1,N}|=\exp\{N\min_{P_1V:D(P_1V||P_1W_1|P_0)\le E}|I_{P_{0,1},V}(U;Y|Q)$$

$$+D(P_1V||P_1W_1|P_0)-E-\delta|^+, \tag{8}$$

such that

$$\frac{1}{N}\log|\mathcal{M}_{0,N}|\ge R_0,\ \ \frac{1}{N}\log|\mathcal{M}_{1,N}|\ge R_1$$

and the receiver decodes the messages m at rates (R_0,R_1) with $e(f_N,g_N,W_1)\le\exp\{-NE\}$, and the eavesdropper decodes m_0 at rate R_0 with small error probability ($e_2<\epsilon$).

Let

$$\mathcal{A}=\{1,...,A\},\ \ \mathcal{B}=\{1,...,B\},$$

where

$$A = \exp\{N\{\min_{P_1V: D(P_1V||P_1W_1|P_0)\le E} |I_{P_{0,1},V}(U;Y|Q) + D(P_1V||P_1W_1|P_0) - E|^+ - I_{P_{0,1},W_2}(U;Z|Q)\}, \quad (9)$$

$$B = \exp\{NI_{P_{0,1},W_2}(U;Z|Q)\}.$$

Let P_0^N be a type on $(\mathcal{Q}^N, \mathcal{U}^N)$ and P^N on $\mathcal{X}^N$. The random codebook is constructed by the following steps. $|\mathcal{M}_{0,N}|$ vectors $\mathbf{q}(m_0)$ are drawn uniformly, independently from $\mathcal{T}_{P_0}^N(Q)$. For each $\mathbf{q}(m_0) \in \mathcal{T}_{P_0}^N(Q)$ $A \times B$ vectors $\mathbf{u}(m_1|m_0)$ are drawn uniformly, independently from $\mathcal{T}_{P_0}^N(U|\mathbf{q}(m_0))$, where A and B satisfy (9), denote them by $\mathbf{u}(m_0, a, b)$, where m_0, a, b run over index sets $\mathcal{M}_{0,N}, \mathcal{A}, \mathcal{B}$. Finally, for each m_o the random sub-codebook of $A \times B$ codewords $\mathbf{ux}(m_0, a, b)$ is constructed by randomly choosing $\mathbf{x}(m_0, a, b)$ from $\mathcal{T}_{P_{0,1}}^N(X|\mathbf{u}(m_0, a, b))$ for each $\mathbf{u}(m_0, a, b)$ (Fig. 2).

	1	2	...	B
1	$\mathbf{ux}(m_0, 1, 1)$	$\mathbf{ux}(m_0, 1, 2)$	...	$\mathbf{ux}(m_0, 1, B)$
2	$\mathbf{ux}(m_0, 2, 1)$	$\mathbf{ux}(m_0, 2, 2)$	...	$\mathbf{ux}(m_0, 2, B)$
	...	...	...	...
A	$\mathbf{ux}(m_0, A, 1)$	$\mathbf{ux}(m_0, A, 2)$	...	$\mathbf{ux}(m_0, A, B)$

Figure 2: Sub-codebook for each m_0

Such a codebook is used because the eavesdropper can decode the column index b at the maximum rate that its channel supports and is not able to decode the row index.

For decoding we use the **divergence minimization criterion** suggested by E. Haroutunian [Haroutunian 2007] and successfully applied for various models [Haroutunian et al. 2007]. The idea of this criterion is the following. Each output vector $\mathbf{y}$ has various conditional types P_1V with various vectors $\mathbf{u}(m_0, a, b)$. The decoder is looking for that P_1V, for which the divergence $D(P_1V||P_1W_1|P_0)$ is minimal. In other word, on the decoder g, each $\mathbf{y}$ is decoded to such (m_0, a, b) for which $\mathbf{y} \in \mathcal{T}_{P_1V}^N(Y|\mathbf{u}(m_0, a, b))$ with P_1V that minimizes $D(P_1V||P_1W_1|P_0)$, i. e.

$$(m_0, a, b) = \operatorname*{argmin}_{P_1V: \mathbf{y} \in \mathcal{T}_{P_1V}^N(Y|\mathbf{u}(m_0,a,b))} D(P_1V||P_1W_1|P_0).$$

