Capacity of Cognitive Interference Channels With and Without Secrecy

Yingbin Liang, *Member, IEEE*, Anelia Somekh-Baruch, *Member, IEEE*, H. Vincent Poor, *Fellow, IEEE*, Shlomo Shamai (Shitz), *Fellow, IEEE*, and Sergio Verdú, *Fellow, IEEE*

***Abstract*—Like the conventional two-user interference channel, the cognitive interference channel consists of two transmitters whose signals interfere at two receivers. It is assumed that there is a common message (message 1) known to both transmitters, and an additional independent message (message 2) known only to the cognitive transmitter (transmitter 2). The cognitive receiver (receiver 2) needs to decode messages 1 and 2, while the noncognitive receiver (receiver 1) should decode only message 1. Furthermore, message 2 is assumed to be a confidential message which needs to be kept as secret as possible from receiver 1, which is viewed as an eavesdropper with regard to message 2. The level of secrecy is measured by the equivocation rate. In this paper, a single-letter expression for the capacity-equivocation region of the discrete memoryless cognitive interference channel is obtained. The capacity-equivocation region for the Gaussian cognitive interference channel is also obtained explicitly. Moreover, particularizing the capacity-equivocation region to the case without a secrecy constraint, the capacity region for the two-user cognitive interference channel is obtained, by providing a converse theorem.**

***Index Terms*—Capacity-equivocation region, cognitive communication, confidential messages, interference channel, rate splitting, secrecy capacity region.**

I. Introduction

INTERFERENCE channels arise in many wired and wireless communication systems, in which signals intended for one receiver cause interference at other receivers. Although the capacity region and the best coding schemes for the interference channel remain unknown, much progress has been made toward understanding this channel (see, e.g., [1]–[7] and the references therein).

Manuscript received December 18, 2007; revised September 30, 2008. Current version published February 04, 2009. The material in this paper was presented in part at the 45th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, September 2007. The work of Y. Liang and H. V. Poor was supported by the National Science Foundation under Grants ANI-03-38807, CNS-06-25637, and CCF-07-28208. The work of A. Somekh-Baruch was supported by a Marie Curie Outgoing International Fellowship within the 6th European Community Framework Programme. The work of S. Shamai and S. Verdú was supported by the US–Israel Binational Science Foundation. The work of S. Verdú was also supported by the National Science Foundation under Grant CCF-0635154.

Y. Liang is with the Department of Electrical Engineering, University of Hawaii, Honolulu, HI 96822 USA (e-mail: yingbinl@hawaii.edu).

A. Somekh-Baruch, H. V. Poor, and S. Verdú are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: anelia@princeton.edu; poor@princeton.edu; verdu@princeton.edu).

S. Shamai (Shitz) is with the Department of Electrical Engineering, Technion–Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: sshlomo@ee.technion.ac.il).

Communicated by H. Yamamoto, Associate Editor for Shannon Theory.

Color versions of Figures 2 and 3 in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2008.2009584

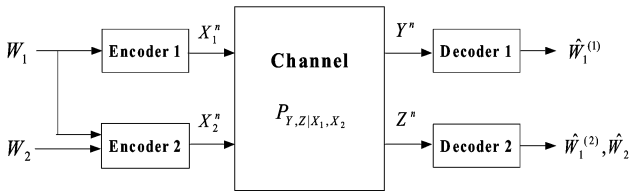

Fig. 1. Cognitive interference channel with a confidential message.

Interference not only affects communication rates, but also raises security issues: information can be extracted by nodes that are not the intended destinations. In certain situations it is desirable to minimize the leakage of information to those unintended receivers (eavesdroppers). It is also important to evaluate the secrecy level of confidential information (defined in [8] as the equivocation rate for the single-user wiretap channel) for the interference channel, and to study the achievable communication rates under a given level of secrecy constraint.

In this paper, we study the two-user cognitive interference channel with a confidential message (Fig. 1). Transmitter 1 knows only message 1, and transmitter 2 (the cognitive transmitter) knows both messages 1 and 2. Message 1 is intended for both receivers while message 2 is intended only for receiver 2. Transmitter 2 wishes to protect message 2 (the confidential message) from being decoded by receiver 1 (an eavesdropper). This channel can model the scenario in which the primary user (transmitter 1) has multicast messages for the receivers.

The problem studied in this paper can further model a cognitive radio (see [9]–[12]), introduced in certain wireless networks in order to exploit unused spectral resources. In the model we study, the cognitive radio is modeled by transmitter 2 which helps transmitter 1 (the primary transmitter) transmit its message. Moreover, the cognitive transmitter also transmits its own message, which should be kept confidential with respect to receiver 1. One scenario in which cognition by transmitter 2 takes place is when the message of transmitter 1 may withstand some delay, in which case an artificial transmission delay is introduced but is made available immediately to transmitter 2. Another scenario is when there is a high-capacity link between the transmitters, e.g., when they are collocated.

In this paper, we establish the capacity-equivocation region for discrete and Gaussian memoryless cognitive interference channels with a confidential message, which characterizes the tradeoff between the achievable communication rates and the achievable secrecy at the eavesdropper. For the case without the secrecy constraint, the capacity-equivocation region reduces to the capacity region of the cognitive interference channel. This

establishes a new capacity theorem for a class of interference channels, by providing a converse theorem.

We note that the cognitive interference channel (without secrecy constraints) was studied in [13, Theorem 5], where an achievable rate region (inner bound on the capacity region) is given. An achievable error exponent for this channel was studied in [14]. In this paper, we provide an outer bound on the capacity region that matches the inner bound given in [13, Theorem 5] and hence establishes the capacity region for this channel. We also note that the channel we study is different from the channel model studied in [11], [12], [15], [16] in that receiver 2 is required to decode both messages 1 and 2. Furthermore, we also address secrecy, which was not considered in [11]–[16]. We finally note that the model we study is different from the model in [17], which does not assume a cognitive transmitter that knows the other transmitter's message and does not assume a receiver that decodes both messages either.

The rest of the paper is organized as follows. In Section II, we introduce the model for the cognitive interference channel with a confidential message. In Section III, we present the capacity-equivocation region, and in Section IV, we apply our results to the Gaussian case. In Section V, we study the cognitive interference channel without secrecy constraints.

II. Channel Model

Definition 1: A discrete memoryless cognitive interference channel consists of finite channel input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, finite channel output alphabets $\mathcal{Y}$ and $\mathcal{Z}$, and a transition probability distribution $P_{Y,Z|X_1,X_2}$ (see Fig. 1), where $x_1 \in \mathcal{X}_1$ and $x_2 \in \mathcal{X}_2$ are channel inputs from transmitters 1 and 2, respectively, and $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$ are channel outputs at receivers 1 and 2, respectively.

Transmitters 1 and 2 jointly send a message denoted by W_1 to receivers 1 and 2, and transmitter 2 sends a message denoted by W_2 to receiver 2 and wants to prevent receiver 1 from decoding W_2 reliably. Hence, the message W_2 is referred to as the confidential message with respect to receiver 1.

In the sequel, we use x^n to indicate the vector $(x_1, \ldots, x_n)$, and use x_i^n to indicate the vector $(x_i, \ldots, x_n)$.

Definition 2: A $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code for the cognitive interference channel consists of the following:

- two message sets: $\mathcal{W}_k = \{1, 2, \ldots, 2^{nR_k}\}$ for $k = 1, 2$;
- two messages: W_1 and W_2 are independent random variables equiprobably distributed over $\mathcal{W}_1$ and $\mathcal{W}_2$, respectively;
- two encoders: a deterministic encoder f_1: $\mathcal{W}_1 \rightarrow \mathcal{X}_1^n$, which maps message $w_1 \in \mathcal{W}_1$ to a codeword $x_1^n \in \mathcal{X}_1^n$; and a stochastic encoder[1] f_2: $\mathcal{W}_1 \times \mathcal{W}_2 \rightarrow \mathcal{X}_2^n$, which maps message pair $(w_1, w_2) \in \mathcal{W}_1 \times \mathcal{W}_2$ to a codeword $x_2^n \in \mathcal{X}_2^n$;
- two decoders: g_1: $\mathcal{Y}^n \rightarrow \mathcal{W}_1$, which maps a received sequence y^n to a message $\hat{w}_1^{(1)} \in \mathcal{W}_1$; and g_2: $\mathcal{Z}^n \rightarrow \mathcal{W}_1 \times \mathcal{W}_2$, which maps a received sequence z^n to a message pair $(\hat{w}_1^{(2)}, \hat{w}_2) \in \mathcal{W}_1 \times \mathcal{W}_2$.

[1]We note that the stochastic encoder f_2 defines a transition probability distribution $f_2(x_2^n|w_1, w_2)$. In fact, f_2 can be equivalently represented by a deterministic mapping $\mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{T} \rightarrow \mathcal{X}_2^n$, which maps $(w_1, w_2, t) \in \mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{T}$ to a codeword $x_2^n \in \mathcal{X}_2^n$, where t is a realization of a randomizing variable T that is independent of (W_1, W_2). The distribution of T is part of the encoding strategy of transmitter 2. We assume this distribution is known at both receivers, but the realization of T is not known at either receiver.

For a given code, we define the probability of error and the secrecy level of the confidential message W_2. The average block probability of error is defined as

$$P_e^{(n)} = \frac{1}{2^{n(R_1+R_2)}} \times \sum_{w_1=1}^{2^{nR_1}} \sum_{w_2=1}^{2^{nR_2}} \Pr\left\{\left(\hat{w}_1^{(1)}, \hat{w}_1^{(2)}, \hat{w}_2\right) \neq (w_1, w_1, w_2)\right\}. \quad (1)$$

The secrecy level of message W_2 at receiver 1 is measured by the normalized equivocation

$$R_e^{(n)} = \frac{1}{n} H(W_2|Y^n) \quad (2)$$

where throughout this paper we use the convention that logarithms are taken to the base 2 (and entropy is measured in bits).

A rate-equivocation triple (R_1, R_2, R_e) is said to be *achievable* if there exists a sequence of $\left(2^{nR_1}, 2^{nR_2}, n\right)$ codes with

$$\lim_{n\rightarrow\infty} P_e^{(n)} = 0$$

and

$$R_e \leq \liminf_{n\rightarrow\infty} R_e^{(n)}.$$

Definition 3: The *capacity-equivocation region* $\mathfrak{C}$ is the closure of the union of all achievable rate-equivocation triples (R_1, R_2, R_e).

