On an Upper Bound of the Secrecy Capacity for a General Wiretap Channel

Hiroki Koga
Graduate School of Systems and Information Engineering
University of Tsukuba
1-1-1 Tennoudai, Tsukuba, Ibaraki 305-8573, Japan
Email: koga@esys.tsukuba.ac.jp

Naoki Sato
Master's Program of Science and Engineering
University of Tsukuba
1-1-1 Tennoudai, Tsukuba, Ibaraki 305-8573, Japan
Email: sato@it.esys.tsukuba.ac.jp

Abstract— **This paper is concerned with coding theorems for a generalized wiretap channel. In the problem of the wiretap channel it is important to characterize the secrecy capacity, i.e., the maximum achievable rate of information securely transmitted from a sender to a legitimate receiver in the presence of a wiretapper. In our model channels are not restricted to memoryless channels. We first define the secrecy capacity C_s and evaluate C_s from information-spectrum approach. We give a new upper bound of C_s not including auxiliary random variables and explore conditions under which the obtained upper bound becomes tight for the cascaded wiretap channel.**

I. Introduction

The problem of the wiretap channel proposed by Wyner [8] is one of basic problems that treats coding for insecure channels. As is given in Fig. 1, in the problem of the wiretap channel we consider two cascaded channels (channel 1 and channel 2). In the problem it is crucial to characterize rate of information that is securely transmitted from a sender to a legitimate receiver through the channel 1 in the presence of a wiretapper who observes an output from the channel 2. The maximum of such a rate is called the *secrecy capacity* C_s. Wyner [8] gives the formula of C_s when both the channels 1 and 2 are stationary memoryless channels with finite input and output alphabets. Csiszár and Körner [1] consider a more general model of the wiretap channel where the two channels are not cascaded (Fig. 2). Csiszár and Körner give the formula of the secrecy capacity C_s under the same assumption of the channels as in [8] as a byproduct of their results.

On the other hand, the information-spectrum approach, which originates from Han and Verdu [2] and is described in detail in Han's book [3], gives a new method that enables us to treat channels without memoryless assumption and finiteness of input and output alphabets. In the information-spectrum approach we first formulate a problem to be considered in a general manner and consider a coding theorem that is valid under such a general setting. Once a coding theorem is established, we can obtain specific results by restricting the general setting to certain cases. It is often that we can obtain stronger versions of known results via such a generalization and reduction argument. Of course, coding theorems in the general settings are also of interest.

The objective of this paper is characterizing the secrecy capacity C_s of a general wiretap channel from the information-spectrum approach. We consider the model given in Fig. 2. The channels 1 and 2 can be any discrete channels, i.e., the channels 1 and 2 are not restricted to memoryless channels with finite input and output alphabets. Quite recently, Hayashi [4], [5] succeeded in obtaining a formula C_s by using his result on the channel resolvability problem. Hayashi's result is of interest not only as a generalization of the result by Csiszár and Körner but also as a result connecting the problem of the wiretap channel with the problem of the channel resolvability first introduced in [2].

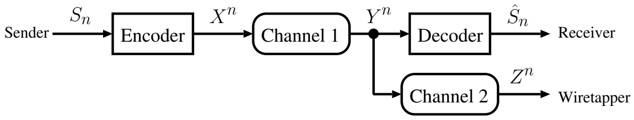

Fig. 1 Block diagram of Wyner's wiretap channel.

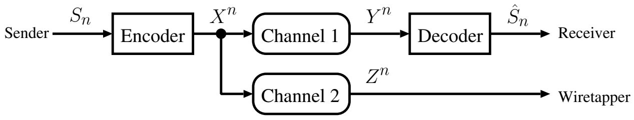

Fig. 2 Block diagram of the Csiszár-Körner wiretap channel.

In this paper we give a new upper bound of the secrecy capacity C_s not including auxiliary random variables for the model given in Fig. 2. In the argument yielding the upper bound, a Markov chain involved in the general wiretap channel plays an important role. In addition, we compare the upper bound with the lower bound of C_s given in [5] and explore conditions under which the two bounds coincide for the model in Fig. 1. As a byproduct, we give a sharpened version of Wyner's result for stationary memoryless channels.

This paper is organized as follows. In Section 2 we formulate the problem to be considered. Quantities used in the information-spectrum approach are defined. In Section 3 we give an upper bound of the secrecy capacity C_s. The upper bound is established by using several lemmas. Section 4 is devoted to investigation of conditions under which the upper bound of C_s becomes tight for the model in Fig. 1.

II. Problem Formulation

We consider the model of the wiretap channel given in Fig. 2. The model in Fig. 2 is defined for each $n \geq 1$ and has two channels. Denote by $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$ input alphabets of the channels 1 and 2, an output alphabet of the channel 1, and an output alphabet of the channel 2, respectively. We assume that $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$ are discrete sets. We consider the situation where both the channels 1 and 2 have n input symbols and n output symbols. Let $X^n \in \mathcal{X}^n$, $Y^n \in \mathcal{Y}^n$ and $Z^n \in \mathcal{Z}^n$ denote n inputs to the channels 1 and 2, n outputs from the channel 1 and n outputs from the channel 2, respectively. The probability distributions of X^n, Y^n and Z^n are denoted by P_{X^n}, P_{Y^n} and P_{Z^n}, respectively.

