

# Secrecy Capacity of Semi-deterministic Wire-tap Channels

Jared Grubb\*, Sriram Vishwanath\*, Yingbin Liang<sup>†</sup>, and H. Vincent Poor<sup>†</sup>

\*Elec. and Comp. Eng., University of Texas at Austin

1 University Station C0803, Austin, TX 78712-0240

Email: {grubb, sriram}@ece.utexas.edu

<sup>†</sup>Dept. of Elec. Eng., Princeton University

Engineering Quadrangle, Olden Street, Princeton, NJ 08544

Email: {yingbinl, poor}@princeton.edu

**Abstract**—This paper studies secrecy capacity in a semi-deterministic setting, in which the channel between legitimate users (called Alice and Bob) is deterministic, while that between Alice and the eavesdropper (called Eve) is a discrete memoryless channel. Such a model is particularly relevant when a pre-existing error correcting code tailored to the legitimate channel is in use on top of which secret information is to be shared.

First, a point-to-point setting is considered with a single wire-tapper, a situation in which the secrecy capacity has an elegant characterization. Next, a generalized multiple access setting with confidential messages is considered in which each user wishes to communicate secret information to a common destination without the other determining its message. In this latter situation, outer bounds on the secrecy capacity are obtained.

1

## I. INTRODUCTION

Security is a complementary consideration to efficiency and capacity in modern communications networks. A vast body of existing information-theoretic literature characterizes the reliable-communication limits of networks. Given the increasing importance of securing these networks, it is important that a significant amount of energy be devoted to using information theoretic concepts to understand how networks can be made both secure and reliable simultaneously.

In 1975, Wyner introduced a model for a communication channel that has been compromised by an eavesdropper [1]. In this model, the channel considered is a degraded broadcast channel. The goal is to encode the message in a manner that provides *information theoretic secrecy* guarantees while communicating reliably between the legitimate source and destination. In our paper, we adopt the concept of *secrecy capacity* as outlined in Wyner’s paper, namely the rate at which the message can be successfully decoded by the receiver while ensuring that the eavesdropper is completely ignorant of the message.

This work was subsequently generalized by Csiszár and Körner in [2]. In this model, a broadcast channel connects the legitimate receiver and wire-tapper to the sender. The sender desires to transmit a common message to both the intended receiver and the wire-tapper while simultaneously

transmitting a confidential message decodable only by the legitimate receiver. There has been significant further work on this topic in [3], [4], [5], including the study of the relay channel with confidential messages [6], and the generalized multiple-access channel (GMAC) with confidential messages [7].

One of the primary criticisms faced by information theoretic analysis of secrecy is the view that it results in extremely stringent constraints on the system, and that computational secrecy models are more appropriate and, perhaps, more valuable from a practical perspective. In this work, our goal is to contend that the main issue that causes information theoretic secrecy to produce pessimistic results (such as zero secrecy capacity) is the model being considered, not the tools or the notion of secrecy being employed.

In order to do this, we take the following steps in the paper:

- 1) We consider a semi-deterministic channel model for the wire-tap channel. In this model, the channel between the legitimate users is deterministic, while that between the legitimate transmitter (Alice) and the eavesdropper (Eve) is a noisy channel. The reasons why such a model is useful to study are:
  - a) Most communication networks already employ error-correction *tailored* to the legitimate channel, thus allowing for a deterministic model to fit the setting.
  - b) Semi-deterministic multi-user channels generally lend themselves better to intuition and analysis than the more general class of discrete memoryless channels; for example, see [8].
  - c) Finally, as we show in this paper, this model leads to results less pessimistic than before for secrecy capacity. We find that, *unless what the legitimate receiver (Bob) receives is a deterministic function of what Eve receives, there is a non-zero secrecy capacity*. This is the crux of the paper - when the channel between Alice and Bob is deterministic, there is a non-zero secrecy capacity unless Bob’s received signal is deterministically “worse” at each time instant than Eve’s.

<sup>1</sup>This research was supported in part by the U. S. National Science Foundation under Grants ANI-03-38807 and CNS-06-25637.

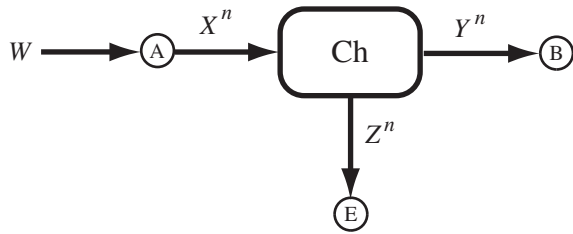


Fig. 1. Wire-tap Channel Model

In general, in many settings in prior work, secrecy capacity was found to be zero when Eve’s channel is stochastically “better” than that of Bob. In the deterministic channel case, secrecy capacity is zero only when Eve’s channel is deterministically “better” than Bob’s.