Definition 4: The secrecy capacity region, $\mathcal{C}_s$, is defined by

$$\mathcal{C}_s = \{(R_1, R_2) : (R_1, R_2, R_2) \in \mathfrak{C}\} \quad (3)$$

that is, the region that includes all achievable rate-pairs (R_1, R_2) such that perfect secrecy is achieved for the message W_2.

III. Main Results

We first provide an achievable rate-equivocation region for the cognitive interference channel in the following lemma.

Lemma 1: The following region is achievable for the cognitive interference channel with a confidential message:

$$\mathfrak{R} = \bigcup_{P_{U,X_1,X_2} P_{Y,Z|X_1,X_2}} \left\{ \begin{array}{l} (R_1, R_2, R_{21}, R_{22}, R_e): \\ R_1 \geq 0, R_2 \geq 0, R_{22} \geq R_e \geq 0, R_{21} \geq 0 \\ R_2 = R_{21} + R_{22} \\ R_1 + R_{21} \leq I(U, X_1; Y) \\ R_{22} \leq I(X_2; Z|U, X_1) \\ R_{21} + R_{22} \leq I(U, X_2; Z|X_1) \\ R_1 + R_{21} + R_{22} \leq I(U, X_1, X_2; Z) \\ R_e \leq I(X_2; Z|U, X_1) - I(X_2; Y|U, X_1) \\ R_{21} + R_e \leq I(U, X_2; Z|X_1) - I(X_2; Y|U, X_1) \\ R_1 + R_{21} + R_e \leq I(U, X_1, X_2; Z) - I(X_2; Y|U, X_1) \end{array} \right\}. \quad (4)$$

Proof: We outline the achievable scheme in the following. The details of the proof and the computation of the equivocation rate are relegated to Appendix A. Message W_2 is split into two components, W_{21} and W_{22}, with rates indicated by R_{21} and R_{22}, respectively, in (4). Receiver 1 decodes both W_1 and W_{21}, and receiver 2 decodes W_1, W_{21} and W_{22}. Since W_{21} is decoded and fully known at receiver 1, W_{21} does not contribute to the secrecy level of W_2 at receiver 1 (the eavesdropper). Hence, only W_{22} may be hidden from the eavesdropper. □

Our main result is the following.

Theorem 1: For the cognitive interference channel with a confidential message, the capacity-equivocation region is given by

$$\mathfrak{C} = \bigcup_{P_{U,X_1,V}P_{X_2|V}P_{Y,Z|X_1,X_2}} \left\{ \begin{array}{l} (R_1, R_2, R_e): \\ R_1 \geq 0, R_2 \geq R_e \geq 0 \\ R_1 \leq \min\{I(U,X_1;Y), I(U,X_1;Z)\} \\ R_2 \leq I(U,V;Z|X_1) \\ R_1 + R_2 \leq \min\{I(U,X_1;Y), I(U,X_1;Z)\} \\ \qquad\qquad +I(V;Z|U,X_1) \\ R_e \leq I(V;Z|U,X_1) - I(V;Y|U,X_1) \end{array} \right\} \quad (5)$$

where the auxiliary random variables U and V are bounded in cardinality by

$$|\mathcal{U}| \leq |\mathcal{X}_1| \cdot |\mathcal{X}_2| + 3$$

and

$$|\mathcal{V}| \leq |\mathcal{X}_1|^2 \cdot |\mathcal{X}_2|^2 + 4|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 3$$

respectively.

Proof: To establish the achievability part of Theorem 1, we first note that if we define a random variable V that satisfies the Markov chain condition $(X_1, U) \leftrightarrow V \leftrightarrow X_2$, and change X_2 to be V in $\mathcal{R}$ given in Lemma 1, the resulting region is also achievable. This follows by prefixing one discrete memoryless channel with the input V and the transition probability $P_{X_2|V}$ to transmitter 2 (similarly to [18, Lemma 4]). For this new achievable region, we apply *Fourier–Motzkin elimination* (see, e.g., [19, pp. 155–156]) to eliminate R_{21} and R_{22} from the bounds and then obtain the following region:

$$\mathfrak{C}' = \bigcup_{P_{U,X_1,V}P_{X_2|V}P_{Y,Z|X_1,X_2}} \left\{ \begin{array}{l} (R_1, R_2, R_e): \\ R_1 \geq 0, R_2 \geq R_e \geq 0 \\ R_1 \leq I(U,X_1;Y) \\ R_2 \leq I(U,V;Z|X_1) \\ R_1 + R_2 \leq \min\{I(U,X_1;Y), I(U,X_1;Z)\} \\ \qquad\qquad +I(V;Z|U,X_1) \\ R_e \leq R_2 \\ R_e \leq I(V;Z|U,X_1) - I(V;Y|U,X_1) \\ R_1 + R_e \leq I(U,V,X_1;Z) - I(V;Y|U,X_1) \end{array} \right\}. \quad (6)$$

Now the achievability of the region $\mathfrak{C}$ in (5) follows from the region $\mathfrak{C}'$ in (6) by adding one bound on R_1 and removing the bound on $R_1 + R_e$ that becomes redundant. The bounds on cardinality of $|\mathcal{U}|$ and $|\mathcal{V}|$ can be derived by following the steps in [18, Appendix].

The proof of the converse part of Theorem 1 is relegated to Appendix B. □

Remark 1: It is easy to see that $\mathfrak{C}' = \mathfrak{C}$. The preceding proof indicates that $\mathfrak{C} \subseteq \mathfrak{C}'$, and $\mathfrak{C}' \subseteq \mathfrak{C}$ follows because $\mathfrak{C}$ is the capacity-equivocation region established by the converse proof given in Appendix B.

Remark 2: The capacity-equivocation region of the cognitive interference channel with a confidential message given in (5) reduces to the capacity-equivocation region of the broadcast channel with confidential messages given in [18, Theorem 1] when setting $X_1 = \phi$.

For the case of perfect secrecy, we obtain the following secrecy capacity region based on Theorem 1.

Corollary 1: The secrecy capacity region of the cognitive interference channel with a confidential message is given by

$$\mathcal{C}_s = \bigcup_{P_{U,X_1,V}P_{X_2|V}P_{Y,Z|X_1,X_2}} \left\{ \begin{array}{l} (R_1, R_2): \\ R_1 \geq 0, R_2 \geq 0 \\ R_1 \leq \min\{I(U,X_1;Y), I(U,X_1;Z)\} \\ R_2 \leq I(V;Z|U,X_1) - I(V;Y|U,X_1) \end{array} \right\} \quad (7)$$

where the auxiliary random variables U and V are bounded in cardinality by

$$|\mathcal{U}| \leq |\mathcal{X}_1| \cdot |\mathcal{X}_2| + 3$$

and

$$|\mathcal{V}| \leq |\mathcal{X}_1|^2 \cdot |\mathcal{X}_2|^2 + 4|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 3$$

respectively.

Next, we present the capacity-equivocation region for two classes of degraded cognitive interference channels, which will be useful when we study the Gaussian case.

Corollary 2: If the cognitive interference channel satisfies the following degradedness condition

$$P_{Y,Z|X_1,X_2} = P_{Y|X_1,X_2} P_{Z|Y,X_1}, \quad (8)$$

then the capacity-equivocation region is given by

$$\mathfrak{C}_{d1} = \bigcup_{P_{X_1,X_2}P_{Y,Z|X_1,X_2}} \left\{ \begin{array}{l} (R_1, R_2, 0): \\ R_1 \geq 0, R_2 \geq 0 \\ R_2 \leq I(X_2;Z|X_1) \\ R_1 + R_2 \leq \min\{I(X_1,X_2;Y), I(X_1,X_2;Z)\} \end{array} \right\}. \quad (9)$$

Proof: The achievability follows from the region $\mathfrak{C}$ given in (5) by setting $U = V = X_2$. The proof of the converse part is relegated to Appendix C. □

We note that no secrecy can be achieved, i.e., $R_e = 0$, if the channel satisfies the degradedness condition (8). This is because receiver 2's input Z is a degraded version of receiver 1's input

Y, and hence receiver 1 can obtain any information that receiver 2 obtains.

Corollary 3: If the cognitive interference channel satisfies the following degradedness condition

$$P_{Y,Z|X_1,X_2} = P_{Z|X_1,X_2} P_{Y|Z,X_1} \tag{10}$$

then the capacity-equivocation region is given by

$$\mathfrak{C}_{d2} = \bigcup_{P_{U,X_1,X_2} P_{Y,Z|X_1,X_2}} \left\{ \begin{array}{l} (R_1, R_2, R_e): \\ R_1 \geq 0, R_2 \geq 0, R_e \geq 0 \\ R_1 \leq \min\{I(U,X_1;Y), I(U,X_1;Z)\} \\ R_2 \leq I(X_2;Z|U,X_1) \\ R_e \leq R_2 \\ R_e \leq I(X_2;Z|U,X_1) - I(X_2;Y|U,X_1) \end{array} \right\} \tag{11}$$

where the auxiliary random variables U is bounded in cardinality by $|\mathcal{U}| \leq |\mathcal{X}_1| \cdot |\mathcal{X}_2| + 1$.

Proof: The achievability follows from (5) by setting $V = X_2$ and observing that $I(X_2;Z|U,X_1) \leq I(U,X_2;Z|X_1)$ and that the sum-rate bound in (5) is equal to the sum of the two bounds on the individual rates in (11). The proof of the converse part is relegated to Appendix D. □

We note that the equivocation rate given in (11) can be positive. This is because now receiver 1's input Y is a degraded version of receiver 2's input Z if X_1 is given. Hence, receiver 2 may be able to receive some information that receiver 1 cannot obtain.

Corollary 2 (and similarly, Corollary 3) continues to hold also for a stochastically degraded channel, i.e., a channel $P_{Y,Z|X_1,X_2}$ whose conditional marginal distributions $P_{Y|X_1,X_2}$ and $P_{Z|X_1,X_2}$ are the same as those of a channel satisfying the degradedness condition (8) (and correspondingly (10) for Corollary 3).

We note that while achieving the capacity-equivocation region for the general cognitive interference channel with a confidential message requires application of a rate splitting scheme (described in the proof for Lemma 1 in Appendix A), it is unnecessary for the degraded channels that satisfy either (8) or (10).