For each $n \geq 1$ the channel 1 is defined as a conditional probability distribution of Y^n given X^n, say $P_{Y^n|X^n}$. We use the notation $W_1^n(Y^n|X^n) = P_{Y^n|X^n}(Y^n|X^n)$ for the channel 1. Similarly, the channel 2 is defined as a conditional probability distribution $W_2^n(Z^n|X^n) = P_{Z^n|X^n}(Z^n|X^n)$. We regard the channels 1 and 2 as sequences of conditional probability distributions $\boldsymbol{W}_1 \overset{\text{def}}{=} \{W_1^n(Y^n|X^n)\}_{n=1}^{\infty}$ and $\boldsymbol{W}_2 \overset{\text{def}}{=} \{W_2^n(Z^n|X^n)\}_{n=1}^{\infty}$, respectively.

In this paper we impose no condition on $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ except for that for each $n \geq 1$ $W_1^n(Y^n|X^n)$ and $W_2^n(Z^n|Y^n)$ are conditional probability distributions from $\mathcal{X}^n \to \mathcal{Y}^n$ and $\mathcal{X}^n \to \mathcal{Z}^n$, respectively. Thus, $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ can be any discrete channels. Hereafter, we call $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ general channels. In particular, if for two conditional probability distributions $W_1 : \mathcal{X} \to \mathcal{Y}$ and $W_2 : \mathcal{X} \to \mathcal{Z}$ it holds that $W_1^n(Y^n|X^n) = \prod_{i=1}^n W_1(Y_i|X_i)$ and $W_2^n(Z^n|X^n) = \prod_{i=1}^n W_2(Z_i|X_i)$ for all $n \geq 1$, we call $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ stationary memoryless channels, where $X^n = X_1 X_2 \cdots X_n$, $Y^n = Y_1 Y_2 \cdots Y_n$ and $Z^n = Z_1 Z_2 \cdots Z_n$.

For each $n \geq 1$ we consider a situation where a sender wants to send a message $S_n \in \mathcal{S}_n$ to a legitimate receiver through the channel 1, where S_n is the random variable uniformly distributed on a set of messages $\mathcal{S}_n = \{1, 2, \ldots, M_n\}$. The sender encodes a message S_n to a codeword X^n by using an encoder φ_n and transmits $X^n \in \mathcal{X}^n$ to the legitimate receiver. The legitimate receiver receives n outputs Y^n from the channel 1 and decodes Y^n to $\hat{S}_n \in \mathcal{S}_n$ by using a decoder ψ_n. We also consider a wiretapper who observes Z^n, n outputs from the channel 2, and wants to know about the message S_n from Z^n. We assume that the encoder is stochastic. That is, the encoder generates a codeword X^n for a message S_n subject to a conditional probability distribution $P_{X^n|S_n}(X^n|S_n)$. On the other hand, the decoder ψ_n is assumed to be a deterministic mapping from $\mathcal{Y}^n$ to $\mathcal{S}_n$. Note that if M_n and a stochastic encoder φ_n are given, the joint probability distribution of S_n, X^n, Y^n and Z^n is determined. In addition, notice that S_n, X^n and $Y^n Z^n$ form a Markov chain in this order for all $n \geq 1$. Such a Markov chain is denoted by $S_n \to X^n \to Y^n Z^n$. Hereafter, we use notations $\boldsymbol{S} = \{S_n\}_{n=1}^{\infty}$, $\boldsymbol{X} = \{X^n\}_{n=1}^{\infty}$, $\boldsymbol{Y} = \{Y^n\}_{n=1}^{\infty}$ and $\boldsymbol{Z} = \{Z^n\}_{n=1}^{\infty}$.

The objective of this paper is characterizing the maximum achievable rate of information transmitted from the sender to the legitimate receiver under the condition that the wiretapper obtains almost no information on S_n from Z^n. Such the maximum rate is called a *secrecy capacity* [1], [8]. Before giving the formal definition of the secrecy capacity, we introduce notions that are usually used in the information-spectrum approach [3]. For a sequence $\boldsymbol{U} = \{U_n\}_{n=1}^{\infty}$ of real-valued random variables, the limsup in probability and the liminf in probability are defined by

$$\operatorname*{p\text{-}lim\,sup}_{n\to\infty} U_n = \inf\bigl\{\alpha : \lim_{n\to\infty} \Pr\{U_n \geq \alpha\} = 0\bigr\},$$

$$\operatorname*{p\text{-}lim\,inf}_{n\to\infty} U_n = \sup\bigl\{\beta : \lim_{n\to\infty} \Pr\{U_n \leq \beta\} = 0\bigr\},$$

respectively. Letting $\boldsymbol{V} = \{V_n\}_{n=1}^{\infty}$ be another sequence of real-valued random variables, the following formulas hold:

$$\operatorname*{p\text{-}lim\,inf}_{n\to\infty}(U_n + V_n) \geq \operatorname*{p\text{-}lim\,inf}_{n\to\infty} U_n + \operatorname*{p\text{-}lim\,inf}_{n\to\infty} V_n, \tag{1}$$

$$\operatorname*{p\text{-}lim\,inf}_{n\to\infty}(U_n + V_n) \leq \operatorname*{p\text{-}lim\,inf}_{n\to\infty} U_n + \operatorname*{p\text{-}lim\,sup}_{n\to\infty} V_n, \tag{2}$$

$$\operatorname*{p\text{-}lim\,inf}_{n\to\infty}(-U_n) = -\operatorname*{p\text{-}lim\,sup}_{n\to\infty} U_n \tag{3}$$