- 2) We also find an outer bound on secrecy capacity in a generalized multiple access channel with confidential messages. This outer bound is a generalization of the techniques used in deriving an outer bound in the (point-to-point) wire-tap channel case.

#### A. Organization

The next section discusses the model and the main results for the semi-deterministic wire-tap channel. Section III details the model and derives an outer bound on the rate region for a generalized multiple access channel with confidential messages. We conclude with a discussion in IV.

#### B. Conventions

Capital letters ( $X, Y$ ) are used to denote random variables. Subscripts ( $X_1, X_2$ ) are used to identify random variables associated to certain nodes in a network. A vector of  $n$  random variables is written as either  $X^n = (X_1, X_2, X_3, \dots, X_n)$  or  $X_1^n = (X_{1,1}, X_{1,2}, X_{1,3}, \dots, X_{1,n})$ , depending on context. A Markov chain of random variables is written in the form  $X \rightarrow Y \rightarrow Z$ .

## II. SEMI-DETERMINISTIC WIRE-TAP CHANNEL: MAIN RESULTS

#### A. Model

We adopt the Wyner wire-tap model as shown in Figure 1. Alice (“A”) has access to a secret message  $W$  and sends  $X^n$  across the channel. The channel is memoryless and has two outputs defined by distribution  $P(y, z|x)$ . Alice desires to reliably transmit the message  $W$  to Bob (“B”) while simultaneously revealing minimal information to the eavesdropper Eve (“E”).

The equivocation rate  $R_e$  in this setting is the extent of “confusion” that Eve has about the message, which is given to be

$$R_e \leq \frac{1}{n} H(W|Z^n)$$

Secrecy capacity is defined to be the maximum rate  $R$  of communication possible between Alice and Bob such that  $R =$

$R_e$ . In the following, we consider the semi-deterministic wire-tap channel with  $P(Y|X)$  having the form  $Y = f(X)$  for some deterministic function  $f$ .

#### B. Results

*Theorem 2.1:* The secrecy capacity of the semi-deterministic wire-tap channel is

$$C_s = \max_{P_X} H(Y|Z)$$

*Proof:* (Converse) We begin by considering a code with codeword length  $n$  and decoding error probability  $p_e \leq \epsilon$ . We have the following bound on  $R_e$ :

$$\begin{aligned} nR_e &\leq H(W|Z^n) \\ &= I(W; Y^n|Z^n) + H(W|Y^n, Z^n) \\ &\leq H(Y^n|Z^n) - H(Y^n|W, Z^n) + n\epsilon \\ &\leq H(Y^n|Z^n) + n\epsilon \\ &\leq \sum_{i=1}^n H(Y_i|Z_i) + n\epsilon \end{aligned} \quad (1) \quad (2) \quad (3)$$

This is justified as follows:

- (1) by the definition of mutual information;
- (2)  $H(W|Y^n, Z^n) \leq n\epsilon$  by Fano’s inequality;
- (3) by the chain rule and the fact that conditioning does not increase entropy.

The secrecy capacity is thus upper bounded by the maximum equivocation rate of the channel:

$$\begin{aligned} C_e &\triangleq \max_{P_{X^n}} R_e|_{P(\cdot)} \\ &\leq \epsilon + \max_{P_{X^n}} \frac{1}{n} \sum_{i=1}^n H(Y_i|Z_i) \\ &\leq \epsilon + \frac{1}{n} \sum_{i=1}^n \max_{P_{X_i}} H(Y_i|Z_i) \\ &= \epsilon + \max_{P_X} H(Y|Z) \end{aligned} \quad (4) \quad (5)$$

(4) follows because the sum of max’s is greater than the max of the sum; (5) follows from the memoryless property of the channel. We note that the converse is valid even when the channel is not semi-deterministic.

