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 $x(m) = (x_1, ..., x_N) \in \mathcal{X}^N$, where $\mathcal{X}$ is a finite alphabet.
where $\mathcal{X}$ is the input alphabet, and $N$ is the transmission length. The codeword $x(m)$ is transmitted over a discrete memoryless channel (DMC) with transition probability $W(y, z|x)$. The noisy version $y \in \mathcal{Y}^N$ is accepted by the legitimate receiver, and $z \in \mathcal{Z}^N$ - by the eavesdropper, respectively. The decoder $g_N$ at the receiver maps the received sequence $y$ to an estimate $\hat{m}$ of the message.

![Diagram of generalized wiretap channel]

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 have 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-reliability 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 $X$, finite output alphabets $Y$ and $Z$, where the memoryless property is expressed as

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

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: $Q \rightarrow U \rightarrow X \rightarrow (Y, Z)$.

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

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

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

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

and the marginal PD of $X$ is

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

We denote

$$P_1W_1(y|u) = \sum_x P_1(x|u)W_1(y|x),$$

$$P_1W_2(z|u) = \sum_x P_1(x|u)W_2(z|x).$$

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

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

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

where $g^{-1}(m) = \{y : g(y) = m\}$ 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 $C(W)$ 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

$$C(W) = \bigcup_{P_{01}} \left\{ (R, R_e) : Q \to U \to X \to (Y, Z), \begin{array}{l} R \leq I_{P_{01}, W_1}(U; Y), \\ 0 \leq R_e \leq R, \\ R_e \leq I_{P_{01}, W_1}(U; Y|Q) - I_{P_{01}, W_2}(U; Z|Q) \end{array} \right\},$$

(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 $|Q| \leq |X| + 3$ and $|U| \leq |X|^2 + 4|X| + 3$, 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

$$C_s(W) = \max_{P_{01}} \left[ I_{P_{01}, W_1}(U; Y) - I_{P_{01}, W_2}(U; Z) \right],$$

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

We investigate the $E$ - capacity - equivocation region $C(E, W)$, 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 satisfying \( e(f_N, g_N, W_1) \leq \exp\{-NE\} \).

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

\[
\mathcal{R}_{sp}(E, W) = \bigcup_{P_{01}} \left\{ (R(E), R_e) : Q \rightarrow U \rightarrow X \rightarrow (Y, Z), \begin{align*}
R(E) &\leq \min_{P_{1V} : D(P_{1V} \mid \mid P_{1W_1}P_0) \leq E} I_{P_{01}V}(U; Y), \\
0 &\leq R_e \leq R(E), \\
R_e &\leq I_{P_{01}W_1}(U; Y | Q) - I_{P_{01}W_2}(U; Z | Q) \end{align*} \right\},
\]

where \( D(P_{1V} \mid \mid P_{1W_1}P_0) \) denotes the divergence between conditional distributions \( P_{1V} \) and \( P_{1W_1}P_0 \) 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

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

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

\[
\mathcal{R}_r(E, W) = \bigcup_{P_{0,1}} \begin{cases} 
(R_0(E), R_1(E), R_e(E)) : Q \rightarrow U \rightarrow X \rightarrow (Y, Z), \\
R_0(E) \leq \min \{I_{P_{0,1}}(Q; Z), \\
\min_{P_1: D(P_1 | P_0) \leq E} [I_{P_{0,1}}(Q; Y) + D(P_1 || P_1 W_1 | P_0) - E]^+}, \\
R_1(E) \leq \min_{P_1: D(P_1 | P_0) \leq E} [I_{P_{0,1}}(U; Y | Q) + D(P_1 || P_1 W_1 | P_0) - E]^+ - I_{P_{0,1}}(U; Z | Q)], \\
0 \leq R_e(E) \leq R_0(E) + R_1(E), \\
R_e(E) \leq \min_{P_1: D(P_1 | P_0) \leq E} [I_{P_{0,1}}(U; Y | Q) + D(P_1 || P_1 W_1 | P_0) - E]^+ - I_{P_{0,1}}(U; Z | Q) 
\end{cases}
\]