IV. Gaussian Cognitive Interference Channels With Confidential Messages

In this section, we consider the Gaussian cognitive interference channel. The channel outputs at receivers 1 and 2 at time instant i are given, respectively, by

$$\begin{aligned} Y_i &= X_{1,i} + aX_{2,i} + N_{1,i} \\ Z_i &= bX_{1,i} + X_{2,i} + N_{2,i} \end{aligned} \tag{12}$$

where $\{N_{1,i}\}_{i=1}^{\infty}$ and $\{N_{2,i}\}_{i=1}^{\infty}$ are independent memoryless unit-variance Gaussian processes, and a and b are real constants. We assume that the transmitters are subject to the following power constraints:

$$\frac{1}{n}\sum_{i=1}^{n} X_{1,i}^2 \leq P_1 \quad \text{and} \quad \frac{1}{n}\sum_{i=1}^{n} X_{2,i}^2 \leq P_2. \tag{13}$$

We consider the cases with $|a| \geq 1$ and $|a| < 1$, separately. For the case when $|a| \geq 1$, the channel satisfies the degradedness condition (8). It follows from Corollary 2 that no secrecy can be achieved whenever $|a| \geq 1$, i.e., $R_e = 0$. We further have the following theorem on the capacity-equivocation region based on Corollary 2.

Theorem 2: For the Gaussian cognitive interference channel with a confidential message, if $|a| \geq 1$, then the capacity-equivocation region is given by

$$\mathfrak{C} = \bigcup_{-1 \leq \rho \leq 1} \left\{ \begin{array}{l} (R_1, R_2, 0): \\ R_1 \geq 0, R_2 \geq 0 \\ R_2 \leq \frac{1}{2}\log\left(1 + (1-\rho^2)P_2\right) \\ R_1 + R_2 \leq \frac{1}{2}\log\left(1 + b^2P_1 + P_2 + 2b\rho\sqrt{P_1P_2}\right) \\ R_1 + R_2 \leq \frac{1}{2}\log\left(1 + P_1 + a^2P_2 + 2a\rho\sqrt{P_1P_2}\right) \end{array} \right\} \tag{14}$$

where the logarithmic function is to the base 2.

Proof: The achievability follows from (9) given in Corollary 2 by computing the mutual information terms with (X_1, X_2) that are zero-mean jointly Gaussian with $E\left[X_1^2\right] = P_1$, $E\left[X_2^2\right] = P_2$, and $E[X_1X_2] = \rho\sqrt{P_1P_2}$.

The converse follows by applying the bounds in the converse proof for Corollary 2 (see Appendix C) to the Gaussian case. The power constraints (13) translate to upper bounds on the second moments of X_1 and X_2, i.e., $E\left[X_1^2\right] \leq P_1$ and $E\left[X_2^2\right] \leq P_2$. The proof also applies the degradedness condition (8). The details of the proof are provided in Appendix E. □

In Fig. 2, the capacity region of the Gaussian cognitive interference channel is shown for $P_1 = P_2 = 1$, $b = 3$, and $a = 1, 2, 3$. In fact, in this case, the capacity region is the same for all $a \geq 3$ as one can see in (14). This is because for the chosen parameters $P_1 = P_2 = 1$ and $b = 3$, if $a \geq 3$, receiver 1 always decodes W_1 if receiver 2 decodes this message. Hence, receiver 2 is the bottleneck receiver.

For the case when $|a| < 1$, the channel satisfies the degradedness condition (10). It follows from Corollary 3 that the equivocation rate in this case can be positive. We give the capacity-equivocation region for this case in the following.

Theorem 3: For the Gaussian cognitive interference channel with a confidential message, if $|a| < 1$, the capacity-equivocation region is given by

$$\mathfrak{C} = \bigcup_{-1 \leq \rho \leq 1, 0 \leq \beta \leq 1} \left\{ \begin{array}{l} (R_1, R_2, R_e): \\ R_1 \geq 0, R_2 \geq R_e \geq 0 \\ R_1 \leq \frac{1}{2}\log\left(1 + \frac{P_1 + \rho^2a^2P_2 + 2\rho a\sqrt{\beta P_1 P_2}}{1 + (1-\rho^2)a^2P_2}\right) \\ R_1 \leq \frac{1}{2}\log\left(1 + \frac{b^2P_1 + \rho^2P_2 + 2\rho b\sqrt{\beta P_1 P_2}}{1 + (1-\rho^2)P_2}\right) \\ R_2 \leq \frac{1}{2}\log\left(1 + (1-\rho^2)P_2\right) \\ R_e \leq \frac{1}{2}\log\left(1 + (1-\rho^2)P_2\right) \\ \qquad -\frac{1}{2}\log\left(1 + (1-\rho^2)a^2P_2\right) \end{array} \right\}. \tag{15}$$

We note that in (15), if $a > 0$ and $b > 0$, then it is sufficient to consider $\beta = 1$ while if $a < 0$ and $b < 0$, then it is sufficient to consider $\beta = 0$.

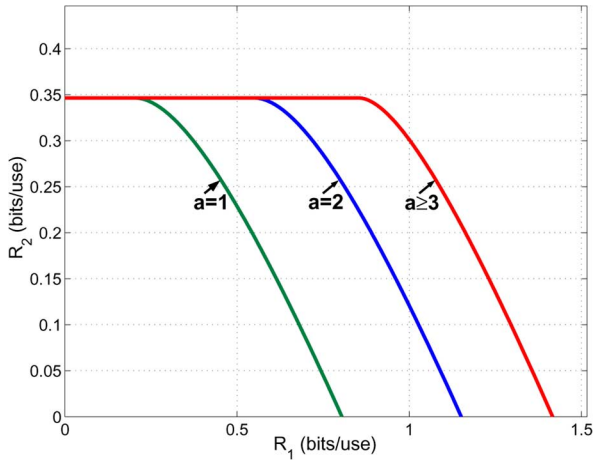

Fig. 2. The capacity region of the Gaussian cognitive interference channel for $P_1 = P_2 = 1$, $b = 3$, and $a > 1$.

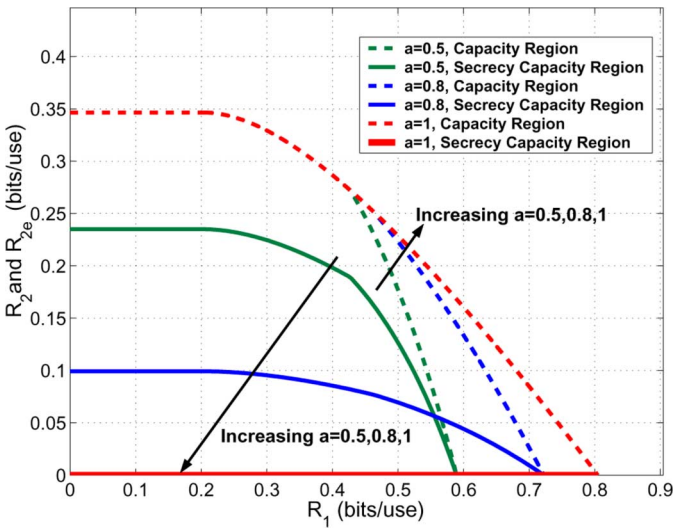

Fig. 3. The capacity region and the secrecy-capacity region of the Gaussian cognitive interference channel for $P_1 = P_2 = 1$ and $b = 1$.

Proof: The achievability follows from (11) given in Corollary 3 by setting $V = X_2$ and computing the mutual information terms with (U, X_1, X_2) having the following joint distribution:

$$\begin{aligned} X_1 &\sim \mathcal{N}(0, P_1) \\ U &= \rho\sqrt{\frac{\beta P_2}{P_1}} X_1 + U' \\ X_2 &= U + X_2' \end{aligned} \tag{16}$$

where $U' \sim \mathcal{N}(0, \bar{\beta}\rho^2 P_2)$ and $X_2' \sim \mathcal{N}(0, (1-\rho^2)P_2)$, and X_1, U' and X_2' are independent.

The converse follows by applying the bounds in the converse proof for Corollary 3 (see Appendix D) to the Gaussian case and applying the entropy power inequality. The proof also applies the degradedness condition (10) that this case satisfies. The details of the proof are provided in Appendix F. □

In Fig. 3, the capacity region and the secrecy capacity region of the Gaussian cognitive interference channel are shown for $P_1 = P_2 = 1$, $b = 1$, and $a = 0.5, 0.8$, and 1. It can be seen that as a increases, receiver 1 decodes more information about W_2 via rate splitting. While this helps receiver 1 improve R_1 by interference cancellation, it causes the equivocation rate R_e to decrease due to more leakage of W_2 to receiver 1. When $a = 1$, receiver 1 decodes everything that receiver 2 decodes, and hence $R_e = 0$, which is consistent with Theorem 2.

Remark 3: Theorems 14 and 15 are valid for both positive and negative values of a and b.

V. Implications for Cognitive Interference Channels

In Sections III and IV, we studied the cognitive interference channel with a confidential message. If we drop the secrecy constraint, i.e., the message W_2 need not be confidential from receiver 1, the capacity-equivocation region given in Theorem 1 reduces to the capacity region of the corresponding cognitive interference channel without secrecy constraints.

Theorem 4: The capacity region of the cognitive interference channel is given by

$$C = \bigcup_{P_{U,X_1,X_2} P_{Y,Z|X_1,X_2}} \left\{ \begin{array}{l} (R_1, R_2): \\ R_1 \geq 0, R_2 \geq 0 \\ R_1 \leq I(U, X_1; Y) \\ R_2 \leq I(X_2; Z|X_1) \\ R_1 + R_2 \leq \min\{I(U, X_1; Y), I(U, X_1; Z)\} \\ \qquad\qquad + I(X_2; Z|U, X_1) \end{array} \right\} \tag{17}$$

where the auxiliary random variable U is bounded in cardinality by $|\mathcal{U}| \leq |\mathcal{X}_1| \cdot |\mathcal{X}_2| + 1$.

