# Partial Strong Converse for the Non-Degraded Wiretap Channel

Yi-Peng Wei Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
*ypwei@umd.edu* *ulukus@umd.edu*

***Abstract*—We prove the partial strong converse property for the discrete memoryless *non-degraded* wiretap channel, for which we require the leakage to the eavesdropper to vanish but allow an asymptotic error probability $\epsilon \in [0, 1)$ to the legitimate receiver. We show that when the transmission rate is above the secrecy capacity, the probability of correct decoding at the legitimate receiver decays to zero exponentially. Therefore, the maximum transmission rate is the same for $\epsilon \in [0, 1)$, and the partial strong converse property holds. Our work is inspired by a recently developed technique based on information spectrum method and Chernoff-Cramer bound for evaluating the exponent of the probability of correct decoding.**

## I. Introduction

We consider the discrete memoryless *non-degraded* wiretap channel, in which a transmitter wishes to send messages to a legitimate receiver while keeping the messages secret from an eavesdropper. The wiretap channel was first studied in [1] with the assumption that the wiretap channel is degraded, and the secrecy capacity of the *non-degraded* wiretap channel was determined in [2]. The general formula for the wiretap channel can be found in [3]. Although [1] and [2] provide the secrecy capacity for the wiretap channel, the proofs rely on Fano's inequality, and therefore, only a weak converse can be shown.

The strong converse property was first proposed in [4] for the point-to-point channel, and has received significant attention recently due to the study of finite block-length channel coding rate [5]–[7]. For the point-to-point channel, the strong converse property states that when the transmission rate is above the capacity, the asymptotic error probability goes to 1. This implies that if we allow a potentially non-zero asymptotic error probability $\epsilon \in [0, 1)$, the maximal transmission rate is still the same as the capacity, which only allows $\epsilon = 0$. That is, allowing a non-zero error probability does not increase the maximal rate. Reference [8] builds equivalent conditions for the strong converse property using the information spectrum method for the point-to-point channel, and [9, Section 3.7] extends it to channels with cost constraints.

The maximal transmission rate for the wiretap channel is constrained by two constraints: reliability and security. Let $\epsilon$ denote the asymptotic error probability for the reliability constraint, and let $\delta$ denote the variational distance for the secrecy constraint[1]. Reference [10] extends the method in [9, Section 3.7] to show the strong converse property for $(\epsilon, \delta) \in [0, 1) \times \{0\}$ for the degraded wiretap channel, and name it *partial strong converse* to account for the strict secrecy constraint. Reference [11] utilizes the relationship between the wiretap channel with feedback and secret key agreement [12] to show that the strong converse property holds when $\epsilon + \delta < 1$ for the degraded wiretap channel. For the degraded quantum wiretap channel, [13] develops a "pretty strong" converse. Reference [14] develops strong Fano's inequalities based on image size characterization, and shows that the partial strong converse property holds for the non-degraded wiretap channel.

Recently, a new strong converse technique has been proposed in [15]–[19]. This technique is based on a novel usage of information spectrum method [9] and a new recursive bounding method. The usage of information spectrum method provides an upper bound for the probability of correct decoding, and the recursive bounding method plays a role similar to single-letterization in the weak converse proof. It bounds the exponent function of the probability of correct decoding, and therefore shows that the probability of correct decoding goes to zero exponentially when the rate is above the capacity. This technique is general and has been applied to degraded broadcast channels in [15], degraded broadcast channels with feedback in [16], asymmetric broadcast channels in [17], state dependent channels in [18], and Wyner-Ziv coding in [19].

Inspired by this new technique, we show that the partial strong converse property holds for the non-degraded wiretap channel. We utilize the information spectrum method and Chernoff-Cramer bound to upper bound the probability of correct decoding. Under the condition that the leakage vanishes asymptotically, we show that the exponent function of the probability of correct decoding is strictly negative when the transmission rate is higher than the secrecy capacity. Thus, the probability of correct decoding decays to zero exponentially, and the partial strong converse property holds. The main difference between our work and [15]–[19] is that we do not construct the auxiliary distributions for the recursive bounding method for the purposes of single-letterization. Therefore, our method can be extended to channels with multi-letter characterizations [20]–[23] for their capacity regions.

This work was supported by NSF Grants CNS 13-14733, CCF 14-22111, CCF 14-22129, and CNS 15-26608.