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 [Csiszar 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 \(u \in U^N\) of the type \(P_0^N\) is denoted by \(T_0^N(U)\), and \(T_{P_{0,1}}^N(X | u)\) is the set of all vectors \(x \in X^N\) with the conditional type \(P_{0,1}^N(x | u)\) given \(u \in T_{P_0}^N(U)\). 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 \(E \rightarrow 0\), the inner and outer bounds coincide and are equal to the capacity - equivocation region (2) obtained in [Csiszar 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

\[
C(W) = \lim_{E \rightarrow 0} \mathcal{R}_r(E, W),
\]
notice that

\[
\lim_{E \to 0} \mathcal{R}_r(E, W) = \bigcup_{P_{0:1}} \left\{ (R_0, R_1, R_c) : Q \to U \to X \to (Y, Z), \right. \\
\left. R_0 \leq \min \{ I_{P_{0:1}, W_1}(Q; Y), I_{P_{0:1}, W_2}(Q; Z) \} \\
R_1 \leq I_{P_{0:1}, W_1}(U; Y|Q), \right. \\
0 \leq R_c \leq R_0 + R_1, \\
R_c \leq I_{P_{0:1}, W_1}(U; Y|Q) - I_{P_{0:1}, W_2}(U; Z|Q) \right\}.
\]

It is clear that \( \lim_{E \to 0} \mathcal{R}_r(E, W) \subset \mathcal{C}(W) \). To show the opposite, consider two cases:
- \( I_{P_{0:1}, W_1}(Q; Y) \leq I_{P_{0:1}, W_2}(Q; Z) \), then \( (R, R_c) \in \lim_{E \to 0} \mathcal{R}_r(E, W) \),
- \( I_{P_{0:1}, W_1}(Q; Y) > I_{P_{0:1}, W_2}(Q; Z) \), then

\[
R_c \leq I_{P_{0:1}, W_1}(U; Y|Q) - I_{P_{0:1}, W_2}(U; Z|Q)
\]
\[
= I_{P_{0:1}, W_1}(U; Y) - I_{P_{0:1}, W_1}(Q; Y) - I_{P_{0:1}, W_2}(U; Z) + I_{P_{0:1}, W_2}(Q; Z)
\]
\[
< I_{P_{0:1}, W_1}(U; Y) - I_{P_{0:1}, W_2}(U; Z).
\]

The required result is achieved by setting \( Q = 0 \).

3 E - Secrecy - Capacity

Since the case of perfect secrecy, when \( R_1 = R_c \), 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

\[
C_s(E, W) = \max_{R_1(E) = R_c(E)} R_1(E).
\]

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

\[
C_u(E, W) \leq \left\{ \begin{array}{ll}
\max_{P_{0:1}} & \max_{P_{0:1}} [I_{P_{0:1}, W_1}(U; Y) - I_{P_{0:1}, W_2}(U; Z)], \text{for } E \leq E_{sp}^*, \\
\min_{P_{0:1} P_{1:V}: D(P_{1:V}, P_{0:1}|P_{0:1}) \leq E} & I_{P_{0:1}, V}(U; Y), \text{for } E \geq E_{sp}^* \end{array} \right\},
\]
where $E_{sp}$ is the value of $E$, for which
\[
\max_{P_{0,1}} [I_{P_{0,1}, W_1}(U; Y) - I_{P_{0,1}, W_2}(U; Z)] = \max_{P_{0,1}} \min_{P_1, V: D(P_1 V || P_1 W_1 | P_0) \leq E} I_{P_{0,1}, V}(U; Y).
\]
Actually, for small $E$ the situation is similar to the case with secrecy capacity, because
\[
\max_{P_{0,1}} [I_{P_{0,1}, W_1}(U; Y) - I_{P_{0,1}, W_2}(U; Z)] \leq \max_{P_{0,1}} \min_{P_1, V: D(P_1 V || P_1 W_1 | P_0) \leq E} I_{P_{0,1}, V}(U; Y)
\]
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
\[
\max_{P_{0,1}} [I_{P_{0,1}, W_1}(U; Y) - I_{P_{0,1}, W_2}(U; Z)] \geq \max_{P_{0,1}} \min_{P_1, V: D(P_1 V || P_1 W_1 | P_0) \leq E} I_{P_{0,1}, V}(U; Y).
\]
Hence for $E \geq E_{sp}$, $E$-secrecy capacity can not be greater than
\[
\max_{P_{0,1}} \min_{P_1, V: D(P_1 V || P_1 W_1 | P_0) \leq E} I_{P_{0,1}, V}(U; Y).
\]
The lower bound of $E$-secrecy capacity will be
\[
C_s(E, W) = \max_{P_{0,1}} \left[ \min_{P_1, V: D(P_1 V || P_1 W_1 | P_0) \leq E} |I_{P_{0,1}, V}(U; Y)|Q) + D(P_1 V || P_1 W_1 | P_0) - E|^+ - I_{P_{0,1}, W_2}(U; Z|Q). \right.
\]
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
\[
I_{P_{0,1}, W_2}(U; Z) \leq I_{P_{0,1}, W_1}(U; Y),
\]
for every $U \rightarrow X \rightarrow (Y, Z)$.