Proof: From Theorem 1, we deduce that the capacity region of the cognitive interference channel is given by (17) with an additional bound $R_1 \leq I(U, X_1; Z)$. This is done by setting $R_e = 0$ and because the remaining bounds do not decrease if one sets $V = X_2$ due to the Markov chain relationship $V \leftrightarrow (X_1, X_2) \leftrightarrow (Y, Z)$. We further show that the bound $R_1 \leq I(U, X_1; Z)$ is, in fact, redundant. This can be seen from the achievability proof in Appendix A that for the case without secrecy constraints, the bound $R_1 \leq I(U, X_1; Z)$ is not necessary. □

We note that region (17) was given as an achievable rate region (i.e., an inner bound on the capacity region) in [13, Theorem 5]. The converse proof in Appendix B that we have given to show the more general result of Theorem 1 provides a converse to establish that the region (17) is, in fact, the capacity region. We also note that another achievable region for the cognitive interference channel (without secrecy constraints) was reported in [14], which is included within the larger achievable region in [13, Theorem 5].

Remark 4: In our definition of the interference channel in Section II, we require encoder 1 be a deterministic encoder. In fact, for the case without secrecy, the capacity region given in (17) holds for the case when encoder 1 is stochastic. This can be seen from the converse proof for Theorem 1 that does not rely on the fact that encoder 1 is deterministic if there is no secrecy constraint.

The cognitive interference channel includes a few classical channels as special cases.

Remark 5: The cognitive interference channel reduces to the broadcast channel with degraded message sets studied in [20] if we set $X_1 = \phi$. Under this condition, it is easy to see that the capacity region of the cognitive interference channel given in Theorem 4 reduces to the capacity region of the broadcast channel with degraded message sets given in [21, p. 360, Theorem 4.1] which was shown to be equivalent to the capacity region given in [20].

Remark 6: The capacity region of the cognitive interference channel reduces to the capacity region of the multiple-access channel with degraded message sets given in [22] (see also [23]) if we set $Y = Z$. In this case, the region given in (17) becomes

$$C = \bigcup_{\substack{P_{U,X_1,X_2} \\ P_{Z|X_1,X_2}}} \left\{ \begin{array}{l} (R_1, R_2): \\ R_1 \geq 0, R_2 \geq 0 \\ R_1 \leq I(U, X_1; Z) \\ R_2 \leq I(X_2; Z|X_1) \\ R_1 + R_2 \leq I(X_1, X_2; Z) \end{array} \right\}. \tag{18}$$

It is easy to see that (18) is maximized by setting $U = X_2$, and hence the bound on R_1 is not necessary. The resulting region is the capacity region of the multiple-access channel with degraded message sets given in [22] (see also [23]).

Corollary 4: By setting $R_e = 0$, Theorems 2 and 3 respectively, reduce to the capacity regions in the cases $|a| \geq 1$ and $|a| < 1$ for the Gaussian cognitive interference channel without secrecy constraints, where the cognitive receiver is required to reliably decode both messages.

It is interesting to compare the cognitive setup studied in this section to the model in which each decoder is interested only in its own message, as in [11], [12], [15], [16]. The additional constraint that decoder 2 decodes also message W_1, enables the determination of the capacity region for a general discrete memoryless channel (DMC) and for all the regimes for the Gaussian case.

VI. Conclusion

In this paper, we have presented a single-letter characterization of the capacity-equivocation region of the cognitive interference channel with a confidential message. The capacity-achieving random scheme is based on superposition coding, rate-splitting, and stochastic encoding. We have further specialized the expression for the capacity-equivocation region to several cases: a) *perfect secrecy*, that is, the secrecy-capacity region; b) no secrecy constraints, i.e., a new capacity theorem for the cognitive interference channel; c) a *degraded channel* in which given the first channel input, the observation available to the receiver that decodes both messages is a degraded version of the observation available to the eavesdropping receiver; and d) a *degraded channel* in which given the first channel input, the observation available to the eavesdropping receiver is a degraded version of the observation available to the other receiver. We have also explicitly characterized the capacity-equivocation region of the Gaussian cognitive interference channel with a confidential message, which falls under cases c) or d).

Appendix A
Proof of Lemma 1

We present the proof in three steps. In step 1, we prove existence of a certain codebook based on a random coding technique. In step 2, we define our encoding scheme. In step 3, we compute the equivocation rate.

Step 1: Existence of a Certain Codebook: For a real number d, let $[1, d]$ denote $\{1, 2, \ldots, \lfloor d \rfloor\}$, where $\lfloor d \rfloor$ denotes the largest integer that is less than or equal to d. We denote the messages by $W_1 \in \mathcal{W}_1 = [1, 2^{nR_1}]$, $W_{21} \in \mathcal{W}_{21} = [1, 2^{nR_{21}}]$, and $W_{22} \in \mathcal{W}_{22} = [1, 2^{nR_{22}}]$, respectively, where we split the message W_2 into two components W_{21} and W_{22} with rates indicated by R_{21} and R_{22}, respectively.

We consider the following joint distribution:

$$P_{UX_1X_2YZ} = P_{U,X_1,X_2} P_{Y,Z|X_1,X_2}.$$

We use $T_\epsilon^n(P_{UX_1X_2YZ})$ to denote the strong typical set based on the distribution $P_{UX_1X_2YZ}$ (see [21, Sec. 1.2]). For a given length-n sequence x^n, $T_\epsilon^n\left(P_{U|X}|x^n\right)$ denotes the set of sequences u^n such that $(u^n, x^n) \in T_\epsilon^n(P_{UX_1})$.

Consider a given nonnegative rate-triple (R_1, R_{21}, R_{22}), i.e., $R_1 \geq 0$, $R_{21} \geq 0$, $R_{22} \geq 0$, that satisfies the following inequalities:

$$\begin{aligned} R_1 + R_{21} &\leq I(U, X_1; Y) \\ R_{22} &\leq I(X_2; Z|U, X_1) \\ R_{21} + R_{22} &\leq I(U, X_2; Z|X_1) \\ R_1 + R_{21} + R_{22} &\leq I(U, X_1, X_2; Z). \end{aligned} \tag{19}$$

We define

$$\begin{aligned} R_2' = \min\{&I(X_2; Z|U, X_1), I(U, X_2; Z|X_1) - R_{21}, \\ &I(U, X_1, X_2; Z) - R_1 - R_{21}\} \end{aligned} \tag{20}$$

and we note that R_2' represents the maximum achievable rate for W_{22}.

We now consider the following codebook:

$$\mathbb{C} = \left\{ \begin{array}{ll} x_{1,i}^n & i = 1, \ldots, 2^{nR_1}; \\ u_{ik}^n & i = 1, \ldots, 2^{nR_1}; k = 1, \ldots, 2^{nR_{21}} \\ x_{2,ikab}^n, & i = 1, \ldots, 2^{nR_1}; k = 1, \ldots, 2^{nR_{21}}; \\ & a = 1, \ldots, A; b = 1, \ldots, B; \end{array} \right\} \tag{21}$$

where all codewords are strongly typical, i.e.,

$$\begin{aligned} &x_{1,i}^n \in T_\epsilon^n(P_{X_1}), u_{ik}^n \in T_\epsilon^n\left(P_{U|X_1}|x_{1,i}^n\right), \\ &x_{2,ikab}^n \in T_\epsilon^n\left(P_{X_2|UX_1}|u_{ik}^n, x_{1,i}^n\right) \end{aligned} \tag{22}$$

for all i, k, a, b, and

$$\begin{aligned} \frac{1}{n}\log A &= R_2' - I(X_2; Y|U, X_1) \\ \frac{1}{n}\log B &= I(X_2; Y|U, X_1). \end{aligned} \tag{23}$$

Note that for the achievability scheme, we are interested in only the joint distributions $P_{UX_1X_2YZ}$ such that

$$R_2' - I(X_2; Y|U, X_1) \geq 0.$$

This can be seen in Lemma 1 by requiring $R_e \geq 0$.

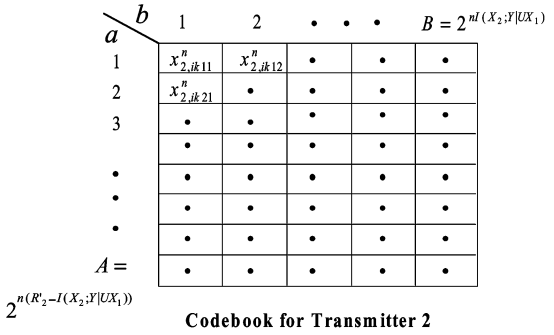

Fig. 4. Codebook for encoder 2.

We define the following error probabilities when the codewords $x_{1,i}^n$ and $x_{2,ikab}^n$ are transmitted by transmitters 1 and 2, respectively:

$$\begin{aligned}\lambda_{ikab} &= \text{Error probability for receiver 1} \\ &\quad \text{in determining } i \text{ and receiver 2} \\ &\quad \text{in determining } i,k,a,b; \\ \lambda_{2,b|ika} &= \text{Error probability for receiver 1} \\ &\quad \text{in determining } b \text{ given } (i,k,a).\end{aligned}$$

We note that receiver 1 decodes b, although it is not required to, because this requirement helps in bounding R_e (see step 3 in the sequel).

Let p_{ikab} be the probability that codewords $x_{1,i}^n$ and $x_{2,ikab}^n$ are transmitted by transmitters 1 and 2, respectively. We further define the following average error probabilities:

$$\lambda = \sum_{ikab} p_{ikab}\lambda_{ikab} \tag{24}$$

$$\lambda_2 = \sum_{ikab} p_{ikab}\lambda_{2,b|ika}. \tag{25}$$

The following lemma guarantees existence of a certain codebook, which will be used for encoding in step 2.

Lemma 2: For any $0 < \eta < 1$, there exists a codebook as described in (21), such that, for sufficiently large n

$$\lambda < \eta \quad \text{and} \quad \lambda_2 < \eta. \tag{26}$$

In Fig. 4, we plot an example codebook for transmitter 2 that is described in the preceding lemma. We can interpret each row of the codebook as a subcodebook. Receiver 2 can decode no matter which codeword in the codebook was transmitted by transmitter 2 with small average error probability, because $\lambda < \eta$. However, receiver 1 is only guaranteed to decode the codeword sent by transmitter 2 with small average probability of error if it knows to which row the transmitted codeword belongs. This is because $\lambda_2 < \eta$.