Decoder g can make an error if (m_0, a, b) is transmitted, but there exists some $(m_0', a', b') \neq (m_0, a, b)$ with which the output $\mathbf{y}$ has some P_1V' conditional type with smaller divergence, i. e.

$$\mathbf{y} \in \mathcal{T}_{P_1V}^N(Y|\mathbf{u}(m_0, a, b)) \bigcap \mathcal{T}_{P_1V'}^N(Y|\mathbf{u}(m_0', a', b'))$$

and

$$D(P_1V'||P_1W_1|P_0) \le D(P_1V||P_1W_1|P_0). \tag{10}$$

Hence, the set of all possible vectors $\mathbf{y}$ that can lead to an error of m_0 at the receiver is

$$\mathcal{S}_0(P_1V, P_1V') = \mathcal{T}^N_{P_1V}(Y|\mathbf{u}(m_0,a,b)) \bigcap \bigcup_{m_0 \neq m_0'(a,b)} \bigcup \mathcal{T}^N_{P_1V'}(Y|\mathbf{u}(m_0',a,b).$$

and the set of all possible vectors $\mathbf{y}$ that can lead to an error of (a,b) for a given m_0 at the receiver is

$$\mathcal{S}_1(P_1V, P_1V', m_0) = \mathcal{T}^N_{P_1V}(Y|\mathbf{u}(m_0,a,b)) \bigcap \bigcup_{(a',b') \neq (a,b)} \mathcal{T}^N_{P_1V'}(Y|\mathbf{u}(m_0,a',b').$$

We denote by $\mathcal{D}^N(P_0)$ the set of all types P_1, V, P_1V' that satisfy (10). Now the error probability will be estimated as follows.

$$e(f_N, g_N, W_1) = \frac{1}{|\mathcal{M}_N|} \sum_{m \in \mathcal{M}_N} W_1^N\{\mathcal{Y}^N - g^{-1}(m)|f(m)\}$$

$$= \frac{1}{|\mathcal{M}_{0,N}| \times A \times B} \sum_{m_0 \in \mathcal{M}_{0,N}} \sum_{a \in \mathcal{A}, b \in \mathcal{B}} W_1^N\{\mathcal{Y}^N - g^{-1}(m)|\mathbf{x}(m_0,a,b)\}$$

$$= \frac{1}{|\mathcal{M}_{0,N}| \times A \times B} \sum_{\mathbf{q}(m_0)} \sum_{\mathbf{u}(m_0,a,b)} \sum_{\mathbf{x}(m_0,a,b)} P_1^N(\mathbf{x}(m_0,a,b)|\mathbf{u}(m_0,a,b)) \times$$

$$W_1^N\{\mathcal{Y}^N - g^{-1}(m)|\mathbf{x}(m_0,a,b)\},$$

where the sums are taken over the following sets

$$\mathbf{q}(m_0) \in \mathcal{T}^N_{P_0}(Q) \cap f(\mathcal{M}_{0,N}), \;\; \mathbf{u}(m_0,a,b) \in \mathcal{T}^N_{P_0}(U|\mathbf{q}(m_0)) \cap f(\mathcal{A} \times \mathcal{B}),$$

$$\mathbf{x}(m_0,a,b) \in \mathcal{T}^N_{P_{0,1}}(X|\mathbf{u}(m_0,a,b)).$$

Here and below, for brevity, we only mention the indices over which we sum, so the last expression equals

$$\frac{1}{|\mathcal{M}_{0,N}| \times A \times B} \sum_{m_0 \in \mathcal{M}_{0,N}} \sum_{a \in \mathcal{A}, b \in \mathcal{B}} P_1 W_1^N\{\mathcal{Y}^N - g^{-1}(m_0,a,b)|\mathbf{u}(m_0,a,b)\}$$

$$\le \frac{1}{|\mathcal{M}_{0,N}| \times A \times B} \sum_{m_0 \in \mathcal{M}_{0,N}} \sum_{a \in \mathcal{A}, b \in \mathcal{B}} P_1 W_1^N\{ \bigcup_{P_1V, P_1V' \in \mathcal{D}^N(P_0)} \mathcal{S}_0(P_1V, P_1V')$$

$$\bigcup \mathcal{S}_1(P_1V, P_1V', m_0)|\mathbf{u}(m_0,a,b)\}.$$

Taking into account that $P_1W_1(\mathbf{y}|\mathbf{u})$ is constant for fixed types P_0, P_1V and equals

$$P_1W_1(\mathbf{y}|\mathbf{u}) = \exp\{-N[D(P_1V||P_1W_1|P_0) + H_{P_{0,1},V}(Y|U)]\},$$