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]:
\[
C(W) = \bigcup P \left\{ \begin{array}{l}
(R, R_e) : R \leq I_{P, W_1}(X; Y), \\
0 \leq R_e \leq R, \\
R_e \leq I_{P, W_1}(X; Y) - I_{P, W_2}(X; Z),
\end{array} \right\}
\]
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

\[ I_{P,W_2}(X;Z) \leq I_{P,W_2}(X;Y), \]

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 \( X \rightarrow Y \rightarrow Z \), 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

\[ W_2(z|x) = \sum_y W_1(y|x)W(z|y), \]

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

\[
\mathcal{R}_{sp}(E,W) = \bigcup_P \left\{ (R(E), R_e) : U \rightarrow X \rightarrow (Y, Z), \begin{array}{l}
R(E) \leq \min_{V : D(V||W_1|P) \leq E} I_{P,V}(X;Y), \\
0 \leq R_e \leq R(E), \\
R_e \leq I_{P,W_1}(X;Y) - I_{P,W_2}(X;Z) 
\end{array} \right\}.
\]

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 \( V \)

\[ I_{P_0,V}(U;Y) \leq I_{P,V}(X;Y), \]

as \( U \rightarrow X \rightarrow Y \), hence

\[
\min_{P_1 : D(V||P_1||W_1|P_0) \leq E} I_{P_0,1,V}(U;Y) \leq \min_{V : D(V||W_1|P) \leq E} I_{P,V}(X;Y).
\]
The second inequality is the same as in (5).

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

$$
R_e(E, W) = \bigcup_P \left\{ (R(E), R_e(E)) : U \rightarrow X \rightarrow (Y, Z), \right. \\
R(E) \leq \min_{V, D(V||W_1|P) \leq E} |I_{P, V}(X; Y) + D(V||W_1|P) - E|^+, \\
0 \leq R_e(E) \leq R(E) \\
R_e(E) \leq \min_{V, D(V||W_1|P) \leq E} |I_{P, V}(X; Y)| + D(V||W_1|P) - E|^+ - I_{P, W_2}(X; Z) \bigg\}. 
$$

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

These upper and lower bounds coincide for small $E$ and when $E \rightarrow 0$ 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

$$
|\mathcal{M}_{0,N}| = \exp\{N \min_{P_{0,1,V} W_1} [I_{P_{0,1}, W_2}(Q; Z)],
$$

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

Let

$$
A = \{1, ..., A\}, \quad B = \{1, ..., B\},
$$
where

\[ A = \exp\left\{ N \min_{P_1V : D(P_1V || P_1W_1|P_0) \leq E} \left| I_{P_0,1,V}(U; Y|Q) + D(P_1V || P_1W_1|P_0) - E \right| \right\} \]

\[ B = \exp\{ NI_{P_0,1,W_2}(U; Z|Q) \}. \]

Let \( P_0^N \) be a type on \( (Q^N, U^N) \) and \( P^N \) on \( X^N \). The random codebook is constructed by the following steps. \( |\mathcal{M}_{0,N}| \) vectors \( q(m_0) \) are drawn uniformly, independently from \( \mathcal{T}_0^N(Q) \). For each \( q(m_0) \in \mathcal{T}_0^N(Q) \) \( A \times B \) vectors \( u(m_1|m_0) \) are drawn uniformly, independently from \( \mathcal{T}_0^N(U|q(m_0)) \), where \( A \) and \( B \) satisfy (9), denote them by \( u(m_0, a, b) \), where \( m_0, a, b \) run over index sets \( \mathcal{M}_{0,N}, A, B \). Finally, for each \( m_0 \), the random sub-codebook of \( A \times B \) codewords \( u(m_0, a, b) \) is constructed by randomly choosing \( x(m_0, a, b) \) from \( \mathcal{T}^N_{P_0}(X|u(m_0, a, b)) \) for each \( u(m_0, a, b) \) (Fig. 2).