(Achievability) We know from [2] that the secrecy capacity of the broadcast channel with one confidential message is given by

$$C_s = \max_{\substack{P_{U,X} \\ U \rightarrow X \rightarrow (Y,Z)}} I(U; Y) - I(U; Z)$$

We choose our auxiliary random variable  $U$  to equal  $Y$ . Because the channel from  $X$  to  $Y$  is deterministic,  $U(= Y) \rightarrow X \rightarrow Y$  forms a trivial Markov chain, resulting in  $I(U; Y) = H(Y)$  and  $I(U; Z) = I(Y; Z)$ . Therefore,

$$\begin{aligned} C_s &\geq \max_{\substack{P_{U,X} \\ U=Y}} I(U; Y) - I(U; Z) \\ &= \max_{P_X} H(Y|Z) \\ &\geq C_e \end{aligned}$$

■

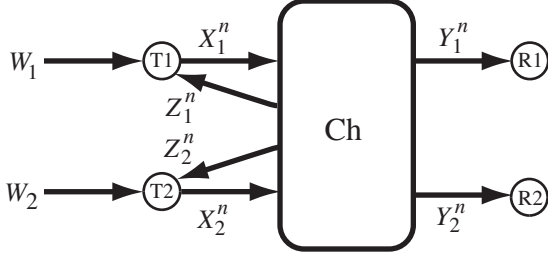


Fig. 2. Parallel Channel Model

### C. Implications

This analysis has some interesting implications. As already pointed out in the introduction, we have a non-zero secrecy capacity when  $Y$  is not a deterministic function of  $Z$ . In other words, “perfectly secure” communication with nonzero capacity from Alice to Bob is possible for a fairly large class of wire-tap channels.

Next, among all channels with a given  $\max_{P_X} H(Y|Z)$ , the semi-deterministic channel achieves the largest secrecy capacity. In essence, the upper bound derived above for secrecy capacity does not utilize determinism in any of its steps. Also, it is relatively straightforward to modify steps to a setting where the wire-tapper’s channel (from Alice to Eve) is much more general in nature (e.g., has memory).

We will use a similar framework for deriving an outer bound on the secrecy capacity region for the GMAC with confidential messages in the next section.

Before we proceed to the GMAC, we discuss a relatively straightforward generalization of the wire-tap channel discussed above. In keeping with convention, we call this channel the generalized parallel channel with confidential messages, as shown in Figure 2. The channel in this setting is defined by  $P(Z_1, Z_2|X_1, X_2)$  along with deterministic functions  $Y_1 = f_1(X_1)$  and  $Y_2 = f_2(X_2)$ .

In this setting, each transmitter  $X_i$ ,  $i \in \{1, 2\}$ , can “hear” the other transmitter as  $Z_i$ ,  $i \in \{1, 2\}$ , but wishes to keep its message confidential, i.e., desires that the other transmitter gain no knowledge of its message. This setting may arise, for example, in a wireless system where the two transmissions are occurring in orthogonal frequency/time bands (thus with no interference among users), and it is desired that each transmitter not be able to comprehend the other’s message. Note that transmitter 1’s signal at time  $t$  ( $X_{1t}$ ) is, in general, a function of its message  $W_1$  and of  $Z_1^{i-1}$ , the entire received sequence received at transmitter 1 until that time. Moreover, the channel between the two transmitters is a two-way channel. It is fairly intuitive and straightforward using the techniques introduced in this section to show that the secrecy rate region in this case is given by

$$\{(R_{1s}, R_{2s}) : R_{1s} \leq H(Y_1|Z_1), R_{2s} \leq H(Y_2|Z_2)\}$$

for all  $P_{X_1} P_{X_2}$ .

## III. GMAC WITH CONFIDENTIAL MESSAGES: MAIN RESULTS

### A. Channel Model

We adopt the GMAC with confidential messages model previously studied in [7]. In this setting, we assume that there is no common source message  $W_0$ .

The channel transition probabilities are defined by the joint  $P(Y_1|X_2)P(Y_2|X_1)P(Y|X_1, X_2)$ . Note that, in this setting we assume that  $Y_1$  is only a function of  $X_2$  at any time instant. We also do not restrict our analysis to (semi)-deterministic channels. Our goal is to determine an outer bound on the secrecy capacity region for this channel.

### B. Results

*Theorem 3.1:* The optimal equivocation rate region (and thus the secrecy capacity region) is contained in

$$R_{1,e} \leq H(Y|Y_2) \quad (6)$$

$$R_{2,e} \leq H(Y|Y_1) \quad (7)$$

$$R_{1,e} + R_{2,e} \leq H(Y|Y_2) + H(Y|Y_1, Y_2) \quad (8)$$

$$R_{1,e} + R_{2,e} \leq H(Y|Y_1) + H(Y|Y_1, Y_2) \quad (9)$$

*Proof:* Note that the steps needed to establish (6) and (7) are very similar to those taken for the wire-tap channel. Further, since (8) and (9) are symmetric in  $Y_1$  and  $Y_2$ , we finish the theorem by proving (8):

$$nR_{1,e} + nR_{2,e} \leq H(W_1|W_2, X_2^n, Y_2^n) + H(W_2|W_1, X_1^n, Y_1^n) \quad (10)$$