(follows from the property of method of types) the error probability will be upper

estimated by

$$\frac{1}{|\mathcal{M}_{0,N}|\times A\times B}\sum_{m_0\in\mathcal{M}_{0,N}}\sum_{a\in\mathcal{A},b\in\mathcal{B}}\sum_{P_1V,P_1V'\in\mathcal{D}^N(P_0)}\exp\{-N[D(P_1V||P_1W_1|P_0)$$

$$+H_{P_{0,1},V}(Y|U)]\}\,[|\mathcal{S}_0(P_1V,P_1V')|+|\mathcal{S}_1(P_1V,P_1V',m_0)|]\,. \tag{11}$$

We will show that the following statement is true.

Lemma 1. *There exists at least one code such that for every $m_0\in\mathcal{M}_{0,N}, a\in\mathcal{A}, b\in\mathcal{B}$ and for any conditional types P_1V, P_1V' and N large enough*

$$|\mathcal{S}_0(P_1V,P_1V')|\le$$

$$\exp\{NH_{P_{0,1},V}(Y|U)\}\exp\{-N|E-D(P_1V'||P_1W_1|P_0)|^+\}, \tag{12}$$

and

$$|\mathcal{S}_1(P_1V,P_1V',m_0)|\le$$

$$\exp\{NH_{P_{0,1},V}(Y|U)\}\exp\{-N|E-D(P_1V'||P_1W_1|P_0)|^+\}. \tag{13}$$

Then from (11), (12) and (13) we will obtain that error probability is not greater than

$$e(f_N,g_N,W_1)\le$$

$$\frac{1}{|\mathcal{M}_{0,N}|\times A\times B}\sum_{m_0\in\mathcal{M}_{0,N}}\sum_{a\in\mathcal{A},b\in\mathcal{B}}\sum_{P_1V,P_1V'\in\mathcal{D}^N(P_0)}2\exp\{-N[D(P_1V||P_1W_1|P_0)$$

$$+H_{P_{0,1},V}(Y|U)]\}\exp\{NH_{P_{0,1},V}(Y|U)\}\exp\{-N|E-D(P_1V'||P_1W_1|P_0)|^+\}$$

$$\le\exp\{-N(E-\epsilon)\},\ \epsilon>0.$$

The last inequality is true, since types P_1V, P_1V' from $\mathcal{D}^N(P_0)$ satisfy (10) and the number of all possible P_1V, P_1V' according to the properties of the method of types is not greater than $(N+1)^{2|\mathcal{Y}||\mathcal{U}|}$.

Proof of Lemma 1. First notice that if $\mathbf{u}(m_0,a,b)$ satisfies (12), (13) for any P_1V, P_1V', then $\mathbf{u}(m_0',a',b')\ne\mathbf{u}(m_0,a,b)$ for $(m,a,b)\ne(m',a',b')$. To verify this, it is enough to choose $P_1V=P_1V'$ and $D(P_1V'||P_1W_1|P_0)<E$. If P_1V' is such that

$$D(P_1V'||P_1W_1|P_0)\ge E,$$

then

$$\exp\{-N|E-D(P_1V'||P_1W_1|P_0)|^+\}=1$$

and (12), (13) are valid for any $|\mathcal{M}_{0,N}|$, A, B.

It remains to prove (12), (13) for P_1V', such that $D(P_1V'||P_1W_1|P_0)<E$. Let us denote this set by $\mathcal{D}(P_0,E)$

$$\mathcal{D}(P_0,E)=\{P_1V: D(P_1V'||P_1W_1|P_0)<E\}.$$

To this end it is enough to show that for N large enough

$$\sum_{P_1V'\in\mathcal{D}(P_0,E)} [\mathbf{E}|\mathcal{S}_0(P_1V,P_1V')| + \mathbf{E}|\mathcal{S}_1(P_1V,P_1V',m_0)|]$$

$$\times \exp\{N(E - D(P_1V'||P_1W_1|P_0) - H_{P_{0,1},V}(Y|U))\} \le 1.$$

For the random code the first mathematical expectation can be bounded in the following way