[3]. Throughout this paper, the following quantities play important roles:

$$\underline{I}(\boldsymbol{X};\boldsymbol{Y}) = \operatorname*{p\text{-}lim\,inf}_{n\to\infty} \frac{1}{n} \log_2 \frac{P_{Y^n|X^n}(Y^n|X^n)}{P_{Y^n}(Y^n)},$$

$$\overline{I}(\boldsymbol{X};\boldsymbol{Y}) = \operatorname*{p\text{-}lim\,sup}_{n\to\infty} \frac{1}{n} \log_2 \frac{P_{Y^n|X^n}(Y^n|X^n)}{P_{Y^n}(Y^n)},$$

$$\underline{I}(\boldsymbol{X};\boldsymbol{Y}|\boldsymbol{Z}) = \operatorname*{p\text{-}lim\,inf}_{n\to\infty} \frac{1}{n} \log_2 \frac{P_{Y^n|X^n Z^n}(Y^n|X^n, Z^n)}{P_{Y^n|Z^n}(Y^n|Z^n)},$$

where these quantities are defined with respect to the joint probability of the random variables included in the expressions. Note that we have $\underline{I}(\boldsymbol{X};\boldsymbol{Y}) = \underline{I}(\boldsymbol{Y};\boldsymbol{X})$ and $\underline{I}(\boldsymbol{X};\boldsymbol{Y}) \leq \overline{I}(\boldsymbol{X};\boldsymbol{Y})$ from their definitions. In addition, it is known that $\underline{I}(\boldsymbol{X};\boldsymbol{Y}) \geq 0$ and $\underline{I}(\boldsymbol{X};\boldsymbol{Y}|\boldsymbol{Z}) \geq 0$ [3]. Furthermore, if $X^n \to Y^n \to Z^n$ holds for all $n \geq 1$, we have $\underline{I}(\boldsymbol{X};\boldsymbol{Z}) \leq \underline{I}(\boldsymbol{X};\boldsymbol{Y})$ [7] similarly to the data processing inequality.

Now, we are ready to define the secrecy capacity of the wiretap channel.

Definition 1: Suppose that the channel 1 $\boldsymbol{W}_1 = \{W_1^n(Y^n|X^n)\}_{n=1}^{\infty}$ and the channel 2 $\boldsymbol{W}_2 = \{W_2^n(Z^n|X^n)\}_{n=1}^{\infty}$ are given. A rate R is called achievable if there exists a sequence $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$ of pairs of an encoder φ_n and a decoder ψ_n satisfying

$$\lim_{n\to\infty} \Pr\{S_n \neq \hat{S}_n\} = 0, \tag{4}$$

$$\lim_{n\to\infty} \frac{1}{n} \log_2 M_n = R, \tag{5}$$

$$\underline{H}(\boldsymbol{S}|\boldsymbol{Z}) \geq R, \tag{6}$$

where

$$\underline{H}(\boldsymbol{S}|\boldsymbol{Z}) = \operatorname*{p\text{-}lim\,inf}_{n\to\infty} \frac{1}{n} \log_2 \frac{1}{P_{S_n|Z^n}(S_n|Z^n)}.$$

The secrecy capacity is defined by

$$C_s(\boldsymbol{W}_1, \boldsymbol{W}_2) = \sup\{R : R \text{ is achievable}\}.$$

If both $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ are stationary memoryless channels specified by two conditional probability distributions $W_1 : \mathcal{X} \to \mathcal{Y}$ and $W_2 : \mathcal{X} \to \mathcal{Z}$, respectively, $C_s(\boldsymbol{W}_1, \boldsymbol{W}_2)$ is simply written as $C_s(W_1, W_2)$.

In Definition 1 (4), (5) and (6) are conditions on the decoding error probability at the legitimate receiver, the rate of transmitted information, and the secrecy of S^n given Z^n, respectively. Notice that in (5) we require the existence of the limit. The condition on the secrecy (6), which was first introduced in [6], is equivalent to $\overline{I}(\boldsymbol{S};\boldsymbol{Z}) = 0$ under (5). Since we have $0 \le \underline{I}(\boldsymbol{S};\boldsymbol{Z}) \le \overline{I}(\boldsymbol{S};\boldsymbol{Z})$, $\overline{I}(\boldsymbol{S};\boldsymbol{Z}) = 0$ implies that for any constant $\gamma > 0$ it holds that

$$\Pr\left\{\left|\frac{1}{n}\log_2 \frac{P_{S_n Z^n}(S_n, Z^n)}{P_{S_n}(S_n) P_{Z^n}(Z^n)}\right| \le \gamma\right\} \to 1 \text{ as } n \to \infty,$$

i.e., on a set with probability arbitrary close to one S_n is almost independent of Z^n if n is sufficiently large.

Csiszár and Körner [1] give the following result.