[1] There are various kinds of secrecy constraints [3, Proposition 1]. For instance, [1] and [2] use normalized mutual information, and [10] and [11] use variational distance. We use normalized mutual information in this paper.

## II. Problem setting and Main Results

### A. System Model and Definitions

A wiretap channel consists of a transmitter (Alice) who wishes to send a message uniformly distributed in $\mathcal{M}_n$ to a legitimate receiver (Bob) secretly in the presence of an eavesdropper (Eve) through a channel $W^n : \mathcal{X}^n \to \mathcal{Y}^n \times \mathcal{Z}^n$. $\mathcal{X}$ denotes the input alphabet for Alice, while $\mathcal{Y}$ and $\mathcal{Z}$ denote the output alphabets for Bob and Eve, respectively. $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ are finite. Here, we consider the discrete memoryless channel, and therefore, we have

$$W^n(y^n, z^n|x^n) = \prod_{t=1}^{n} W(y_t, z_t|x_t), \tag{1}$$

where $W(y,z|x)$ is the conditional probability mass function (pmf) of the channel.

In the following, $X^n$ denotes a random variable taking values in $\mathcal{X}^n$, and the elements of $\mathcal{X}^n$ are denoted by $x^n$. The pmf of random variable $X^n$ is denoted by $p_{X^n}$. Similar notation also applies to other random variables. To satisfy the secrecy constraint, we require

$$\lim_{n\to\infty} \frac{1}{n} I(M_n; Z^n) = 0. \tag{2}$$

The encoder $\phi^{(n)}$ maps the message $m \in \mathcal{M}_n$ to a codeword $x^n \in \mathcal{X}^n$. We allow the encoder $\phi^{(n)}$ to be a stochastic encoder and denote it as $\phi^{(n)} = \{\phi^{(n)}(x^n|m)\}_{(m,x^n)\in\mathcal{M}_n\times\mathcal{X}^n}$, where $\phi^{(n)}(x^n|m)$ is a conditional pmf. The decoder is denoted by $\psi^{(n)}$ such that $\psi^{(n)} : \mathcal{Y}^n \to \mathcal{M}_n$. The joint pmf on $\mathcal{M}_n \times \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ is given by

$$\begin{aligned} &p_{M_n X^n Y^n Z^n}(m, x^n, y^n, z^n) \\ &\quad = \frac{1}{|\mathcal{M}_n|} \phi^{(n)}(x^n|m) \prod_{t=1}^{n} W(y_t, z_t|x_t). \end{aligned} \tag{3}$$

The average probability of correct decoding is given by

$$\begin{aligned} \mathrm{P}_c^{(n)} &= \mathrm{P}_c^{(n)}(\phi^{(n)}, \psi^{(n)}) && (4)\\ &\triangleq \Pr\{\psi^{(n)}(Y^n) = M_n\}. && (5) \end{aligned}$$

The average probability of error is $\mathrm{P}_e^{(n)} = 1 - \mathrm{P}_c^{(n)}$. For fixed $\epsilon \in [0,1)$, a rate $R$ is *$\epsilon$-achievable* if there exists a sequence of codes $\{\phi^{(n)}, \psi^{(n)}\}_{n=1}^{\infty}$ such that

$$\begin{aligned} &\limsup_{n\to\infty} \mathrm{P}_e^{(n)} \le \epsilon, && (6)\\ &\liminf_{n\to\infty} \frac{1}{n} \log|\mathcal{M}_n| \ge R. && (7) \end{aligned}$$

In this work, we consider the partial strong converse property. Therefore, we require the code to satisfy (2). Let $\mathcal{C}_s(\epsilon|W)$ denote the maximal *$\epsilon$-achievable* rate satisfying (2) through the wiretap channel $W(y,z|x)$. From [2], we have

$$\mathcal{C}_s(0|W) = \max_{p\in\mathcal{P}(W)} I(U;Y) - I(U;Z), \tag{8}$$

where $\mathcal{P}(W)$ is defined as

$$\begin{aligned} \mathcal{P}(W) \triangleq \Big\{ &p_{UXYZ}(u,x,y,z) : |\mathcal{U}| \le |\mathcal{X}|, \\ &p_{YZ|X}(y,z|x) = W(y,z|x), \\ &U \to X \to (Y,Z) \Big\}. \end{aligned} \tag{9}$$