$$\mathbf{E}|\mathcal{S}_0(P_1V,P_1V')| \le \sum_{\mathbf{y}\in\mathcal{T}^N_{P_{0,1}V}(Y)} \sum_{m_0\ne m_0'} \Pr\{\mathbf{y}\in\mathcal{T}^N_{P_{0,1}V}(Y|\mathbf{u}(m_0,a,b))\}$$

$$\times \Pr\{\mathbf{y}\in\bigcup_{(a,b)}\mathcal{T}^N_{P_{0,1}V'}(Y|\mathbf{u}(m_0',a,b)\},$$

since the events in the brackets are independent. Notice, that the first probability is different from zero if and only if $\mathbf{y}\in\mathcal{T}^N_{P_{0,1}V}(Y)$, then for N large enough

$$\Pr\{\mathbf{y}\in\mathcal{T}^N_{P_{0,1}V}(Y|\mathbf{u}(m_0,a,b))\} = \frac{|\mathcal{T}^N_{P_{0,1}V}(U|\mathbf{y})|}{|\mathcal{T}^N_{P_{0,1}V}(U)|}$$

$$\le (N+1)^{|\mathcal{U}|}\exp\{N(H_{P_{0,1}V}(U|Y) - H_{P_0}(U))\} \le \exp\{-N(I_{P_{0,1}V}(U;Y) - \delta/4)\}.$$

Here the number of vectors in the type class was estimated by the method of types.

The second probability, by a similar reasoning, is upper estimated by

$$\Pr\{\mathbf{y}\in\bigcup_{(a,b)}\mathcal{T}^N_{P_{0,1}V'}(Y|\mathbf{u}(m_0',a,b)\} \le \Pr\{\mathbf{y}\in\mathcal{T}^N_{P_{0,1}V'}(Y|\mathbf{q}(m_0')\}$$

$$= \frac{|\mathcal{T}^N_{P_{0,1}V'}(Q|\mathbf{y})|}{|\mathcal{T}^N_{P_0V'}(Q)|} \le \exp\{-N(I_{P_{0,1}V'}(Q;Y) - \delta/4)\}.$$

Finally we have

$$\mathbf{E}|\mathcal{S}_0(P_1V,P_1V')| \le (|\mathcal{M}_{0,N}| - 1)|\mathcal{T}^N_{P_{0,1}V}(Y)| \times \exp\{-N(I_{P_{0,1}V}(U;Y)$$

$$+I_{P_{0,1}V'}(Q;Y) - \delta/2)\}.$$

From (7) it follows that for any $P_1V'\in\mathcal{D}(P_0,E)$

$$|\mathcal{M}_{0,N}| - 1 \le \exp\{N(I_{P_{0,1},V'}(Q;Y) + D(P_1V'||P_1W_1|P_0) - E - \delta)\}$$

and we obtain

$$\mathbf{E}|\mathcal{S}_0(P_1V,P_1V')|\exp\{N(E - H_{P_{0,1}V}(Y|U) - D(P_1V'||P_1W_1|P_0))\}$$

$$\le \exp\{-N\delta/2\}.$$

By analogy we obtain

$$\mathbf{E}|\mathcal{S}_1(P_1V, P_1V', m_0)| \exp\{N(E - H_{P_{0,1}V}(Y|U) - D(P_1V'||P_1W_1|P_0))\}$$

$$\leq \exp\{-N\delta/2\}.$$

It means that there exists at least one code satisfying properties (12) and (13). Lemma 1 is proved.

The proof of Theorem 4 will be completed by estimating the equivocation rate.

5.2 Step 2: Estimation of the equivocation rate

We now estimate the equivocation of $M = (M_0, M_1)$ at the eavesdropper.

$$\begin{aligned}
H_{P_{01}W_2}(M|Z^N) &= H_{P_{01}W_2}(M_0, M_1|Z^N) \geq H_{P_{01}W_2}(M_0|M_1, Z^N) \\
&= H_{P_{01}W_2}(Z^N, M_1|M_0) - H_{P_{01}W_2}(Z^N|M_0) \\
&= H_{P_{01}W_2}(Z^N, M_1, U^N|M_0) - H_{P_{01}W_2}(U^N|Z^N, M_1, M_0) - H_{P_{01}W_2}(Z^N|M_0) \\
&= H_{P_{01}W_2}(M_1, U^N|M_0) + H_{P_{01}W_2}(Z^N|M_1, U^N, M_0) \\
&\quad - H_{P_{01}W_2}(U^N|M_1, Z^N, M_0) - H_{P_{01}W_2}(Z^N|M_0) \\
&\geq H_{P_{01}W_2}(U^N|M_0) + H_{P_{01}W_2}(Z^N|U^N) \qquad (14) \\
&\quad - H_{P_{01}W_2}(U^N|M_0, M_1, Z^N) - H_{P_{01}W_2}(Z^N|M_0).
\end{aligned}$$