Theorem 1 (Csiszár and Körner [1]): Suppose that $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$ are finite alphabets and $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ are stationary memoryless channels determined by conditional probability distributions $W_1 : \mathcal{X} \to \mathcal{Y}$ and $W_2 : \mathcal{X} \to \mathcal{Z}$, respectively. Then, the secrecy capacity is given by

$$C_s(W_1, W_2) = \max_V [I(V;Y) - I(V;Z)], \tag{7}$$

where $X \in \mathcal{X}$, $Y \in \mathcal{Y}$ and $Z \in \mathcal{Z}$ are the random variables subject to the joint probability distribution $P_{XYZ}(X,Y,Z) = P_X(X)W_1(Y|X)W_2(Z|X)$, $I(V;Y)$ is the mutual information of V and Y. The maximum in (7) is taken with respect to all the random variables $V \in \mathcal{V}$ satisfying $V \to X \to YZ$ and $|\mathcal{V}| \le |\mathcal{X}|^2 + 4|\mathcal{X}| + 3$, where $|\cdot|$ denotes the cardinality.

Hayashi [5] generalizes Theorem 1 to the case where the channels 1 and 2 are general channels.

Theorem 2 (Hayashi [5]): Let $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ be general channels. Then, it holds that

$$C_s(\boldsymbol{W}_1, \boldsymbol{W}_2) = \sup_{\mathbf{V}} [\underline{I}(\boldsymbol{V};\boldsymbol{Y}) - \overline{I}(\boldsymbol{V};\boldsymbol{Z})], \tag{8}$$

where the supremum in (8) is taken with respect to $\boldsymbol{V} = \{V_n\}_{n=1}^{\infty}$ satisfying $V_n \to X^n \to Y^n Z^n$ for all $n \ge 1$. Here, V_n takes values in an arbitrary discrete set $\mathcal{V}_n$. In addition, it also holds that

$$C_s(\boldsymbol{W}_1, \boldsymbol{W}_2) \ge \sup_{\mathbf{X}} [\underline{I}(\boldsymbol{X};\boldsymbol{Y}) - \overline{I}(\boldsymbol{X};\boldsymbol{Z})]. \tag{9}$$

The main objective of this paper is characterization of $C_s(\boldsymbol{W}_1, \boldsymbol{W}_2)$ from a viewpoint different from [5]. In the next section we give a new upper bound of $C_s(\boldsymbol{W}_1, \boldsymbol{W}_2)$ not including a sequence of auxiliary random variables $\boldsymbol{V}$ and related to the conditional mutual information.

Remark: Strictly speaking, in Theorem 1 the criterion on secrecy in (6) is stronger than the condition given by Csiszár and Körner [1] that requires $\liminf_{n\to\infty} \frac{1}{n} H(S_n|Z^n) \ge R$. We can easily verify this fact because it holds that $\underline{H}(\boldsymbol{S}|\boldsymbol{Z}) \le \liminf_{n\to\infty} \frac{1}{n} H(S_n|Z^n)$ [3]. On the other hand, [5] requires $d_E^{(n)} \to 0$ as $n \to \infty$, where

$$d_E^{(n)} \overset{\text{def}}{=} \frac{1}{M_n(M_n - 1)} \sum_{s_n \ne s'_n} d(P_{Z^n|S_n}(\,\cdot\,|s_n),\, P_{Z^n|S_n}(\,\cdot\,|s'_n))$$

and $d(\,\cdot\,,\,\cdot\,)$ denotes the variational distance. We can prove that Hayashi's criterion is stronger than (6). ■

III. An Upper Bound of the Secrecy Capacity

We can obtain the following upper bound of $C_s(\boldsymbol{W}_1, \boldsymbol{W}_2)$.

Theorem 3: Let $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ be two general channels. Then, it holds that

$$C_s(\boldsymbol{W}_1, \boldsymbol{W}_2) \le \sup_{\mathbf{X}} \underline{I}(\boldsymbol{X};\boldsymbol{Y}|\boldsymbol{Z}), \tag{10}$$

where the supremum in (10) is taken with respect to all the inputs $\boldsymbol{X}$ to the channel 1.

We prove Theorem 3 by using the five lemmas below. The first lemma describes an easy consequence which follows from the assumption of the existence of the limit in (5).

Lemma 1: If the limit of $\frac{1}{n}\log_2 M_n$, $n \ge 1$, exists, then

$$\underline{H}(\boldsymbol{S}) = \overline{H}(\boldsymbol{S}) = \lim_{n\to\infty} \frac{1}{n}\log_2 M_n. \tag{11}$$

Proof: Since $S_n \in \mathcal{S}_n = \{1, 2, \ldots, M_n\}$ is assumed to be uniformly distributed, it is easy to see that $\underline{H}(\boldsymbol{S}) = \liminf_{n\to\infty} \frac{1}{n}\log_2 M_n$ and $\overline{H}(\boldsymbol{S}) = \limsup_{n\to\infty} \frac{1}{n}\log_2 M_n$. If $\frac{1}{n}\log_2 M_n$ converges to a limit, we have (11). ■

The following two lemmas characterize properties of $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$ satisfying (4)–(6).