### B. Main Result

**Theorem 1.** *For a discrete memoryless non-degraded wiretap channel $W(y,z|x)$, the partial strong converse property holds, i.e., for $\epsilon \in [0,1)$, for any code $(\phi^{(n)}, \psi^{(n)})$ satisfying* (2),

$$\mathcal{C}_s(\epsilon|W) = \mathcal{C}_s(0|W). \tag{10}$$

The proof is provided in Section III. It is inspired by the new strong converse proof technique developed in [15]–[19]. We first use Verdu-Han bound and Chernoff-Cramer bound to upper bound the probability of correct decoding. Then, we focus on bounding the exponent function. We show that when the transmission rate is above $\mathcal{C}_s(0|W)$ and (2) is satisfied, the probability of correct decoding decays to zero exponentially fast, and the partial strong converse property holds.

## III. Proof of the Main Result

Consider a sequence of codes for which (2) is satisfied. Therefore, for each $\delta > 0$, there exists $n_0$ such that $\forall n > n_0$, we have

$$\frac{1}{n} I(M_n; Z^n) < \delta. \tag{11}$$

In the following, we consider $n > n_0$.

**Lemma 1.** *(Verdu-Han [8, Theorem 4]) For any $\eta > 0$ and for any $(\phi^{(n)}, \psi^{(n)})$ satisfying $\frac{1}{n}\log|\mathcal{M}_n| \ge R$, we have*

$$\begin{aligned} &\mathrm{P}_c^{(n)}(\phi^{(n)}, \psi^{(n)}) \le p_{M_n X^n Y^n Z^n} \Bigg\{ \\ &\qquad R \le \frac{1}{n} \log \frac{p_{Y^n|M_n}(Y^n|M_n)}{p_{Y^n}(Y^n)} + \eta \Bigg\} + e^{-n\eta}. \end{aligned} \tag{12}$$

**Lemma 2.** *(Chernoff-Cramer) For any real valued random variable $A$ and any $\theta > 0$, we have*

$$\Pr\{A \ge a\} \le \exp\{-[\theta a - \log \mathrm{E}[\exp(\theta A)]]\}. \tag{13}$$

By Lemmas 1 and 2, we have the following lemma.

**Lemma 3.** *For any $\theta > 0$, and for any $(\phi^{(n)}, \psi^{(n)})$ satisfying $\frac{1}{n}\log|\mathcal{M}_n| \ge R$, we have*

$$\begin{aligned} &\mathrm{P}_c^{(n)}(\phi^{(n)}, \psi^{(n)}) \\ &\quad \le \exp\Big\{ n\big[\theta\eta - \theta R + \frac{1}{n}\Omega_{p^{(n)}}^{(\theta)}(X^n Y^n Z^n|M_n)\big]\Big\} \\ &\qquad + e^{-n\eta} \end{aligned} \tag{14}$$

*where $\Omega_{p^{(n)}}^{(\theta)}(X^n Y^n Z^n|M_n)$ is defined as*

$$\begin{aligned} &\Omega_{p^{(n)}}^{(\theta)}(X^n Y^n Z^n|M_n) \\ &\qquad \triangleq \log \mathrm{E}_{p^{(n)}}\left[ \left\{ \frac{p_{Y^n|M_n}(Y^n|M_n)}{p_{Y^n}(Y^n)} \right\}^{\theta} \right] \end{aligned} \tag{15}$$

*where* $p^{(n)} = p_{M_nX^nY^nZ^n}$ *is defined in* (3).

**Proof:** We define the random variable $B$ as

$$B \triangleq \frac{1}{n}\log\frac{p_{Y^n|M_n}(Y^n|M_n)}{p_{Y^n}(Y^n)} - R. \tag{16}$$

Then, by (12) in Lemma 1, we have

$$\begin{aligned}&\mathrm{P}_c^{(n)}(\phi^{(n)},\psi^{(n)})\\ &\quad\le p_{M_nX^nY^nZ^n}\{B \ge -\eta\} + e^{-n\eta} &(17)\\ &\quad= p_{M_nX^nY^nZ^n}\{nB \ge -n\eta\} + e^{-n\eta} &(18)\end{aligned}$$