We prove the lemma using a random coding technique. We define the following sum of error probabilities:

$$p_e = \lambda + \lambda_2 = \sum_{ikab} p_{ikab}(\lambda_{ikab} + \lambda_{2,b|ika}). \tag{27}$$

We show that the average of p_e over a random codebook ensemble is small for sufficiently large codeword length n. Then, there must exist at least one codebook such that p_e is small for sufficiently large n.

For a given distribution P_{U,X_1,X_2}, we construct random codebooks by the following generating steps.

1. Generate 2^{nR_1} codewords $x_{1,i}^n$, $i = 1,\ldots,2^{nR_1}$, each uniformly drawn from the set $T_\epsilon^n(P_{X_1})$.
2. For each $x_{1,i}^n$, generate $2^{nR_{21}}$ codewords u_{ik}^n, $k = 1,\ldots,2^{nR_{21}}$, each uniformly drawn from the set $T_\epsilon^n(P_{U|X_1}|x_{1,i}^n)$.
3. For each $x_{1,i}^n$ and u_{ik}^n, generate $A \cdot B$ codewords $x_{2,ikab}^n$, $a = 1,\ldots,A$; $b = 1,\ldots,B$, each uniformly drawn from the set $T_\epsilon^n\left(P_{X_2|UX_1}|u_{ik}^n, x_{1,i}^n\right)$.

Suppose the codewords $x_{1,i}^n$ and $x_{2,ikab}^n$ are transmitted by transmitters 1 and 2, respectively, and define the following decoding strategies at receivers 1 and 2.

1. Receiver 1 declares that the index of x_1^n is $\hat{i}$ if all $\left(x_{1,i}^n, u_{ik}^n, y^n\right) \in T_\epsilon^n(P_{UX_1Y})$ have the common index $i = \hat{i}$. If no such $\hat{i}$ is found an error is declared.
2. Receiver 1, if given the indices (i,k,a), declares that the index of $x_{2,ikab}^n$ is $\hat{b}$ if it is the unique index such that $\left(x_{1,i}^n, u_{ik}^n, x_{2,ika\hat{b}}^n, y^n\right) \in T_\epsilon^n(P_{UX_1X_2Y})$. If no such $\hat{b}$ is found an error is declared.
3. Receiver 2 declares that the indices of x_1^n and x_2^n are $(\hat{i},\hat{k},\hat{a},\hat{b})$ if it is the unique set of these indices such that $\left(x_{1,\hat{i}}^n, u_{\hat{i}\hat{k}}^n, x_{2,\hat{i}\hat{k}\hat{a}\hat{b}}^n, z^n\right) \in T_\epsilon^n(P_{UX_1X_2Z})$. If no such $(\hat{i},\hat{k},\hat{a},\hat{b})$ are found an error is declared.

We can compute $\mathrm{E}_{\mathbb{C}}[p_e]$ by following the standard techniques as in [24, Ch. 15], where $\mathrm{E}_{\mathbb{C}}$ indicates an average over the random codebook ensemble. We can show that

$$\mathrm{E}_{\mathbb{C}}[p_e] < \eta \tag{28}$$

for sufficiently large codeword length n, by using the sizes of indices i, k, a, and b given in (19) and(23).

Hence there exists one codebook such that for sufficiently large codebook size n

$$p_e = \lambda + \lambda_2 < \eta. \tag{29}$$

This leads to the conclusion that for sufficiently large codebook size n

$$\lambda < \eta \quad \text{and} \quad \lambda_2 < \eta. \tag{30}$$

Step 2: Encoding: In the following, we consider the case in which $R_{22} > \frac{1}{n}\log A$ and compute the equivocation rate for this case in step 3. For the case in which $R_{22} \le \frac{1}{n}\log A$, the encoding scheme and computation of the equivocation rate are similar and are briefly described at the end of the proof. We define the following sets:

$$\mathcal{A} = [1, A], \quad \mathcal{B} = [1, B] \tag{31}$$

where A and B are defined in (23). We let

$$\mathcal{W}_{22} = \mathcal{A} \times \mathcal{J} \tag{32}$$

where $\mathcal{J} = [1, J]$ and $\frac{1}{n}\log J = R_{22} - \frac{1}{n}\log A$.

We define the mapping $g : \mathcal{B} \to \mathcal{J}$ to be partitioning $\mathcal{B}$ into J subsets with nearly equal size, where "nearly equal size" means

$$\|g^{-1}(j_1)\| \le 2\|g^{-1}(j_2)\|, \quad \forall\, j_1, j_2 \in \mathcal{J}. \tag{33}$$

The two encoders are defined as

$$\begin{aligned}
\text{Encoder 1 } f_1: &\quad W_1 \to \left\{x_{1,i}^n\right\}, \text{ mapping } w_1 \to i;\\
\text{Encoder 2 } f_{21}: &\quad (W_1, W_{21}) \to \{u_{ik}^n\},\\
&\quad \text{mapping } w_1 \to i \text{ and } w_{21} \to k;\\
P_{X_2^n|W_1,W_{21},W_{22}}: &\quad (W_1, W_{21}, W_{22}) \to \left\{x_{2,ikab}^n\right\},\\
&\quad \text{mapping } w_1 \to i, w_{21} \to k, \text{ and}\\
&\quad w_{22} = (a,j) \to (a,b) \text{ with } b \text{ chosen}\\
&\quad \text{randomly, uniformly from the set}\\
&\quad g^{-1}(j) \subset \mathcal{B}.
\end{aligned} \tag{34}$$

Step 3: Equivocation Computation: Based on the codebook given in Lemma 2 in step 1 and the encoding functions defined in (34) in step 2, we have the following joint probability distribution:

$$\begin{aligned}
&P_{W_1} P_{W_{21}} P_{W_{22}} 1\{X_1^n = f_1(W_1)\}\, 1\{U_{ik}^n = f_{21}(W_1, W_{21})\}\\
&\qquad \cdot P_{X_2^n|W_1,W_{21},W_{22}} P_{Y^n,Z^n|X_1^n,X_2^n}
\end{aligned} \tag{35}$$

where P_{W_1}, $P_{W_{21}}$, and $P_{W_{22}}$ are uniform distributions, and $1\{\cdot\}$ is the indicator function that is 1 if its argument is true, and is 0 otherwise. The encoding functions f_1 and f_{21} are deterministic one-to-one mapping, and $P_{X_2^n|W_1,W_{21},W_{22}}$ is a random mapping function (probability distribution) as defined in (34).

We now compute the equivocation rate of W_2 at receiver 1 in the following:

$$\begin{aligned}
H(W_{21}W_{22}|Y^n) &\ge H(W_{22}|Y^n, W_1, W_{21})\\
&= H(W_{22}, Y^n|W_1, W_{21}) - H(Y^n|W_1, W_{21})\\
&= H(W_{22}, Y^n, X_2^n|W_1, W_{21})\\
&\quad - H(X_2^n|W_1, W_{21}, W_{22}, Y^n) - H(Y^n|W_1, W_{21})\\
&= H(W_{22}, X_2^n|W_1, W_{21}) + H(Y^n|W_1, W_{21}, W_{22}, X_2^n)\\
&\quad - H(X_2^n|W_1, W_{21}, W_{22}, Y^n) - H(Y^n|W_1, W_{21})\\
&\ge H(X_2^n|W_1, W_{21}) + H(Y^n|X_1^n, X_2^n)\\
&\quad - H(X_2^n|W_1, W_{21}, W_{22}, Y^n) - H(Y^n|W_1, W_{21})
\end{aligned} \tag{36}$$

where (36) follows because conditioning does not increase entropy and Y^n is independent of (W_1, W_{21}, W_{22}) given (X_1^n, X_2^n).

We now compute each of the four terms in (36). To compute the first term, we use the following lemma given in [18].

Lemma 3: ([18]) Consider a discrete random variable X taking values in $\{x_1, \ldots, x_m\}$ and the probability mass function satisfying

$$\frac{P_X(x_i)}{P_X(x_j)} \le 2^{\delta}, \qquad \text{for } \delta \ge 1 \text{ and } \forall\, i, j \in [1, \ldots, m]. \tag{37}$$

Then[2]

$$H(X) \ge \log m - \delta. \tag{38}$$

[2]As before, the entropy is measured in bits.

For the first term in (36), we note that for each $(W_1 = i, W_{21} = k)$, X_2^n has $A \cdot B$ possible values. According to the encoding mapping function μ_{22} defined in (34), we have

$$\frac{P_{X_2^n}(x_2^n)}{P_{X_2^n}(\bar{x}_2^n)} \le 2, \quad \forall\, x_2^n,\ \bar{x}_2^n \in \{x_{2,ikab}^n\}. \tag{39}$$

By using (37) given in Lemma 3, we obtain

$$\frac{1}{n} H(X_2^n|W_1, W_{21}) \ge \frac{1}{n}\log A + \frac{1}{n}\log B - \frac{1}{n} = R_2' - \frac{1}{n}. \tag{40}$$

For the second term in (36), we have (41)–(43) shown at the top of the following page, where $O(\epsilon_1') \to 0$ as $\epsilon_1' \to 0$, $N(a, b|x_1^n, x_2^n)$ in (41) denotes the number of indices $i \in [1, n]$ for which $(x_{1,i}, x_{2,i}) = (a, b)$, and (42) follows from the definition that $(x_1^n, x_2^n) \in T_\epsilon^n(P_{X_1X_2})$.

To compute the third term in (36), we define $\rho(w_1, w_{21}, w_{22}, y^n)$ in (44) also at the top of the following page. Then

$$\begin{aligned}
&\Pr\{X_2^n \ne \rho(W_1, W_{21}, W_{22}, Y^n)\}\\
&= \sum_{w_1, w_{21}, a, b} \Big[p_{w_1, w_{21}, a, b}\\
&\qquad \Pr\Big\{ x_{2, w_1 w_{21} ab}^n \ne \rho(w_1, w_{21}, w_{22}, Y^n) \,\Big|\, w_1, w_{21}, a, b \Big\} \Big]\\
&= \lambda_2 < \eta.
\end{aligned} \tag{45}$$

Therefore, by Fano's inequality, we obtain

$$\begin{aligned}
&\frac{1}{n} H(X_2^n|W_1, W_{21}, W_{22}, Y^n)\\
&\quad \le \frac{1}{n}\left(1 + \lambda_2 \log\left(2^{n\left(R_1 + R_{21} + R_2'\right)}\right)\right)\\
&\quad < \epsilon_2
\end{aligned} \tag{46}$$

where ϵ_2 is small for sufficiently large n.