Lemma 2: For an arbitrary constant $\gamma > 0$ define $E_n^{(1)}$ by

$$E_n^{(1)} = \Big\{(s_n, y^n, z^n) \in \mathcal{S}_n \times \mathcal{Y}^n \times \mathcal{Z}^n : \left|\frac{1}{n}\log_2 \frac{P_{S_n|Z^n}(s_n|z^n)}{P_{S_n}(s_n)}\right| \le \gamma\Big\}. \tag{12}$$

Then, for any $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$ satisfying (5) and (6) we have

$$\Pr\{(S_n, Y^n, Z^n) \in E_n^{(1)}\} \to 1 \quad \text{as } n \to \infty.$$

Proof: It suffices to prove that

$$\Pr\{(S_n, Z^n) \in \tilde{E}_n^{(1)}\} \to 1 \quad \text{as } n \to \infty, \tag{13}$$

where $\tilde{E}_n^{(1)}$ is defined by

$$\tilde{E}_n^{(1)} = \Big\{(s_n, z^n) \in \mathcal{S}_n \times \mathcal{Z}^n : \left|\frac{1}{n}\log_2 \frac{P_{S_n|Z^n}(s_n|z^n)}{P_{S_n}(s_n)}\right| \le \gamma\Big\}.$$

Since we have $\overline{H}(\boldsymbol{S}) = \lim_{n\to\infty} \frac{1}{n}\log_2 M_n$ from Lemma 1, (6) means that $\overline{H}(\boldsymbol{S}|\boldsymbol{Z}) \ge \overline{H}(\boldsymbol{S})$. This inequality, together with Theorem 8 (d) in [7], tells us that $\overline{I}(\boldsymbol{S};\boldsymbol{Z}) \le 0$. On the other hand, since we have $0 \le \underline{I}(\boldsymbol{S};\boldsymbol{Z}) \le \overline{I}(\boldsymbol{S};\boldsymbol{Z})$, $\overline{I}(\boldsymbol{S};\boldsymbol{Z}) = 0$ means that $\underline{I}(\boldsymbol{S};\boldsymbol{Z}) = \overline{I}(\boldsymbol{S};\boldsymbol{Z}) = 0$. This, together with the definitions of $\underline{I}(\boldsymbol{S};\boldsymbol{Z})$ and $\overline{I}(\boldsymbol{S};\boldsymbol{Z})$, implies (13). ■

Lemma 3: For an arbitrary constant $\gamma > 0$ define $E_n^{(2)}$ by

$$E_n^{(2)} = \Big\{(s_n, y^n, z^n) \in \mathcal{S}_n \times \mathcal{Y}^n \times \mathcal{Z}^n : \frac{1}{n}\log_2 P_{S_n|Y^nZ^n}(s_n|y^n, z^n) \ge -\gamma\Big\}. \tag{14}$$

Then, for any $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$ satisfying (4) it holds that

$$\Pr\{(S_n, Y^n, Z^n) \in E_n^{(2)}\} \to 1 \quad \text{as } n \to \infty. \tag{15}$$

Proof: Fix $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$ satisfying (4) arbitrarily. Consider a virtual decoder $\xi_n : \mathcal{Y}^n \times \mathcal{Z}^n \to \mathcal{S}_n$ that takes both Y^n and Z^n as the inputs and outputs $\hat{S}'_n \overset{\text{def}}{=} \xi_n(Y^n, Z^n)$. Note that for any constant $\gamma > 0$ the Verdú-Han lemma (Theorem 4 in [7]) and Bayes' theorem tell us that

$$\Pr\{P_{S_n|Y^nZ^n}(S_n|Y^n, Z^n) < 2^{-n\gamma}\} < \Pr\{S_n \neq \hat{S}'_n\} + 2^{-n\gamma} \tag{16}$$

for any ξ_n. Now, we define ξ_n as the mapping $(Y^n, Z^n) \mapsto \hat{S}_n = \varphi_n(Y^n)$. Then, it follows from (4) and (16) that

$$\Pr\{P_{S_n|Y^nZ^n}(S_n|Y^nZ^n) < 2^{-n\gamma}\} \to 0 \quad \text{as } n \to \infty,$$

which is equivalent to (15). ■

Lemmas 2 and 3 lead to the following key lemma.

Lemma 4: Let $\gamma > 0$ be an arbitrary constant. Then, for any $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$ satisfying (4)–(6) it holds that

$$\Pr\Big\{\frac{1}{n}\log_2 \frac{P_{Y^n|S_nZ^n}(Y^n|S_n, Z^n)}{P_{Y^n|Z^n}(Y^n|Z^n)} \ge \frac{1}{n}\log_2 M_n - 2\gamma\Big\} \to 1 \quad \text{as } n \to \infty. \tag{17}$$

Proof: Fix $\gamma > 0$ arbitrarily. We define $E_n^{(1)}$ and $E_n^{(2)}$ by (12) and (14), respectively. We also define $E_n^{(3)}$ by

$$E_n^{(3)} = \Big\{(s_n, y^n, z^n) \in \mathcal{S}_n \times \mathcal{Y}^n \times \mathcal{Z}^n : \frac{1}{n}\log_2 \frac{P_{Y^n|S_nZ^n}(y^n|s_n, z^n)}{P_{Y^n|Z^n}(y^n|z^n)} \ge \frac{1}{n}\log_2 M_n - 2\gamma\Big\}.$$