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>...</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( u(x(m_0, 1, 1)) )</td>
<td>( u(x(m_0, 1, 2)) )</td>
<td>...</td>
<td>( u(x(m_0, 1, B)) )</td>
</tr>
<tr>
<td>2</td>
<td>( u(x(m_0, 2, 1)) )</td>
<td>( u(x(m_0, 2, 2)) )</td>
<td>...</td>
<td>( u(x(m_0, 2, B)) )</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>( u(x(m_0, A, 1)) )</td>
<td>( u(x(m_0, A, 2)) )</td>
<td>...</td>
<td>( u(x(m_0, A, B)) )</td>
</tr>
</tbody>
</table>

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. Harout unian [Haroutunian 2007] and successfully applied for various models [Haroutunian et al. 2007]. The idea of this criterion is the following. Each output vector \( x \) has various conditional types \( P_1V \) with various vectors \( u(m_0, a, b) \). 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 \( y \) is decoded to such \( (m_0, a, b) \) for which \( y \in \mathcal{T}^N_{P_1V}(Y|x(m_0, a, b)) \) with \( P_1V \) that minimizes \( D(P_1V || P_1W_1|P_0) \), i.e.

\[ (m_0, a, b) = \arg\min_{P_1V : y \in \mathcal{T}^N_{P_1V}(Y|x(m_0, a, b))} D(P_1V || P_1W_1|P_0). \]

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 \( y \) has some \( P_1V' \) conditional type with smaller divergence, i.e.

\[ y \in \mathcal{T}^N_{P_1V}(Y|x(m_0, a, b)) \cap \mathcal{T}^N_{P_1V'}(Y|x(m'_0, a', b')) \]
and
\[
D(P_1 V' || P_1 W_1 | P_0) \leq D(P_1 V || P_1 W_1 | P_0).
\]

Hence, the set of all possible vectors \( y \) that can lead to an error of \( m_0 \) at the receiver is
\[
S_0(P_1 V, P_1 V') = T^N_{P_1 V}(Y | \mathbf{u}(m_0, a, b)) \bigcap \bigcup_{m_0 \neq m'_0(a, b)} T^N_{P_1 V}(Y | \mathbf{u}(m'_0, a, b)).
\]

and the set of all possible vectors \( y \) that can lead to an error of \((a, b)\) for a given \( m_0 \) at the receiver is
\[
S_1(P_1 V, P_1 V', m_0) = T^N_{P_1 V}(Y | \mathbf{u}(m_0, a, b)) \bigcap \bigcup_{(a', b') \neq (a, b)} T^N_{P_1 V}(Y | \mathbf{u}(m_0, a', b')).
\]

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

\[
e(f_N, g_N, W_1) = \frac{1}{|\mathcal{M}_N|} \sum_{m \in \mathcal{M}_N} W^N_1 \{ \mathcal{Y}^N - g^{-1}(m) | f(m) \}
\]

\[
= \frac{1}{|\mathcal{M}_{0,N} \times A \times B|} \sum_{m_0 \in \mathcal{M}_{0,N}} \sum_{a \in A} \sum_{b \in B} W^N_1 \{ \mathcal{Y}^N - g^{-1}(m) | \mathcal{X}(m_0, a, b) \}
\]

\[
= \frac{1}{|\mathcal{M}_{0,N} \times A \times B|} \sum_{m_0 \in \mathcal{M}_{0,N}} \sum_{a \in A} \sum_{b \in B} P^N_1(\mathcal{X}(m_0, a, b)) \mathcal{X}(m_0, a, b) \times
\]

\[
W^N_1 \{ \mathcal{Y}^N - g^{-1}(m) | \mathcal{X}(m_0, a, b) \},
\]

where the sums are taken over the following sets
\[
\mathbf{q}(m_0) \in T^N_{P_0}(Q) \cap f(\mathcal{M}_{0,N}), \ \mathbf{u}(m_0, a, b) \in T^N_{P_0}(U | \mathbf{q}(m_0)) \cap f(A \times B),
\]

\[
\mathcal{X}(m_0, a, b) \in T^N_{P_0,1}(X | \mathbf{u}(m_0, a, b)).
\]