To compute the fourth term in (36), we define

$$\hat{y}^n = \begin{cases} y^n, & \text{if} \left(x_{1,w_1}^n, u_{w_1,w_{21}}^n, y^n\right) \in T_\epsilon^n(P_{UX_1Y}) \\ y_1^n, & \text{otherwise} \end{cases} \tag{47}$$

where y_1^n is an arbitrary sequence that is contained in $\mathcal{Y}^n$.

We then obtain (48) on the following page. The first term in (48) can be bounded as

$$\begin{aligned}
&\frac{1}{n} \sum_{w_1, w_{21}} \Big[\Pr\{W_1 = w_1, W_{21} = w_{21}\}\\
&\qquad \times H\left(\hat{Y}^n | W_1 = w_1, W_{21} = w_{21}\right) \Big]\\
&\le \frac{1}{n} \sum_{w_1, w_{21}} \Big[\Pr\{W_1 = w_1, W_{21} = w_{21}\}\\
&\qquad \times \log \left| T_\epsilon^n\left(P_{Y|UX_1} | x_{1,w_1}^n, u_{w_1 w_{21}}^n, \right) \right| \Big]\\
&\le \sum_{w_1, w_{21}} \Pr\{W_1 = w_1, W_{21} = w_{21}\} (H(Y|U, X_1) + \epsilon)\\
&\le H(Y|U, X_1) + \epsilon.
\end{aligned} \tag{49}$$

To bound the second term in (48), we use Fano's inequality and obtain (50) also on the following page, where ϵ_3 is small for

$$\begin{aligned}
\frac{1}{n}H\left(Y^n|X_1^n,X_2^n\right) &= \frac{1}{n}\sum_{x_1^n,x_2^n}\left[\Pr\left\{X_1^n=x_1^n,X_2^n=x_2^n\right\}H\left(Y^n|X_1^n=x_1^n,X_2^n=x_2^n\right)\right] \\
&\geq \frac{1}{n}\sum_{\left(x_1^n,x_2^n\right)\in T_\epsilon^n[P_{X_1X_2}]}\left[\Pr\left\{X_1^n=x_1^n,X_2^n=x_2^n\right\}H\left(Y^n|X_1^n=x_1^n,X_2^n=x_2^n\right)\right] \\
&= \frac{1}{n}\sum_{\left(x_1^n,x_2^n\right)\in T_\epsilon^n[P_{X_1X_2}]}\Bigg[\Pr\left\{X_1^n=x_1^n,X_2^n=x_2^n\right\}\times\sum_{(a,b)\in\mathcal{X}_1\times\mathcal{X}_2}\Big[N\left(a,b|x_1^n,x_2^n\right) \\
&\qquad\qquad \times\sum_{y\in\mathcal{Y}}-P_{Y|X_1,X_2}(y|a,b)\log P_{Y|X_1,X_2}(y|a,b)\Big]\Bigg] \qquad (41) \\
&\geq \sum_{\left(x_1^n,x_2^n\right)\in T_\epsilon^n[P_{X_1X_2}]}\Bigg[\Pr\left\{X_1^n=x_1^n,X_2^n=x_2^n\right\}\times\sum_{(a,b)\in\mathcal{X}_1\times\mathcal{X}_2}\Big[\left(P(X_1=a,X_2=b)-\epsilon_1'\right) \\
&\qquad\qquad \times\sum_{y\in\mathcal{Y}}-P_{Y|X_1,X_2}(y|a,b)\log P_{Y|X_1,X_2}(y|a,b)\Big]\Bigg] \qquad (42) \\
&= \sum_{\left(x_1^n,x_2^n\right)\in T_\epsilon^n[P_{X_1X_2}]}\Big[\Pr\left\{X_1^n=x_1^n,X_2^n=x_2^n\right\}\left(H(Y|X_1,X_2)-O\left(\epsilon_1'\right)\right)\Big] \\
&\geq \left(1-\epsilon_2'\right)H(Y|X_1,X_2)-O\left(\epsilon_1'\right) \\
&\geq H(Y|X_1,X_2)-\epsilon_1 \qquad (43)
\end{aligned}$$

$$\rho\left(w_1,w_{21},w_{22},y^n\right)=\begin{cases}x_{2,w_1w_{21}ab}^n, & \text{if there is a unique } b \text{ such that} \left(x_{1,w_1}^n,u_{w_1,w_{21}}^n x_{2,w_1w_{21}ab}^n,y^n\right)\in T_\epsilon^n(P_{UX_1X_2Y}) \\ x_{2,1111}^n, & \text{otherwise.}\end{cases} \qquad (44)$$

$$\begin{aligned}
&\frac{1}{n}H\left(Y^n|W_1,W_{21}\right) \\
&\quad=\frac{1}{n}\sum_{w_1,w_{21}}\Big[\Pr\{W_1=w_1,W_{21}=w_{21}\}H\left(Y^n|W_1=w_1,W_{21}=w_{21}\right)\Big] \\
&\quad\leq\frac{1}{n}\sum_{w_1,w_{21}}\Big[\Pr\{W_1=w_1,W_{21}=w_{21}\}H\left(Y^n,\hat{Y}^n|W_1=w_1,W_{21}=w_{21}\right)\Big] \\
&\quad=\frac{1}{n}\sum_{w_1,w_{21}}\Pr\{W_1=w_1,W_{21}=w_{21}\}\Big(H\left(\hat{Y}^n|W_1=w_1,W_{21}=w_{21}\right)+H\left(Y^n|W_1=w_1,W_{21}=w_{21},\hat{Y}^n\right)\Big). \qquad (48)
\end{aligned}$$

$$\begin{aligned}
&\frac{1}{n}\sum_{w_1,w_{21}}\Big[\Pr\{W_1=w_1,W_{21}=w_{21}\}H\left(Y^n|W_1=w_1,W_{21}=w_{21},\hat{Y}^n\right)\Big] \\
&\quad\leq\frac{1}{n}\sum_{w_1,w_{21}}\Big[\Pr\{W_1=w_1,W_{21}=w_{21}\}\Big(1+\Pr\Big\{Y^n\neq\hat{Y}^n|W_1=w_1,W_{21}=w_{21}\Big\}\log|\mathcal{Y}|^n\Big)\Big] \\
&\quad=\frac{1}{n}+\sum_{w_1,w_{21}}\Pr\{W_1=w_1,W_{21}=w_{21}\}\Pr\Big\{\left(x_{1,w_1}^n,u_{w_1w_{21}}^n,y^n\right)\notin T_\epsilon^n(P_{UX_1Y})\Big\}\log|\mathcal{Y}| \\
&\quad\leq\epsilon_3 \qquad (50)
\end{aligned}$$

sufficiently large n. Hence, the fourth term in (36) is bounded as

$$\frac{1}{n}H\left(Y^n|W_1,W_{21}\right)\leq H(Y|U,X_1)+\epsilon_3. \qquad (51)$$

Substituting (40), (43), (46), and (51) into (36), we obtain

$$\begin{aligned}
\frac{1}{n}H\left(W_2|Y^n\right) &\geq R_2'+H(Y|X_1,X_2)-H(Y|X_1,U)-\epsilon_4 \\
&= R_2'-I(X_2;Y|U,X_1)-\epsilon_4 \qquad (52)
\end{aligned}$$

where ϵ_4 is small for sufficiently large n. By the definition of R_e, we conclude

$$R_e\leq R_2'-I(X_2;Y|U,X_1). \qquad (53)$$

Therefore, the region $\mathfrak{R}$ in (4) follows by using (19), (20), and (53).

In steps 2 and 3, we assume that

$$R_{22}>\frac{1}{n}\log A.$$

For the case in which

$$R_{22} \leq \frac{1}{n}\log A$$

we change the encoder $P_{X_2^n|W_1,W_{21},W_{22}}$ in (34) to be the following:

$$\begin{aligned}&(W_1, W_{21}, W_{22}) \to \left\{x_{2,ikab}^n\right\}, \text{ that maps}\\ &(w_1, w_{21}, w_{22}) \to x_{2,w_1 w_{21} w_{22} b}^n, \text{ where } b \text{ is chosen}\\ &\text{randomly, uniformly from the set } [1, 2^{nI(X_2;Y|U,X_1)}].\end{aligned} \tag{54}$$

In this case, note that the number of messages is less than the number of rows in the codebook. The encoding strategy is to map each message to a different row. It is expected that in this case receiver 1 is not able to decode any information about W_2, and hence perfect secrecy is achieved. In fact, the first term of the equivocation rate in (36) becomes

$$\frac{1}{n}H\left(X_2^n|W_1, W_{21}\right) = R_{22} + I(X_2; Y|U, X_1) \tag{55}$$

because for each (W_1, W_{21}), X_2^n has $2^{n(R_{22}+I(X_2;Y|U,X_1))}$ possible equally likely values. All other terms in (36) remain the same as before. We hence have

$$\begin{aligned}&\frac{1}{n}H\left(W_{21}W_{22}|Y^n\right)\\ &\quad\geq R_{22} + I(X_2; Y|U, X_1)\\ &\qquad + H(Y|X_1, X_2) - H(Y|X_1, U) - \epsilon_4\\ &\quad= R_{22} - \epsilon_4.\end{aligned} \tag{56}$$

Thus, for sufficiently large n

$$R_e \leq R_{22} \tag{57}$$

which concludes the proof.

Appendix B
Proof of the Converse Part of Theorem 1

Consider a $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code with an average block error probability $P_e^{(n)}$. The probability distribution on $\mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{X}_1^n \times \mathcal{X}_2^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ is given by

$$\begin{aligned}&P_{W_1,W_2,X_1^n,X_2^n,Y^n,Z^n}\\ &= P_{W_1}P_{W_2}1\left\{X_1^n = f_1(W_1)\right\}P_{X_2^n|W_1,W_2}\prod_{i=1}^n P_{Y_i,Z_i|X_{1,i},X_{2,i}}.\end{aligned} \tag{58}$$

By Fano's inequality, we have

$$H\left(W_1|Y^n\right) \leq nR_1P_e^{(n)} + 1 = n\delta_{1,n} \tag{59}$$

$$H\left(W_1, W_2|Z^n\right) \leq n(R_1 + R_2)P_e^{(n)} + 1 = n\delta_{2,n} \tag{60}$$

where $\delta_{1,n}$ and $\delta_{2,n} \to 0$ if $P_e^{(n)} \to 0$.