In order to establish the claim of this lemma, in view of Lemmas 2 and 3 it suffices to show that $E_n^{(3)} \supseteq E_n^{(1)} \cap E_n^{(2)}$. To this end, fix $(s_n, y^n, z^n) \in E_n^{(1)} \cap E_n^{(2)}$ arbitrarily. Then, it follows that

$$\begin{aligned}
&\frac{1}{n}\log_2 \frac{P_{Y^n|S_nZ^n}(y^n|s_n, z^n)}{P_{Y^n|Z^n}(y^n|z^n)} \\
&\overset{1)}{=} \frac{1}{n}\log_2 \frac{P_{S_n|Y^nZ^n}(s_n|y^n, z^n)}{P_{S_n|Z^n}(s_n|z^n)} \\
&= \frac{1}{n}\log_2 \frac{P_{S_n|Y^nZ^n}(s_n|y^n, z^n)}{P_{S_n}(s_n)} - \frac{1}{n}\log_2 \frac{P_{S_n|Z^n}(s_n|z^n)}{P_{S_n}(s_n)} \\
&\overset{2)}{\ge} \frac{1}{n}\log_2 \frac{P_{S_n|Y^nZ^n}(s_n|y^n, z^n)}{P_{S_n}(s_n)} - \gamma \\
&\overset{3)}{=} \frac{1}{n}\log_2 P_{S_n|Y^nZ^n}(s_n|y^n, z^n) + \frac{1}{n}\log_2 M_n - \gamma \\
&\overset{4)}{\ge} \frac{1}{n}\log_2 M_n - 2\gamma,
\end{aligned} \tag{18}$$

where the marked equalities and inequalities in (18) follow because

1): the conditional version of Bayes' theorem,
2): $(s_n, y^n, z^n) \in E_n^{(1)}$,
3): $P_{S_n}(s_n) = 1/M_n$ for all $s_n \in \mathcal{S}_n$,
4): $(s_n, y^n, z^n) \in E_n^{(2)}$.

Clearly, (18) guarantees that $(s_n, y^n, z^n) \in E_n^{(3)}$. ■

Finally, we give the following lemma that can be regarded as an extended version of the data processing inequality. This lemma is proved similarly to the proof of Theorem 9 in [7].

Lemma 5:

$$\underline{I}(\boldsymbol{S}; \boldsymbol{Y}|\boldsymbol{Z}) \le \underline{I}(\boldsymbol{X}; \boldsymbol{Y}|\boldsymbol{Z}). \tag{19}$$

Proof of Theorem 3: Suppose that a rate R is achievable. Then, there exists a sequence $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$ satisfying (4)–(6). Notice that we have for an arbitrary constant $\gamma > 0$

$$R \le \frac{1}{n}\log_2 M_n + \gamma \quad \text{for all sufficiently large } n \tag{20}$$

from (5). Since Lemma 4 and (20) lead to

$$\Pr\Big\{\frac{1}{n}\log_2 \frac{P_{Y^n|S_nZ^n}(Y^n|S_n, Z^n)}{P_{Y^n|Z^n}(Y^n|Z^n)} \ge R - 3\gamma\Big\} \to 1$$

as $n \to \infty$, we have $R \le \underline{I}(\boldsymbol{S}; \boldsymbol{Y}|\boldsymbol{Z}) \le \underline{I}(\boldsymbol{X}; \boldsymbol{Y}|\boldsymbol{Z})$, where the last inequality follows from Lemma 5. Thus, by taking the supremum with respect to $\boldsymbol{X}$, it holds that

$$R \le \sup_{\mathbf{X}} \underline{I}(\boldsymbol{X}; \boldsymbol{Y}|\boldsymbol{Z}). \tag{21}$$

Note that the right hand side of (21) no longer depends on $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$. Then, the claim of the theorem follows because R is an arbitrary achievable rate. ■

IV. Secrecy Capacity of the Cascaded Wiretap Channel

In this section we consider the cascaded wiretap channel given in Fig 1. In Fig. 1 let $X^n \in \mathcal{X}^n, Y^n \in \mathcal{Y}^n$ and $Z^n \in \mathcal{Z}^n$ be n inputs to the channel 1, n outputs from the channel 2 (also n inputs to the channel 2), and n outputs from the channel 2. Let $\boldsymbol{W}_1 = \{W_1^n(Y^n|X^n)\}_{n=1}^{\infty}$ and $\boldsymbol{W}_2 = \{W_2^n(Z^n|Y^n)\}_{n=1}^{\infty}$ be general channels corresponding to the channels 1 and 2, respectively. Other notations are the same as in the preceding sections.

The cascaded wiretap channel in Fig. 1 is a special case of the wiretap channel in Fig. 2 satisfying

$$P_{Y^nZ^n|X^n}(Y^n, Z^n|X^n) = W_1^n(Y^n|X^n)W_2^n(Z^n|Y^n)$$

for all $n \ge 1$, i.e., $X^n \to Y^n \to Z^n$ for all $n \ge 1$. Wyner [8] gives the following result on the cascaded wiretap channel.

Theorem 4 (Wyner [8]): Suppose that $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$ are finite alphabet and $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ are stationary memoryless channels determined by conditional probability distributions $W_1 : \mathcal{X} \to \mathcal{Y}$ and $W_2 : \mathcal{Y} \to \mathcal{Z}$, respectively. Then, the secrecy capacity is given by

$$\begin{aligned}
C_s(W_1, W_2) &= \max_X [I(X;Y) - I(X;Z)] \\
&= \max_X I(X;Y|Z),
\end{aligned} \tag{22}$$

where $X \in \mathcal{X}$, $Y \in \mathcal{Y}$ and $Z \in \mathcal{Z}$ are the random variables subject to the joint probability distribution $P_{XYZ}(X, Y, Z) =$

$P_X(X)W_1(Y|X)W_2(Z|Y)$ and $I(X;Y|Z)$ is the conditional mutual information of X and Y given Z.

Notice that $I(X;Y) - I(X;Z) = I(X;Y|Z)$ for any random variables X, Y and Z satisfying $X \to Y \to Z$. Thus, the second equality in (22) is an easy consequence of the Markov chain.