By identifying $A = nB$, $a = -n\eta$ and applying (13) in Lemma 2, we have

$$\begin{aligned}&\mathrm{P}_c^{(n)}(\phi^{(n)},\psi^{(n)})\\ &\quad\le \exp\{-[\theta(-n\eta) - \log \mathrm{E}_{p^{(n)}}[\exp(n\theta B)]]\} + e^{-n\eta} &(19)\\ &\quad= \exp\left\{n\big[\theta\eta - \theta R + \frac{1}{n}\Omega^{(\theta)}_{p^{(n)}}(X^nY^nZ^n|M_n)\big]\right\}\\ &\qquad + e^{-n\eta}. &(20)\end{aligned}$$

■

Let $\mathcal{P}^{(n)}(W)$ be a set of all pmfs $p_{M_nX^nY^nZ^n}$ on $\mathcal{M}_n \times \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ defined in (3). Moreover, define the subset of all pmfs in $\mathcal{P}^{(n)}(W)$ that satisfy the secrecy constraint in (11) as,

$$\mathcal{P}_\delta^{(n)}(W) = \left\{p_{M_nX^nY^nZ^n}: \quad p_{M_nX^nY^nZ^n} \in \mathcal{P}^{(n)}(W),\right.$$
$$\left.\frac{1}{n}I(M_n;Z^n) < \delta\right\}. \tag{21}$$

In order to bound the exponent function in (14), we define the communication potential $\overline{\Omega}^{(\theta)}_n(W)$ as follows:

$$\overline{\Omega}^{(\theta)}_n(W) \triangleq \max_{p^{(n)}\in\mathcal{P}^{(n)}_\delta(W)} \frac{1}{n}\Omega^{(\theta)}_{p^{(n)}}(X^nY^nZ^n|M_n). \tag{22}$$

We note that we do not construct the auxiliary distributions for single-letterization. Therefore, the definition of communication potential is different from the definitions given in [15]–[19]. References [15]–[19] apply a new technique called recursive bounding method for the single-letterized exponent. Here, we keep the multi-letterized form, and connect it to the proof of the weak converse.

From (14) in Lemma 3, we have

$$\begin{aligned}\mathrm{P}_c^{(n)}(\phi^{(n)},\psi^{(n)}) &\le \exp\left\{n\big[\theta\eta - \theta R + \overline{\Omega}^{(\theta)}_n(W)\big]\right\}\\ &\quad + e^{-n\eta}. \end{aligned}\tag{23}$$

We remark that there are two main factors affecting the exponent function in (23): the code rate $R$ and the communication potential $\overline{\Omega}^{(\theta)}_n(W)$.

To further study (23), we show that $\Omega^{(\theta)}_{p^{(n)}}(X^nY^nZ^n|M_n)$ has the properties listed in Lemma 4 below. Lemma 4 connects communication potential to the mutual information expression. We note that the properties listed in Lemma 4 are first obtained in [15]–[19].

**Lemma 4.**

1) $\Omega^{(\theta)}_{p^{(n)}}(X^nY^nZ^n|M_n)$ *is a convex function of* $\theta > 0$, *where* $\Omega^{(\theta)}_{p^{(n)}}(X^nY^nZ^n|M_n)$ *is defined in* (15).
2)
$$\lim_{\theta\to 0^+}\frac{\frac{1}{n}\Omega^{(\theta)}_{p^{(n)}}(X^nY^nZ^n|M_n)}{\theta} = \frac{1}{n}I(M_n;Y^n) \tag{24}$$
3) *For each* $\Delta > 0$, *there exists* $\theta > 0$ *such that*
$$\overline{\Omega}^{(\theta)}_n(W) \le \theta\left[\max_{p^{(n)}\in\mathcal{P}^{(n)}_\delta}\frac{1}{n}I(M_n;Y^n) + \frac{\Delta}{2}\right], \tag{25}$$
*where* $\overline{\Omega}^{(\theta)}_n(W)$ *is given in* (22).