The following lemma is useful in the proof.

Lemma 4: [18, Lemma 7] For any $(T, Y_1, \ldots, Y_n, Z_1, \ldots, Z_n)$

$$\sum_{i=1}^n I\left(Z_i; Y^{i-1}|Z_{i+1}^n, T\right) = \sum_{i=1}^n I\left(Y_i; Z_{i+1}^n|Y^{i-1}, T\right).$$

We define the following auxiliary random variables:

$$U_i = \left(W_1, X_1^n, Y^{i-1}, Z_{i+1}^n\right) \quad \text{and} \quad V_i = (W_2, U_i) \tag{61}$$

which satisfy the following Markov chain conditions:

$$\begin{aligned}X_{1,i} \leftrightarrow U_i \leftrightarrow V_i \leftrightarrow X_{2,i}\\ (U_i, V_i) \leftrightarrow (X_{1,i}, X_{2,i}) \leftrightarrow (Y_i, Z_i)\end{aligned} \tag{62}$$

for $i = 1, \ldots, n$.

We first bound R_1

$$\begin{aligned}nR_1 &\leq I(W_1; Y^n) + n\delta_n = \sum_{i=1}^n I(W_1; Y_i|Y^{i-1}) + n\delta_n\\ &\leq \sum_{i=1}^n I(W_1, X_1^n, Y^{i-1}, Z_{i+1}^n; Y_i) + n\delta_n\\ &= \sum_{i=1}^n I(U_i, X_{1,i}; Y_i) + n\delta_n\end{aligned} \tag{63}$$

where $\delta_n = \delta_{1,n} + \delta_{2,n}$. Similarly, we can obtain the following bound on R_1:

$$nR_1 \leq I(W_1; Z^n) + n\delta_n \leq \sum_{i=1}^n I(U_i, X_{1,i}; Z_i) + n\delta_n. \tag{64}$$

We then bound R_2

$$\begin{aligned}nR_2 &\leq I(W_2; Z^n) + n\delta_n\\ &\leq I(W_2; Z^n, W_1, X_1^n) + n\delta_n\\ &= I(W_2; Z^n|W_1, X_1^n) + n\delta_n \qquad (65)\\ &\leq \sum_{i=1}^n H(Z_i|X_{1,i}) - H(Z_i|W_1, W_2, X_1^n, Z_{i+1}^n) + n\delta_n\\ &\leq \sum_{i=1}^n I(W_2, W_1, X_1^n, Y^{i-1}, Z_{i+1}^n; Z_i|X_{1,i}) + n\delta_n\\ &= \sum_{i=1}^n I(U_i, V_i; Z_i|X_{1,i}) + n\delta_n \qquad (66)\end{aligned}$$

where (65) follows since W_2 and (W_1, X_1^n) are independent.

We can next bound the sum-rate in two different forms

$$\begin{aligned}nR_1 + nR_2 &\leq I\left(W_1, W_2; Z^n\right) + n\delta_n\\ &= \sum_{i=1}^n I\left(W_1, W_2; Z_i|Z_{i+1}^n\right) + n\delta_n\\ &\leq \sum_{i=1}^n I\left(W_1, W_2, X_1^n, Y^{i-1}, Z_{i+1}^n; Z_i\right) + n\delta_n\\ &= \sum_{i=1}^n I(U_i, V_i, X_{1,i}; Z_i) + n\delta_n\end{aligned} \tag{67}$$

and get (68)–(70) at the top of the following page, where (69) follows from Lemma 4 applied to $T = (W_1, X_1^n)$.

We now bound the equivocation rate R_e as shown in (71)–(73), also at the top of the following page, where (71) follows from Lemma 4 applied to $T = (W_1, W_2)$, (72) follows from the chain rule and Lemma 4 applied to $T = (W_1, W_2)$,

$$
\begin{aligned}
&nR_1 + nR_2 \qquad (68)\\
&\quad \le I\left(W_1, X_1^n; Y^n\right) + I\left(W_2; Z^n | W_1, X_1^n\right) + n\delta_n\\
&\quad = \sum_{i=1}^{n}\Big[I\left(W_1, X_1^n; Y_i | Y^{i-1}\right) + I\left(W_2; Z_i | W_1, X_1^n, Z_{i+1}^n\right)\Big] + n\delta_n\\
&\quad \le \sum_{i=1}^{n}\Big[I\left(W_1, X_1^n, Z_{i+1}^n; Y_i | Y^{i-1}\right) - I\left(Z_{i+1}^n; Y_i | W_1, X_1^n, Y^{i-1}\right) + I\left(Y^{i-1}, W_2; Z_i | W_1, X_1^n, Z_{i+1}^n\right)\Big] + n\delta_n\\
&\quad \le \sum_{i=1}^{n}\Big[I\left(W_1, X_1^n, Z_{i+1}^n; Y_i | Y^{i-1}\right) - I\left(Z_{i+1}^n; Y_i | W_1, X_1^n, Y^{i-1}\right)\\
&\qquad\quad + I\left(Y^{i-1}; Z_i | W_1, X_1^n, Z_{i+1}^n\right) + I\left(W_2; Z_i | W_1, X_1^n, Y^{i-1}, Z_{i+1}^n\right)\Big] + n\delta_n\\
&\quad = \sum_{i=1}^{n}\Big[I\left(W_1, X_1^n, Z_{i+1}^n; Y_i | Y^{i-1}\right) + I\left(W_2; Z_i | W_1, X_1^n, Y^{i-1}, Z_{i+1}^n\right)\Big] + n\delta_n \qquad (69)\\
&\quad \le \sum_{i=1}^{n}\Big[I(U_i, X_{1,i}; Y_i) + I(V_i; Z_i | U_i, X_{1,i})\Big] + n\delta_n \qquad (70)
\end{aligned}
$$

$$
\begin{aligned}
nR_e &\le H\left(W_2 | Y^n\right)\\
&= H\left(W_2 | Y^n W_1\right) + I\left(W_2; W_1 | Y^n\right)\\
&= H(W_2 | W_1) - I\left(W_2; Y^n | W_1\right) + I\left(W_2; W_1 | Y^n\right)\\
&= I\left(W_2; Z^n | W_1\right) - I\left(W_2; Y^n | W_1\right) + H\left(W_2 | Z^n, W_1\right) + I\left(W_1; W_2 | Y^n\right)\\
&\le I\left(W_2; Z^n | W_1\right) - I\left(W_2; Y^n | W_1\right) + n\delta_n\\
&= \sum_{i=1}^{n}\Big[I\left(W_2; Z_i | W_1, Z_{i+1}^n\right) - I\left(W_2; Y_i | W_1, Y^{i-1}\right)\Big] + n\delta_n\\
&= \sum_{i=1}^{n}\Big[I\left(W_2, Y^{i-1}; Z_i | W_1, Z_{i+1}^n\right) - I\left(Y^{i-1}; Z_i | W_1, W_2, Z_{i+1}^n\right)\\
&\qquad\quad - I\left(W_2, Z_{i+1}^n; Y_i | W_1, Y^{i-1}\right) + I\left(Z_{i+1}^n; Y_i | W_1, W_2, Y^{i-1}\right)\Big] + n\delta_n\\
&= \sum_{i=1}^{n}\Big[I\left(W_2, Y^{i-1}; Z_i | W_1, Z_{i+1}^n\right) - I\left(W_2, Z_{i+1}^n; Y_i | W_1, Y^{i-1}\right)\Big] + n\delta_n \qquad (71)\\
&= \sum_{i=1}^{n}\Big[I\left(W_2; Z_i | W_1, Y^{i-1}, Z_{i+1}^n\right) - I\left(W_2; Y_i | W_1, Y^{i-1}, Z_{i+1}^n\right)\Big] + n\delta_n \qquad (72)\\
&= \sum_{i=1}^{n}\Big[I\left(V_i; Z_i | U_i, X_{1,i}\right) - I\left(V_i; Y_i | U_i, X_{1,i}\right)\Big] + n\delta_n \qquad (73)
\end{aligned}
$$

and (73) follows from (61) and from the fact that X_1^n is a deterministic function of W_1.

Using (64) and (73), we finally bound the following sum-rate:

$$
\begin{aligned}
&nR_1 + nR_e\\
&\quad \le \sum_{i=1}^{n}\Big[I(U_i, X_{1,i}; Z_i) + I\left(V_i; Z_i | U_i, X_{1,i}\right)\\
&\qquad\quad - I(V_i; Y_i | U_i, X_{1,i})\Big] + n\delta_n\\
&\quad = \sum_{i=1}^{n}\Big[I(U_i, V_i, X_{1,i}; Z_i) - I(V_i; Y_i | U_i, X_{1,i})\Big] + n\delta_n. \qquad (74)
\end{aligned}
$$

Equations (63)–(74) conclude the proof of the converse part of Theorem 1 as they establish the existence of random variables (U, V, X_1, X_2) such that $(X_1, U) \leftrightarrow V \leftrightarrow X_2$ and $(U, V) \leftrightarrow (X_1, X_2) \leftrightarrow (Y, Z)$ are Markov chains and the inequalities in (6) are satisfied.