Hereafter, we evaluate the secrecy capacity $C_s(\boldsymbol{W}_1, \boldsymbol{W}_2)$ for general channels $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$. The combination of (9) in Theorem 2 and (10) in Theorem 3 leads to

$$\sup_{\mathbf{X}} [\underline{I}(\boldsymbol{X};\boldsymbol{Y}) - \overline{I}(\boldsymbol{X};\boldsymbol{Z})] \le C_s(\boldsymbol{W}_1, \boldsymbol{W}_2) \le \sup_{\mathbf{X}} \underline{I}(\boldsymbol{X};\boldsymbol{Y}|\boldsymbol{Z}). \tag{23}$$

However, the upper and the lower bounds in (23) are not tight in general. In fact, we can prove only

$$\underline{I}(\boldsymbol{X};\boldsymbol{Y}) - \overline{I}(\boldsymbol{X};\boldsymbol{Z}) \le \underline{I}(\boldsymbol{X};\boldsymbol{Y}|\boldsymbol{Z}) \le \underline{I}(\boldsymbol{X};\boldsymbol{Y}) - \underline{I}(\boldsymbol{X};\boldsymbol{Z}) \tag{24}$$

for any $\boldsymbol{X}$, where (24) follows from $X^n \to Y^n \to Z^n$ for all $n \ge 1$, (1), (3) and symmetries of $\overline{I}(\cdot\,;\cdot)$ and $\overline{I}(\cdot\,;\cdot\,|\boldsymbol{Z})$.

The following two corollaries explore conditions under which the lower and upper bounds of $C_s(\boldsymbol{W}_1, \boldsymbol{W}_2)$ in (23) coincide. If the two bounds coincide, we have the formula of $C_s(\boldsymbol{W}_1, \boldsymbol{W}_2)$ that is similar to Theorem 4.

Corollary 1: Assume that the supremums in (23) are simultaneously attained by some $\boldsymbol{X} = \boldsymbol{X}^*$ and such $\boldsymbol{X}^*$ satisfies $\underline{I}(\boldsymbol{X}^*;\boldsymbol{Z}^*) = \overline{I}(\boldsymbol{X}^*;\boldsymbol{Z}^*)$, where $\boldsymbol{Z}^*$ denotes the output form the channel 2 corresponding to $\boldsymbol{X}^*$. Then, $C_s(\boldsymbol{W}_1, \boldsymbol{W}_2)$ can be written as

$$C_s(\boldsymbol{W}_1, \boldsymbol{W}_2) = \sup_{\mathbf{X}} [\underline{I}(\boldsymbol{X};\boldsymbol{Y}) - \overline{I}(\boldsymbol{X};\boldsymbol{Z})] \tag{25}$$

$$= \sup_{\mathbf{X}} \underline{I}(\boldsymbol{X};\boldsymbol{Y}|\boldsymbol{Z}). \tag{26}$$

Corollary 2: If $C_s(\boldsymbol{W}_1, \boldsymbol{W}_2)$ can be written as (25) and (26) and the supremum in (25) is attained by some $\boldsymbol{X} = \boldsymbol{X}^*$, then the supremum in (26) is attained by the same $\boldsymbol{X}^*$. Furthermore, if $C_s(\boldsymbol{W}_1, \boldsymbol{W}_2)$ can also be written as

$$C(\boldsymbol{W}_1, \boldsymbol{W}_2) = \sup_{\mathbf{X}} [\underline{I}(\boldsymbol{X};\boldsymbol{Y}) - \underline{I}(\boldsymbol{X};\boldsymbol{Z})] \tag{27}$$

and the supremum of (25) is attained by some $\boldsymbol{X} = \boldsymbol{X}^*$, then the supremums in (26) and (27) are attained by the same $\boldsymbol{X}^*$. Such $\boldsymbol{X}^*$ satisfies $\underline{I}(\boldsymbol{X}^*;\boldsymbol{Z}^*) = \overline{I}(\boldsymbol{X}^*;\boldsymbol{Z}^*)$, where $\boldsymbol{Z}^*$ denotes the output from the channel 2 corresponding to $\boldsymbol{X}^*$.

Corollary 1 trivially follows from (23) and assumption in the corollary. We give the proof of Corollary 2 below.

Proof of Corollary 2: Suppose that the $C_s(\boldsymbol{W}_1, \boldsymbol{W}_2)$ is expressed in both (25) and (26). Then, it follows that

$$\sup_{\mathbf{X}} [\underline{I}(\boldsymbol{X};\boldsymbol{Y}) - \overline{I}(\boldsymbol{X};\boldsymbol{Z})] \ge \underline{I}(\boldsymbol{X};\boldsymbol{Y}|\boldsymbol{Z}) \text{ for any } \boldsymbol{X}. \tag{28}$$

Since $\boldsymbol{X}^*$ attains the supremum in (28), we have

$$\underline{I}(\boldsymbol{X}^*;\boldsymbol{Y}^*) - \overline{I}(\boldsymbol{X}^*;\boldsymbol{Z}^*) \ge \underline{I}(\boldsymbol{X};\boldsymbol{Y}|\boldsymbol{Z}) \text{ for any } \boldsymbol{X}, \tag{29}$$

where $\boldsymbol{Y}^*$ and $\boldsymbol{Z}^*$ are outputs from the channels 1 and 2 corresponding to $\boldsymbol{X}^*$, respectively. By setting $\boldsymbol{X} = \boldsymbol{X}^*$ in (29), we have

$$\underline{I}(\boldsymbol{X}^*;\boldsymbol{Y}^*) - \overline{I}(\boldsymbol{X}^*;\boldsymbol{Z}^*) \ge \underline{I}(\boldsymbol{X}^*;\boldsymbol{Y}^*|\boldsymbol{Z}^*). \tag{30}$$