**Proof:** To simplify the notation, define

$$\begin{aligned}\underline{a} &\triangleq (m, y^n), &(26)\\ \underline{A} &\triangleq (M_n, Y^n), &(27)\\ \underline{\mathcal{A}} &\triangleq \mathcal{M}_n \times \mathcal{Y}^n, &(28)\\ \rho(\underline{a}) &\triangleq \log\frac{p_{Y^n|M_n}(y^n|m)}{p_{Y^n}(y^n)}, &(29)\\ \xi(\theta) &\triangleq \Omega^{(\theta)}_{p^{(n)}}(X^nY^nZ^n|M_n). &(30)\end{aligned}$$

From (15), we have

$$\xi(\theta) = \Omega^{(\theta)}_{p^{(n)}}(X^nY^nZ^n|M_n) = \log\left[\sum_{\underline{a}\in\underline{\mathcal{A}}} p^{(n)}_{\underline{A}}(\underline{a})e^{\theta\rho(\underline{a})}\right]. \tag{31}$$

We evaluate the second derivative to show the convexity of $\theta$

$$\xi'(\theta) = e^{-\xi(\theta)}\left[\sum_{\underline{a}\in\underline{\mathcal{A}}} p^{(n)}_{\underline{A}}(\underline{a})\rho(\underline{a})e^{\theta\rho(\underline{a})}\right], \tag{32}$$

$$\begin{aligned}\xi''(\theta) &= e^{-2\xi(\theta)}\\ &\quad\times\left[\sum_{\underline{a},\underline{b}\in\underline{\mathcal{A}}} p^{(n)}_{\underline{A}}(\underline{a})p^{(n)}_{\underline{A}}(\underline{b})\frac{\{\rho(\underline{a})-\rho(\underline{b})\}^2}{2}e^{\theta\{\rho(\underline{a})+\rho(\underline{b})\}}\right].\end{aligned}\tag{33}$$

From (33), since $\xi''(\theta) \ge 0$, $\Omega^{(\theta)}_{p^{(n)}}(X^nY^nZ^n|M_n)$ is a convex function of $\theta > 0$. Hence, part 1) holds.

For part 2), consider $\theta = 0$ in (32), and $\xi(0) = 0$. We have

$$\xi'(0) = I(M_n;Y^n). \tag{34}$$

For part 3), given $\Delta > 0$, define the following function:

$$\zeta(\theta) \triangleq \overline{\Omega}^{(\theta)}_n(W) - \theta\left[\max_{p^{(n)}\in\mathcal{P}^{(n)}_\delta(W)}\frac{1}{n}I(M_n;Y^n) + \frac{\Delta}{2}\right]. \tag{35}$$

The function $\zeta(\theta)$ has the following properties:

$$\zeta(0) = 0, \tag{36}$$

$$\zeta'(0) = -\frac{\Delta}{2} < 0, \tag{37}$$

$$\zeta''(\theta) = \frac{1}{n}\xi''(\theta) \geq 0. \tag{38}$$

By the definition given in (22) and (24), (37) holds. (38) follows (33). For each $\Delta > 0$, there exists $f(\Delta) > 0$ such that for $\theta \in (0, f(\Delta)]$, we have $\zeta(\theta) \leq 0$. Finally, (25) holds. ■

Now, consider a code with rate

$$R = \mathcal{C}_s(0|W) + 4\delta. \tag{39}$$

We can further bound $\overline{\Omega}_n^{(\theta)}(W)$ in (25) as in the following lemma.

**Lemma 5.** *For each $\delta > 0$, there exists $\theta > 0$ such that*

$$\overline{\Omega}_n^{(\theta)}(W) \leq \theta \left[\mathcal{C}_s(0|W) + 3\delta\right], \tag{40}$$

*where $\overline{\Omega}_n^{(\theta)}(W)$ is given in (22).*

**Proof:** Take $\Delta = 4\delta$. For the fixed $\Delta > 0$, from (25) in Lemma 4, there exits a $\theta > 0$ such that

$$\overline{\Omega}_n^{(\theta)}(W) \leq \theta \left[\max_{p^{(n)}\in\mathcal{P}_\delta^{(n)}} \frac{1}{n} I(M_n; Y^n) + 2\delta\right] \tag{41}$$

$$\leq \theta \left[\max_{p^{(n)}\in\mathcal{P}^{(n)}} \frac{1}{n} I(M_n; Y^n) + \left(\delta - \frac{1}{n} I(M_n; Z^n)\right) + 2\delta\right] \tag{42}$$

$$\leq \theta \left[\mathcal{C}_s(0|W) + 3\delta\right], \tag{43}$$

where (42) holds due to the definition in (21), and (43) holds due to [2] [24, Section 22.1.2]. ■

We are now ready to prove Theorem 1. We consider a sequence of codes for which (2) is satisfied. Therefore, given $\delta > 0$, there exists $n_0$ such that $\forall n > n_0$, we have (11).