$$= I(W_1; Y^n|W_2, X_2^n, Y_2^n) \quad (11)$$

$$+ H(W_1|W_2, X_2^n, Y_2^n, Y^n)$$

$$+ I(W_2; Y_2^n|W_1, X_1^n, Y_1^n)$$

$$+ H(W_2|W_1, X_1^n, Y_1^n, Y_2^n)$$

$$\leq I(W_1; Y^n|W_2, X_2^n, Y_2^n)$$

$$+ H(W_2|Y_1^n, Y_2^n) + n\epsilon_1$$

$$= I(W_1; Y^n|W_2, X_2^n, Y_2^n)$$

$$+ I(W_2; Y^n|Y_1^n, Y_2^n)$$

$$+ H(W_2|Y_1^n, Y_2^n, Y^n) + n\epsilon_1$$

$$\leq I(W_1; Y^n|W_2, X_2^n, Y_2^n) \quad (12)$$

$$+ I(W_2; Y^n|Y_1^n, Y_2^n) + n\epsilon_2$$

$$\leq H(Y^n|W_2, X_2^n, Y_2^n) \quad (13)$$

$$+ H(Y^n|Y_1^n, Y_2^n) + n\epsilon_2$$

$$\leq H(Y^n|Y_2^n) + H(Y^n|Y_1^n, Y_2^n) + n\epsilon_2$$

$$\leq \sum_{i=1}^n (H(Y_i|Y_{2i}) + H(Y_i|Y_{1i}, Y_{2i})) + n\epsilon_2$$

This can be justified as follows:

(10) by the definition of equivocation rate;

(11) and (13) from definition of mutual information;

(12)  $H(W_1|W_2, X_2^n, Y_2^n, Y^n) \leq n\epsilon_1$  by Fano’s inequality and  $I(W_2; Y_2^n|W_1, X_1^n, Y_1^n) = 0$  due to conditional independence of  $W_2$  and  $Y_2^n$  given  $W_1, X_1^n, Y_1^n$ .

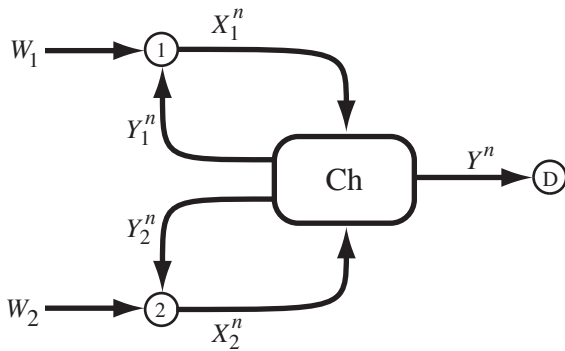


Fig. 3. GMAC with Confidential Messages Model

Note: The single-letter characterization (from the channel definition) can now be obtained by performing a suitable weighted maximization of equivocation rates, similar in spirit to the steps taken previously in obtain a single letter characterization for the wire-tap channel. ■

This is one of the first non-trivial outer bounds on the secrecy capacity for the GMAC with confidential messages. We conjecture it to be tight for the semi-deterministic GMAC with confidential messages, where the legitimate multiple access channel is deterministic. This conjecture is motivated by similar results in the (simpler) wire-tap channel case.

#### IV. DISCUSSION

In this paper, we have studied the secrecy capacity of channels (wire-tap, generalized parallel, GMAC) and of a semi-deterministic channel. Semi-deterministic channels are meaningful as they specifically model a setting where the legitimate channel has a pre-existing error correction mechanism on top of which one desires to communicate securely. The results indicate that a non-zero secrecy rate can be obtained in such systems unless the wire-tapper deterministically knows the legitimate receiver's signal. Note that regardless of the problem setting under consideration (information theoretic or computational), little to no secrecy can be guaranteed when the wire-tapper is deterministically better than/equivalent to the destination.

#### REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channel with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [3] S. K. L. Yan Cheong, "On a special class of wiretap channels," *IEEE Trans. Inform. Theory*, Sept. 1977.
- [4] H. Yamamoto, "Coding theorem for secret sharing communication systems with two noisy channels," *IEEE Trans. Inform. Theory*, May 1989.
- [5] H. Koga and N. Sato, "On an upper bound for the secrecy capacity for a general wiretap channel," *Proc. IEEE Intl. Symp. Inform. Theory*, Sept. 2005.
- [6] Y. Oohama, "Coding for relay channels with confidential messages," *Proc. IEEE Inform. Theory Workshop*, Sept. 2001.
- [7] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," *IEEE Trans. Inform. Theory*, April 2006, under review.

- [8] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inform. Theory*, May 1979.