On the other hand, (24) tells us that

$$\underline{I}(\boldsymbol{X}^*;\boldsymbol{Y}^*) - \overline{I}(\boldsymbol{X}^*;\boldsymbol{Z}^*) \le \underline{I}(\boldsymbol{X}^*;\boldsymbol{Y}^*|\boldsymbol{Z}^*). \tag{31}$$

Then, the first claim of this corollary follows from (30) and (31). Next, suppose that all of (25), (26) and (27) hold. Let $\boldsymbol{X}^*$ be an input of the channel 1 attaining the supremum in (25). Then, by repeating the same argument, we have $\underline{I}(\boldsymbol{X}^*;\boldsymbol{Y}^*) - \overline{I}(\boldsymbol{X}^*;\boldsymbol{Z}^*) = \underline{I}(\boldsymbol{X}^*;\boldsymbol{Y}^*|\boldsymbol{Z}^*) = \underline{I}(\boldsymbol{X}^*;\boldsymbol{Y}^*) - \underline{I}(\boldsymbol{X}^*;\boldsymbol{Z}^*)$. This means that $\underline{I}(\boldsymbol{X}^*;\boldsymbol{Z}^*) = \overline{I}(\boldsymbol{X}^*;\boldsymbol{Z}^*)$. ■

Now, suppose that both $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ are stationary memoryless channels defined by two conditional probability distributions $W_1 : \mathcal{X} \to \mathcal{Y}$ and $W_2 : \mathcal{Y} \to \mathcal{Z}$. Denote by X_0 the random variable on $\mathcal{X}$ that maximizes $I(X;Y|Z)$ in Theorem 4 and by P_{X_0} the probably distribution of X_0. Let $\boldsymbol{X}_0$ be the stationary memoryless process induced by P_{X_0}. Define $\boldsymbol{Y}_0$ and $\boldsymbol{Z}_0$ the outputs from the channels 1 and 2 corresponding to $\boldsymbol{X}_0$, respectively. Then, we can show that, if $I(X;Y) < \infty$, $\underline{I}(\boldsymbol{X};\boldsymbol{Y}|\boldsymbol{Z})$ is maximized by $\boldsymbol{X}_0$ and $\underline{I}(\boldsymbol{X}_0;\boldsymbol{Z}_0) = \overline{I}(\boldsymbol{X}_0;\boldsymbol{Z}_0)$ is satisfied. Thus, Corollary 1 tells us that $C_s(W_1, W_2) = \underline{I}(\boldsymbol{X}_0;\boldsymbol{Y}_0|\boldsymbol{Z}_0)$. Furthermore, we can show that $\underline{I}(\boldsymbol{X}_0;\boldsymbol{Y}_0|\boldsymbol{Z}_0) = I(X_0;Y_0|Z_0)$ by the weak law of large numbers, where $Y_0 \in \mathcal{Y}$ and $Z_0 \in \mathcal{Z}$ are the random variables subject to $P_{Y_0|X_0}(Y_0|X_0) = W_1(Y_0|X_0)$ and $P_{Z_0|Y_0}(Z_0|Y_0) = W_2(Z_0|Y_0)$. This argument leads to the following corollary:

Corollary 3: Suppose that $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ are stationary memoryless channels determined by two conditional probability distributions $W_1 : \mathcal{X} \to \mathcal{Y}$ and $W_2 : \mathcal{Y} \to \mathcal{Z}$, respectively. If $I(X;Y) < \infty$, then it holds that

$$C_s(W_1, W_2) = \max_X [I(X;Y) - I(X;Z)] = \max_X I(X;Y|Z).$$

Note that in Corollary 3 we use the condition (6) on secrecy and $\mathcal{Y}$ and $\mathcal{Z}$ can be countably infinite alphabets. Corollary 3 can be regarded as a sharpened version of Theorem 4.

Acknowledgment

The authors thank Professor Hirosuke Yamaoto in Graduate School of Frontier Science, University of Tokyo, who suggested a relationship between [4] and this study. The authors acknowledge Dr. Masahito Hayashi in ERATO who sent [5] to them.

References

[1] I. Csiszár and J. Körner, "Broadcast channels with condifential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 3, pp. 339–348, 1978.

[2] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. on Inform. Theory*, vol. IT-39, pp. 752–772, 1993.

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

[4] M. Hayashi, "Exponents of channel resolvability and wire-tapped channel," *Proc. of ISITA*, Parma, Italy, pp. 1080–1085, 2004.

[5] M. Hayashi, "General non-asymptotic and asymptotic formulas in channel resolvability and identification capacity and its application to wire-tap channel," preprint, 2005.

[6] H. Koga, "Coding theorems on Shannon's cipher system with a general source," *Proc. of 2000 IEEE ISIT*, Sorrento, Italy, p. 158, 2000.

[7] S. Verdú and T. S. Han, "A general formula for channel capacity," *IEEE Trans. Inform. Theory*, vol. IT-40, no. 4, pp. 1147–1157, 1994.

[8] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, pp. 1355–1387, 1975.