Now, assume that the code rate, $R$, equals to $\mathcal{C}_s(0|W) + 4\delta$. From Lemma 3, we upper bound the probability of correct decoding as (14). We further upper bound (14) as (23). Now, taking $\Delta = 4\delta$, from 3) in Lemma 4, there exists $\theta > 0$ such that (25) holds, which can be further upper bounded by (40) in Lemma 5. Therefore, (23) becomes

$$\mathrm{P}_c^{(n)}(\phi^{(n)}, \psi^{(n)}) \leq \exp\Big\{n\big[\theta\eta - \theta R + \theta\left[\mathcal{C}_s(0|W) + 3\delta\right]\big]\Big\} + e^{-n\eta} \tag{44}$$

$$= \exp\Big\{n\theta\big[\eta - \delta\big]\Big\} + e^{-n\eta}. \tag{45}$$

Finally, by picking $\eta = \frac{\delta}{2}$, we have

$$\mathrm{P}_c^{(n)}(\phi^{(n)}, \psi^{(n)}) \leq e^{-n\theta\frac{\delta}{2}} + e^{-n\frac{\delta}{2}}. \tag{46}$$

Thus, the probability of correct decoding decays to zero exponentially fast. For each $\delta > 0$ and $R \geq \mathcal{C}_s(0|W) + 4\delta$, we have shown $\limsup_{n\to\infty} \mathrm{P}_e^{(n)} = 1$. Therefore, for fixed $\epsilon \in [0, 1)$, if (2) and (6) are satisfied, then $R < \mathcal{C}_s(0|W) + 4\delta$. Hence, we have $\mathcal{C}_s(\epsilon|W) = \mathcal{C}_s(0|W)$, completing the proof of Theorem 1.

## IV. Conclusions and remarks

In this work, we proved the partial strong converse property for the discrete memoryless non-degraded wiretap channel, for which we require the leakage to the eavesdropper to vanish. Our work is based on the information spectrum method and Chernoff-Cramer bound for upper bounding the probability of correct decoding. We focus on bounding the exponent function of the probability of correct decoding. There are two main factors affecting the exponent function: the transmission rate and the communication potential. When the transmission rate is higher than the secrecy capacity, we show that the exponent is strictly negative. Therefore, the probability of correct decoding decays to zero exponentially fast, which implies that the partial strong converse property holds.

We remark that the proof of Theorem 1 can also be adapted to the proof of the strong converse for the point-to-point discrete memoryless channel. First, we define $\mathcal{C}(0|W)$ as the channel capacity for the point-to-point channel. For this channel, $p^{(n)} = p_{M_n X^n Y^n}$ in Lemma 3. Since there is no security constraint, the communication potential for the point-to-point channel becomes

$$\overline{\Omega}_n^{(\theta)}(W) \triangleq \max_{p^{(n)}\in\mathcal{P}^{(n)}(W)} \frac{1}{n} \Omega_{p^{(n)}}^{(\theta)}(X^n Y^n | M_n). \tag{47}$$

Moreover, (25) in Lemma 4 becomes

$$\overline{\Omega}_n^{(\theta)}(W) \leq \theta \left[\max_{p^{(n)}\in\mathcal{P}^{(n)}} \frac{1}{n} I(M_n; Y^n) + \frac{\Delta}{2}\right]. \tag{48}$$

Therefore, given $\Delta > 0$, for a code with $R \geq \mathcal{C}(0|W) + \Delta$, we have $\limsup_{n\to\infty} \mathrm{P}_e^{(n)} = 1$.

We also remark that the proof of Theorem 1 can also be adapted to the proof of the strong converse for the discrete memoryless multiple access channel, discrete memoryless interference channel and discrete memoryless broadcast channel. Although we do not know the single-letterized capacity region expressions for interference and broadcast channels, we have the multi-letterized capacity region expressions [22], [23]. With the multi-letterized capacity region expressions [21]–[23], we can show that these channels satisfy the strong converse property. For the multiple access channel, the strong converse property has been reported in [25], [26]. Our method can be viewed as an alternative proof without resorting to the wringing technique. For broadcast channels, the strong converse properties reported so far are for those with known single-letterized capacity regions, such as the degraded broadcast channel [15], [27] and the broadcast channel with degraded message sets [17], [28].

## References

[1] A. D. Wyner. The wire-tap channel. *Bell System Tech. J.*, 54(8):1355–1387, Oct. 1975.