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

\[
\frac{1}{|\mathcal{M}_{0,N} \times A \times B|} \sum_{m_0 \in \mathcal{M}_{0,N}} \sum_{a \in A} \sum_{b \in B} P^N_1 \{ \mathcal{Y}^N - g^{-1}(m_0, a, b) | \mathbf{u}(m_0, a, b) \}
\]

\[
\leq \frac{1}{|\mathcal{M}_{0,N} \times A \times B|} \sum_{m_0 \in \mathcal{M}_{0,N}} \sum_{a \in A} \sum_{b \in B} P^N_1 \{ \bigcup_{P_1 V, P_1 V' \in \mathcal{D}^N(P_0)} S_0(P_1 V, P_1 V', m_0 | \mathbf{u}(m_0, a, b))
\]

\[
\bigcup \bigcup_{P_1 V, P_1 V' \in \mathcal{D}^N(P_0)} S_1(P_1 V, P_1 V', m_0 | \mathbf{u}(m_0, a, b)).
\]

Taking into account that \( P^N_1 \mathbf{y} | \mathbf{u} \) is constant for fixed types \( P_0, P_1 V \) and equals

\[
P^N_1 \mathbf{y} | \mathbf{u} = \exp \{-N[D(P_1 V || P_1 W_1 | P_0) + H_{P_0,1,V}(V | U)] \},
\]

(follows from the property of method of types) the error probability will be upper
denote this set by $|M|$ and (12), (13) are valid for any
number of all possible types $P_{1V}, P_{1V'}$ and $N$ large enough to choose $P_{1V}, P_{1V'}$ with

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 $(N + 1)^{2|D||B|}$.

Proof of Lemma 1. First notice that if $u(m_0, a, b)$ satisfies (12), (13) for any $P_{1V}, P_{1V'}$, then $u(m'_0, a', b') \neq u(m_0, a, b)$ for $(m, a, b) \neq (m', a', b')$. To verify this, it is enough to choose $P_{1V} = P_{1V'}$ and $D(P_{1V'}||P_{1V}|P_0) < E$. If $P_{1V'}$ is such that

then

and (12), (13) are valid for any $|M_{0,N}|, A, B$.

It remains to prove (12), (13) for $P_{1V'}$, such that $D(P_{1V'}||P_{1V}|P_0) < E$. Let us denote this set by $\mathcal{D}(P_0, E)$

$$\mathcal{D}(P_0, E) = \{ P_{1V} : D(P_{1V'}||P_{1V}|P_0) < E \}.$$

estimated by

$$\frac{1}{|M_{0,N}| \times A \times B} \sum_{m_0 \in M_{0,N}} \sum_{a \in A, b \in B} \sum_{P_{1V}, P_{1V'} \in \mathcal{D}^N(P_0)} \exp\{-N[D(P_{1V}||P_{1V}|P_0) - E]\}$$

$$+ H_{P_{0,1V}}(Y|U) \{ |S_0(P_{1V}, P_{1V'})| + |S_1(P_{1V}, P_{1V'}, m_0)| \}.$$  \hfill (11)

We will show that the following statement is true.