We will bound each term separately. Given $M = m$, U^N has $A \times B$ possible values. From [Csiszár and Körner 1978] we know that

$$H_{P_{01}W_2}(U^N|M_0) \geq \log A + \log B - 1$$

hence,

$$\frac{1}{N} H_{P_{01}W_2}(U^N|M_0) \geq \min_{P_1V: D(P_1V||P_1W_1|P_0) \leq E} |I_{P_{0,1},V}(U;Y|Q) +$$

$$D(P_1V||P_1W_1|P_0) - E - \delta/4|^+ - \frac{1}{N}. \qquad (15)$$

For the second term it is easy to see that

$$\frac{1}{N} H_{P_{01}W_2}(Z^N|U^N) = H_{P_{01}W_2}(Z|U), \qquad (16)$$

as $\mathbf{u} \in \mathcal{T}^N_{P_0}(U)$.

The third term in (14) can be upper bounded by Fano's inequality.

$$\frac{1}{N} H_{P_{01}W_2}(U^N|M_0, M_1, Z^N) \leq \frac{1}{N}(1 + e_2 \log(|\mathcal{M}_{0N}|AB)). \qquad (17)$$

To estimate the fourth term in (14), consider a RV $\hat{Z}$ as

$$\hat{\mathbf{z}} = \mathbf{z}, \text{ if } (\mathbf{q}(m_0), \mathbf{z}) \in \mathcal{T}^N_{P_0W_2}(QZ).$$

Then

$$H_{P_{01}W_2}(Z^N|M_0) \le H_{P_{01}W_2}(Z^N, \hat{Z}^N|M_0)$$
$$= H_{P_{01}W_2}(Z^N|M_0, \hat{Z}^N) + H_{P_{01}W_2}(\hat{Z}^N|M_0)$$
$$\le H_{P_{01}W_2}(Z^N|\hat{Z}^N) + H_{P_{01}W_2}(\hat{Z}^N|M_0). \tag{18}$$

Now, by Fano's inequality

$$\frac{1}{N}H_{P_{01}W_2}(Z^N|\hat{Z}^N) \le \frac{1}{N} + \epsilon \log |\mathcal{Z}|$$

and

$$\frac{1}{N}H_{P_{01}W_2}(\hat{Z}^N|M_0) \le H_{P_{01}W_2}(Z|Q).$$

Hence, from (18) the fourth term in (14) is

$$\frac{1}{N}H_{P_{01}W_2}(Z^N|M_0) \le H_{P_{01}W_2}(Z|Q). \tag{19}$$

Substituting (15), (16), (17) and (19) into (14), we obtain

$$\frac{1}{N}H_{P_{01}W_2}(M|Z^N) \ge \min_{P_1V:D(P_1V||P_1W_1|P_0)\le E} |I_{P_{0,1},V}(U;Y|Q)$$
$$+D(P_1V||P_1W_1|P_0) - E\delta/4|^+ - \frac{1}{N} + H_{P_{01}W_2}(Z|U) - H_{P_{01}W_2}(Z|Q)$$
$$-\frac{1}{N}(1 + e_2 \log(|\mathcal{M}_{0,N}|AB)).$$

Since the inequality is valid for N large enough, we conclude

$$\lim_{N\to\infty} \frac{1}{N}H_{P_{01}W_2}(M|Z^N) \ge \min_{P_1V:D(P_1V||P_1W_1|P_0)\le E} |I_{P_{0,1},V}(U;Y|Q)$$
$$+D(P_1V||P_1W_1|P_0) - E|^+ - I_{P_{01}W_2}(U;Z|Q).$$

By the definition of R_e we conclude

$$R_e(E) \le \min_{P_1V:D(P_1V||P_1W_1|P_0)\le E} |I_{P_{0,1},V}(U;Y|Q)$$
$$+D(P_1V||P_1W_1|P_0) - E|^+ - I_{P_{01}W_2}(U;Z|Q).$$

The proof of Theorem 3 is completed.