[2] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[3] M. R. Bloch and J. N. Laneman. Strong secrecy from channel resolvability. *IEEE Trans. Inf. Theory*, 59(12):8077–8098, Dec. 2013.

[4] J. Wolfowitz. The coding of messages subject to chance errors. *Illinois Journal of Mathematics*, 1(4):591–606, 1957.

[5] M. Hayashi. Information spectrum approach to second-order coding rate in channel coding. *IEEE Trans. Inf. Theory*, 55(11):4947–4966, Nov. 2009.

[6] Y. Polyanskiy, H. V. Poor, and S. Verdu. Channel coding rate in the finite blocklength regime. *IEEE Trans. Inf. Theory*, 56(5):2307–2359, May 2010.

[7] V. Y. F. Tan. Asymptotic estimates in information theory with non-vanishing error probabilities. *Foundations and Trends in Communications and Information Theory*, 11(1-2):1–184, Sep. 2014.

[8] S. Verdu and T. S. Han. A general formula for channel capacity. *IEEE Trans. Inf. Theory*, 40(4):1147–1157, Jul. 1994.

[9] T. S. Han. *Information-Spectrum Methods in Information Theory*. Springer-Verlag, Feb. 2003.

[10] V. Y. F. Tan and M. R. Bloch. Information spectrum approach to strong converse theorems for degraded wiretap channels. *IEEE Trans. Inf. Forensics and Security*, 10(9):1891–1904, Sep. 2015.

[11] M. Hayashi, H. Tyagi, and S. Watanabe. Strong converse for a degraded wiretap channel via active hypothesis testing. In *Allerton Conf.*, Sep. 2014.

[12] H. Tyagi and S. Watanabe. Converses for secret key agreement and secure computing. *IEEE Trans. Inf. Theory*, 61(9):4809–4827, Sep. 2015.

[13] A. Winter. “Pretty strong” converse for the private capacity of degraded quantum wiretap channels. *https://arxiv.org/abs/1601.06611*, Apr. 2016.

[14] E. Graves and T. F. Wong. Equal-image-size source partitioning: Creating strong Fano’s inequalities for multi-terminal discrete memoryless channels. *https://arxiv.org/abs/1512.00824*, Jan. 2016.

[15] Y. Oohama. Strong converse exponent for degraded broadcast channels at rates outside the capacity region. In *IEEE ISIT*, Jun. 2015.

[16] Y. Oohama. Strong converse theorems for degraded broadcast channels with feedback. In *IEEE ISIT*, Jun. 2015.

[17] Y. Oohama. New strong converse for asymmetric broadcast channels. *http://arxiv.org/abs/1604.02901v3*, Apr. 2016.

[18] Y. Oohama. Strong converse exponent for state dependent channels with full state information at the sender and partial state information at the receiver. *https://arxiv.org/abs/1603.06344*, Mar. 2016.

[19] Y. Oohama. Exponent function for source coding with side information at the decoder at rates below the rate distortion function. *http://arxiv.org/abs/1601.05650*, Jan. 2016.

[20] R. L. Dobrushin. General formulation of Shannon’s main theorem in information theory. *Amer. Math. Soc. Trans*, 33:323–438, 1963.

[21] E. C. van der Meulen. The discrete memoryless channel with two senders and one receiver. In *IEEE ISIT*, Sep. 1971.

[22] R. Ahlswede. Multi-way communication channels. In *IEEE ISIT*, Sep. 1971.

[23] E. C. van der Meulen. Random coding theorems for the general discrete memoryless broadcast channel. *IEEE Trans. Inf. Theory*, 21(2):180–190, Mar. 1975.

[24] A. El Gamal and Y-H. Kim. *Network Information Theory*. Cambridge University Press, 2011.

[25] G. Dueck. The strong converse to the coding theorem for the multiple–access channel. *J. Comb. Inform. Syst. Sci*, 6(3):187–196, 1981.

[26] R. Ahlswede. An elementary proof of the strong converse theorem for the multiple-access channel. *J. Comb. Inform. Syst. Sci*, 7(3):216–230, 1982.

[27] R. Ahlswede, P. Gacs, and J. Korner. Bounds on conditional probabilities with applications in multi-user communication. *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, 34(2):157–177, 1976.

[28] J. Korner and K. Marton. General broadcast channels with degraded message sets. *IEEE Trans. Inf. Theory*, 23:60–64, Jan. 1977.