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

$$|S_0(P_{1V}, P_{1V'})| \leq \exp\{NH_{P_{0,1V}}(Y|U)\} \exp\{-N|E - D(P_{1V'}||P_{1V}|P_0)|^+\},$$  \hfill (12)

$$|S_1(P_{1V}, P_{1V'}, m_0)| \leq \exp\{NH_{P_{0,1V}}(Y|U)\} \exp\{-N|E - D(P_{1V'}||P_{1V}|P_0)|^+\}.$$  \hfill (13)

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

$$e(f_N, g_N, W_1) \leq \frac{1}{|M_{0,N}| \times A \times B} \sum_{m_0 \in M_{0,N}} \sum_{a \in A, b \in B} \sum_{P_{1V}, P_{1V'} \in \mathcal{D}^N(P_0)} 2 \exp\{-N[D(P_{1V}||P_{1V}|P_0) - E]\}$$

$$+ H_{P_{0,1V}}(Y|U) \{ |S_0(P_{1V}, P_{1V'})|^+ + \exp\{-N|E - \epsilon\} \}, \ \epsilon > 0.$$
To this end it is enough to show that for \( N \) large enough
\[
\sum_{P_1V' \in D(P_0, E)} |E|S_0(P_1 V, P_1 V')| + E|S_1(P_1 V, P_1 V', m_0)|
\]
\[
\times \exp\{N(E - D(P_1 V', P_1 W_1 | P_0) - H_{P_0, V}(Y | U))\} \leq 1.
\]
For the random code the first mathematical expectation can be bounded in the following way
\[
E|S_0(P_1 V, P_1 V')| \leq \sum_{y \in T_{P_0,1,V}(Y)} \sum_{m_0 \neq m'_0} \Pr\{y \in T_{P_0,1,V}^{N}(Y|u(m_0, a, b))\}
\]
\[
\times \Pr\{y \in \bigcup_{(a,b)} T_{P_0,1,V}^{N}(Y|u(m'_0, a, b)),
\]
since the events in the brackets are independent. Notice, that the first probability is different from zero if and only if \( y \in T_{P_0,1,V}^{N}(Y) \), then for \( N \) large enough
\[
\Pr\{y \in T_{P_0,1,V}^{N}(Y|u(m_0, a, b))\} = \frac{|\mathcal{T}_{P_0,1,V}^{N}(U|y)|}{|\mathcal{T}_{P_0,1,V}^{N}(U)|} \leq (N + 1)^{[\lambda]} \exp\{N(H_{P_0,1,V}(U|Y) - H_{P_0}(U))\} \leq \exp\{-N(I_{P_0,1,V}(U; Y) - \delta/4)\}.
\]
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
\[
\Pr\{y \in \bigcup_{(a,b)} T_{P_0,1,V}^{N}(Y|u(m'_0, a, b))\} \leq \Pr\{y \in T_{P_0,1,V}^{N}(Y|q(m'_0))\}
\]
\[
= \frac{|\mathcal{T}_{P_0,1,V}^{N}(Q|y)|}{|\mathcal{T}_{P_0,1,V}^{N}(Q)|} \leq \exp\{-N(I_{P_0,1,V}(Q; Y) - \delta/4)\}.
\]
Finally we have
\[
E|S_0(P_1 V, P_1 V')| \leq (|M_{0,N}| - 1)|\mathcal{T}_{P_0,1,V}^{N}(Y)| \times \exp\{-N(I_{P_0,1,V}(U; Y) + I_{P_0,1,V}(Q; Y) - \delta/2)\}.
\]
From (7) it follows that for any \( P_1 V' \in D(P_0, E) \)
\[
|M_{0,N}| - 1 \leq \exp\{N(I_{P_0,1,V}(Q; Y) + D(P_1 V'||P_1 W_1 | P_0) - E - \delta)\}
\]
and we obtain
\[
E|S_0(P_1 V, P_1 V')| \exp\{N(E - H_{P_0,1,V}(Y|U) - D(P_1 V'||P_1 W_1 | P_0))\}\]
\[
\leq \exp\{-N\delta/2\}.
\]
By analogy we obtain
\[ E[S_1(P_1V, P_1V', m_0)] \exp\{N(E - H_{P_01} Y|U) - D(P_1V||P_1W_1|P_0)\} \]
\[ \leq \exp\{-N\delta/2\}. \]

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.