6 Conclusions and Future Work

E - capacity - equivocation region and E - secrecy - capacity new notions of wiretap channel are introduced and investigated by constructing outer and inner bounds. These notions are, correspondingly, the generalizations of capacity - equivocation region and secrecy - capacity introduced and studied by [Csiszár and Körner 1978], since the latter can be obtained from the corresponding constructed bounds as a particular case when $E \to 0$. Special classes of the basic wiretap channel are considered and the corresponding bounds are constructed. In the future, other models of wiretap channels will be investigated from this point of view.

References

[Chen, Vinck 2008] Chen Y., Vinck A. J. H.: "Wiretap channel with side information", IEEE Transactions on Information Theory, 54(1),(2008), 395–402. doi: 10.1109/TIT.2007.911157.

[Chia, Gamal 2012] Chia Y., Gamal A. E.: "Wiretap channel with causal state information", IEEE Transactions on Information Theory, 58(5), (2012), 2838–2849. doi: 10.1109/TIT.2011.2181329.

[Cover and Thomas 2006] Cover, T. M., Thomas, J. A.: "Elements of Information Theory". 2nd edn. A Wiley-Interscience Publication, USA (2006).

[Csiszár 1998] Csiszár, I.: "Method of types", IEEE Transactions on Information Theory, 44(6),(1998), 2505–-2523. doi: 10.1109/18.720546.

[Csiszár and Körner 1978] Csiszár, I., Körner, J.: "Broadcast channel with confidential messages", IEEE Transactions on Information Theory, 24(3), (1978), 339–-348. doi: 10.1109/TIT.1978.1055892.

[Goldfeld et al. 2020] Goldfeld Z., Cuff P., Permuter H. H.: "Wiretap channels with random states non-causally available at the encoder," IEEE Transactions on Information Theory, 66(3), (2020), 1497–1519. doi: 10.1109/TIT.2019.2952389.

[Han et al. 2019] Han T. S., Sasaki M.: "Wiretap channels with causal state information: strong secrecy," IEEE Transactions on Information Theory, 65(10), (2019), 6750–6765. doi: 10.1109/TIT.2019.2925611.

[Haroutunian 2007] Haroutunian, E.: "E-capacity of DMC", IEEE Transactions on Information Theory, 53(11),(2007), 4210–4220. doi: 10.1109/TIT.2007.907506.

[Haroutunian et al. 2007] Haroutunian, E., Haroutunian, M., Harutyunyan, A.: "Reliability criteria in information theory and in statistical hypothesis testing", Foundations and Trends in Communications and Information Theory, 4(2-3), (2007), 97–263. doi: 10.1561/0100000008.

[Haroutunian 2019] Haroutunian, M.: "Outer bound for E-capacity – equivocation region of the wiretap channel", In: 12th International Conference on Computer Science and Information technologies, Yerevan, Armenia (Sept. 2019) 129–-131. Reprint In: IEEE Revised selected papers,(2019), 93–95. doi: 10.1109/CSITechnol.2019.8895005.

[Haroutunian 2020] Haroutunian, M.: "Inner bound of E-capacity – equivocation region for the generalized wiretap channel", In: 2nd CODASSCA workshop, Yerevan, Armenia (2020), 117–122.

[Liang et al. 2008] Liang, Y., Poor, V., Shamai (Shitz), S.: "Information theoretic security", Foundations and Trends in Communications and Information Theory, 5(4-5), (2008), 355–580. DOI:10.1561/0100000036

[Liang et al. 2009] Liang, Y., Kramer, G., Poor, H.V. et al.: "Compound wiretap channels". J Wireless Com Network, 142374 (2009). https://doi.org/10.1155/2009/142374

[Nötzel et al. 2016] Nötzel J., Wiese M., Boche H.: ”The arbitrarily varying wiretap channel - secret randomness, stability and super-activation”, IEEE Transactions on Information Theory, 62(6), (2016), 3504–3531. doi: 10.1109/TIT.2016.2550587.

[Wang, Safavi-Naini 2016] Wang P., Safavi-Naini R.: ”A model for adversarial wire-tap channels,” IEEE Transactions on Information Theory, 62(2), (2016), 970–983. doi: 10.1109/TIT.2015.2503766.

[Wyner 1975] Wyner, A. D.: ”The wire-tap channel”, Bell System Technical Journal, 54(8), (1975), 1355–-1387.