\[ H_{P_01} w_2(M|Z) = H_{P_01} w_2(M_0, M_1|Z) \geq H_{P_01} w_2(M_0|M_1, Z) \]
\[ = H_{P_01} w_2(Z, M_1|M_0) - H_{P_01} w_2(Z|M_0) \]
\[ = H_{P_01} w_2(Z, M_1, U|M_0) - H_{P_01} w_2(U|Z, M_1, M_0) - H_{P_01} w_2(Z|M_0) \]
\[ = H_{P_01} w_2(M_1, U|M_0) + H_{P_01} w_2(Z|M_1, U, M_0) \]
\[ - H_{P_01} w_2(U|M_1, Z, M_0) - H_{P_01} w_2(Z|M_0) \]
\[ \geq H_{P_01} w_2(U|M_0) + H_{P_01} w_2(Z|U) \quad (14) \]
\[ - H_{P_01} w_2(U|M_0, M_1, Z) - H_{P_01} w_2(Z|M_0). \]

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

\[ H_{P_01} w_2(U|M_0) \geq \log A + \log B - 1 \]

hence,

\[ \frac{1}{N} H_{P_01} w_2(U|M_0) \geq \min_{P_{1V}:D(P_1V||P_1W_1|P_0) \leq E} J_{P_01, V(Y|Q)} + \]
\[ D(P_1V||P_1W_1|P_0) - E - \delta/4 \geq 0 \]
\[ = \frac{1}{N}. \quad (15) \]

For the second term it is easy to see that

\[ \frac{1}{N} H_{P_01} w_2(Z|U) = H_{P_01} w_2(Z), \quad (16) \]

as \( u \in T^N_0(U) \).

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

\[ \frac{1}{N} H_{P_01} w_2(U|M_0, M_1, Z) \leq \frac{1}{N} (1 + e_2 \log(|M_0N|AB)). \quad (17) \]
To estimate the fourth term in (14), consider a RV $\hat{Z}$ as
$$\hat{z} = z, \text{ if } (q(m_0), z) \in T_{P_0W_2}(QZ).$$

Then
$$H_{P_0W_2}(Z^N|M_0) \leq H_{P_0W_2}(Z^N, \hat{Z}^N|M_0)$$
$$= H_{P_0W_2}(Z^N|M_0, \hat{Z}^N) + H_{P_0W_2}(\hat{Z}^N|M_0)$$
$$\leq H_{P_0W_2}(Z^N|\hat{Z}^N) + H_{P_0W_2}(\hat{Z}^N|M_0).$$  \(18\)

Now, by Fano’s inequality
$$\frac{1}{N} H_{P_0W_2}(Z^N|\hat{Z}^N) \leq \frac{1}{N} + \epsilon \log |Z|$$
and
$$\frac{1}{N} H_{P_0W_2}(\hat{Z}^N|M_0) \leq H_{P_0W_2}(Z|Q).$$

Hence, from (18) the fourth term in (14) is
$$\frac{1}{N} H_{P_0W_2}(Z^N|M_0) \leq H_{P_0W_2}(Z|Q).$$  \(19\)

Substituting (15), (16), (17) and (19) into (14), we obtain
$$\frac{1}{N} H_{P_0W_2}(M|Z^N) \geq \min_{P_{1V}: D(P_1V||P_1W_1P_0) \leq E} \left| I_{P_01,V}(U;Y|Q) \right|$$
$$+ D(P_1V||P_1W_1P_0) - E \delta/4 |^+ - \frac{1}{N} + H_{P_0W_2}(Z|U) - H_{P_0W_2}(Z|Q)$$
$$- \frac{1}{N}(1 + e_2 \log(|Q_0N|AB)).$$

Since the inequality is valid for $N$ large enough, we conclude
$$\lim_{N \to \infty} \frac{1}{N} H_{P_0W_2}(M|Z^N) \geq \min_{P_{1V}: D(P_1V||P_1W_1P_0) \leq E} \left| I_{P_01,V}(U;Y|Q) \right|$$
$$+ D(P_1V||P_1W_1P_0) - E |^+ - I_{P_0W_2}(U;Z|Q).$$

By the definition of $R_e$ we conclude
$$R_e(E) \leq \min_{P_{1V}: D(P_1V||P_1W_1P_0) \leq E} \left| I_{P_01,V}(U;Y|Q) \right|$$
$$+ D(P_1V||P_1W_1P_0) - E |^+ - I_{P_0W_2}(U;Z|Q).$$

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 $E \rightarrow 0$. 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


[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,

tap channels," IEEE Transactions on Information Theory, 62(2), (2016), 970–983. doi:
10.1109/TIT.2015.2503766.

1355–1387.