Appendix C
Proof of Corollary 2

We apply the bounds in (5) and obtain

$$
\begin{aligned}
R_2 &\le I(U, V; Z | X_1) \le I(X_2; Z | X_1)\\
R_1 + R_2 &\le (V, U, X_1; Z) \le I(X_2, X_1; Z)\\
R_1 + R_2 &\le I(U, X_1; Y) + I(V; Z | U, X_1)
\end{aligned}
$$

$$
\begin{aligned}
nR_e &\le I\left(W_2;Z^n|W_1\right)-I\left(W_2;Y^n|W_1\right)\\
&\le I\left(W_2;Z^n|W_1,X_1^n\right)-I\left(W_2;Y^n|W_1,X_1^n\right)\\
&= I\left(W_2,X_2^n;Z^n|W_1,X_1^n\right)-I\left(X_2^n;Z^n|W_1,W_2,X_1^n\right)-I\left(W_2,X_2^n;Y^n|W_1,X_1^n\right)+I\left(X_2^n;Y^n|W_1,W_2,X_1^n\right)\\
&\le I\left(X_2^n;Z^n|W_1,X_1^n\right)-I\left(X_2^n;Y^n|W_1,X_1^n\right) \qquad (80)\\
&= \sum_{i=1}^{n}\Big[I\left(X_2^n;Z_i|W_1,X_1^n,Z^{i-1}\right)-I\left(X_2^n;Y_i|W_1,X_1^n,Y^{i-1}\right)\Big]\\
&\le \sum_{i=1}^{n}\Big[H\left(Z_i|W_1,X_1^i,Z^{i-1}\right)-H\left(Z_i|W_1,X_1^i,Z^{i-1},X_{2,i}\right)-H\left(Y_i|W_1,X_1^n,Y^{i-1}\right)+H\left(Y_i|W_1,X_1^n,X_2^n,Y^{i-1}\right)\Big]\\
&\le \sum_{i=1}^{n}\Big[I(X_{2,i};Z_i|U_i)-H\left(Y_i|W_1,X_1^n,Y^{i-1},Z^{i-1}\right)+H\left(Y_i|W_1,X_1^n,X_{2,i},Z^{i-1}\right)\Big] \qquad (81)\\
&\le \sum_{i=1}^{n}\Big[I(X_{2,i};Z_i|U_i)-H\left(Y_i|W_1,X_1^n,Z^{i-1}\right)+H\left(Y_i|W_1,X_1^n,X_{2,i},Z^{i-1}\right)\Big] \qquad (82)\\
&= \sum_{i=1}^{n}\Big[I(X_{2,i};Z_i|X_{1,i},U_i)-I(X_{2,i};Y_i|X_{1,i},U_i)\Big] \qquad (83)
\end{aligned}
$$

$$
\begin{aligned}
&\le I(U,X_1;Y)+I(V;Y|U,X_1)\\
&= I(V,U,X_1;Y)\le I(X_2,X_1;Y) \qquad (75)
\end{aligned}
$$

where (75) follows from the degradedness condition (8).

To bound R_e, we apply the last bound in (5) and obtain

$$R_e \le I(V;Z|U,X_1)-I(V;Y|U,X_1)\le 0 \qquad (76)$$

where the last inequality follows from the degradedness condition (8), which concludes the proof.

Appendix D
Proof of Corollary 3

We follow the initial steps in Appendix B except that we now define $U_i=\left(W_1,Z^{i-1},X_1^n\right)$.

$$
\begin{aligned}
nR_1 &\le \sum_{i=1}^{n} I\left(W_1;Y_i|Y^{i-1}\right)\\
&\le \sum_{i=1}^{n} H(Y_i)-H\left(Y_i|W_1,Y^{i-1}\right)\\
&\le \sum_{i=1}^{n} H(Y_i)-H\left(Y_i|W_1,Y^{i-1},Z^{i-1},X_1^n\right)\\
&\le \sum_{i=1}^{n} H(Y_i)-H\left(Y_i|W_1,Z^{i-1},X_1^n\right)\\
&= \sum_{i=1}^{n} I(U_i,X_{i,1};Y_i). \qquad (77)
\end{aligned}
$$

Similarly

$$nR_1 \le \sum_{i=1}^{n} I(U_i,X_{i,1};Z_i). \qquad (78)$$

We now bound R_2

$$
\begin{aligned}
nR_2 &\le I\left(W_2;Z^n|W_1,X_1^n\right)\\
&= \sum_{i=1}^{n} I\left(W_2;Z_i|W_1,X_1^n,Z^{i-1}\right)\\
&\le \sum_{i=1}^{n} H\left(Z_i|W_1,X_1^n,Z^{i-1}\right)\\
&\quad - H\left(Z_i|W_1,W_2,X_1^n,Z^{i-1},X_{2,i}\right)\\
&\le \sum_{i=1}^{n} H(Z_i|U_i,X_{1,i})-H(Z_i|U_i,X_{1,i},X_{2,i})\\
&= \sum_{i=1}^{n} I(X_{2,i};Z_i|U_i,X_{1,i}). \qquad (79)
\end{aligned}
$$

We finally bound $R_e$as shown in (80)–(83) at the top of the page, where (80) follows because $I\left(X_2^n;Y^n|W_1,W_2,X_1^n\right)\le I\left(X_2^n;Z^n|W_1,W_2,X_1^n\right)$ due to the degradedness condition (10), (81) follows because conditioning reduces entropy and because $\left(Y^{i-1},Z^{i-1}\right)\leftrightarrow\left(W_1,X_{1,i},X_{2,i}\right)\leftrightarrow Y_i$, and (82) follows because of the degradedness condition (10).

Appendix E
Proof of the Converse Part of Theorem 2

Similarly to the steps in Appendix C, we apply the degradedness condition in (8) to the bounds (66), (67), and (70) in Appendix B, and obtain the following bounds:

$$nR_2 \le \sum_{i=1}^{n} I(X_{2,i};Z_i|X_{1,i})+n\delta_n \qquad (84)$$

$$nR_1+nR_2 \le \sum_{i=1}^{n} I(X_{1,i},X_{2,i};Z_i)+n\delta_n \qquad (85)$$

$$nR_1+nR_2 \le \sum_{i=1}^{n} I(X_{1,i},X_{2,i};Y_i)+n\delta_n. \qquad (86)$$

In the following, we further derive the bounds (84)–(86) for the Gaussian channel. For simplicity of exposition, we ignore the term $n\delta_n$. We start with (85), and obtain

$$\begin{aligned}
R_1+R_2 &\le \frac{1}{n}\sum_{i=1}^{n} h(Z_i) - \frac{1}{2}\log 2\pi e \\
&\le \frac{1}{2n}\sum_{i=1}^{n}\log\left(\mathrm{E}(bX_{1,i}+X_{2,i})^2+1\right) && (87)\\
&\le \frac{1}{2}\log\left(\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}(bX_{1,i}+X_{2,i})^2+1\right) && (88)\\
&= \frac{1}{2}\log\left(\frac{1}{n}\sum_{i=1}^{n}\Big(b^2\mathrm{E}X_{1,i}^2+\mathrm{E}X_{2,i}^2+2b\mathrm{E}(X_{1,i}X_{2,i})\Big)+1\right)\\
&\le \frac{1}{2}\log\left(b^2P_1+P_2+\frac{2b}{n}\sum_{i=1}^{n}\mathrm{E}(X_{1,i}X_{2,i})+1\right) && (89)
\end{aligned}$$

where (87) follows from the fact that a Gaussian distribution maximizes the entropy for given second moments and (88) follows from the concavity of the $\log(\cdot)$ function and Jensen's inequality.

We note that

$$\begin{aligned}
&\left|\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}(X_{1,i}X_{2,i})\right|\\
&\quad\le \frac{1}{n}\sum_{i=1}^{n}\sqrt{\mathrm{E}[X_{1,i}^2]\mathrm{E}\left[X_{2,i}^2\right]} && (90)\\
&\quad\le \sqrt{\left(\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\left[X_{1,i}^2\right]\right)\cdot\left(\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\left[X_{2,i}^2\right]\right)}\\
&\quad\le \sqrt{P_1P_2} && (91)
\end{aligned}$$

where (90) and (91) follow from the Cauchy–Schwarz inequality.

Hence, there exits $-1\le\rho\le 1$ such that

$$\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\left[X_{1,i}X_{2,i}\right]=\rho\sqrt{P_1P_2}. \tag{92}$$

Applying (92) to (89), we obtain

$$R_1+R_2\le\frac{1}{2}\log\left(b^2P_1+P_2+2b\rho\sqrt{P_1P_2}+1\right). \tag{93}$$

Similarly to the above, we obtain

$$R_1+R_2\le\frac{1}{2}\log\left(P_1+a^2P_2+2a\rho\sqrt{P_1P_2}+1\right). \tag{94}$$

To bound R_2, we first derive the following useful property:

$$\begin{aligned}
&|\rho\sqrt{P_1P_2}|\\
&\quad=\left|\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\left[X_{1,i}X_{2,i}\right]\right|\\
&\quad=\left|\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\left[X_{1,i}\mathrm{E}(X_{2,i}|X_{1,i})\right]\right|\\
&\quad\le\frac{1}{n}\sum_{i=1}^{n}\sqrt{\mathrm{E}\left[X_{1,i}^2\right]\mathrm{E}\left[\mathrm{E}^2\left[X_{2,i}|X_{1,i}\right]\right]}\\
&\quad\le\sqrt{\left(\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\left[X_{1,i}^2\right]\right)\cdot\left(\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\left[\mathrm{E}^2(X_{2,i}|X_{1,i})\right]\right)}\\
&\quad\le\sqrt{P_1A}, && (95)
\end{aligned}$$

where $A=\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\left[\mathrm{E}^2(X_{2,i}|X_{1,i})\right]$. This implies

$$A\ge\rho^2P_2. \tag{96}$$

We now further derive (84) and obtain

$$\begin{aligned}
R_2 &\le \frac{1}{n}\sum_{i=1}^{n}\Big[h(Z_{1,i}|X_{1,i})-h(Z_{1,i}|X_{1,i},X_{2,i})\Big]\\
&\le \frac{1}{2n}\sum_{i=1}^{n}\mathrm{E}\log 2\pi e\mathsf{Var}(Z_i|X_{1,i})-\frac{1}{2}\log 2\pi e\\
&= \frac{1}{2n}\sum_{i=1}^{n}\log 2\pi e\mathrm{E}\big[\mathsf{Var}(X_{2,i}|X_{1,i})+1\big]-\frac{1}{2}\log 2\pi e\\
&\le \frac{1}{2}\log\left(\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\big[\mathsf{Var}(X_{2,i}|X_{1,i})\big]+1\right)\\
&= \frac{1}{2}\log\left(\frac{1}{n}\sum_{i=1}^{n}\Big[\mathrm{E}\left(X_{2,i}^2\right)-\mathrm{E}\left[\mathrm{E}^2(X_{2,i}|X_{1,i})\right]\Big]+1\right)\\
&\le \frac{1}{2}\log\left(P_2-A+1\right)\\
&\le \frac{1}{2}\log\left((1-\rho^2)P_2+1\right) && (97)
\end{aligned}$$

where (97) follows from (96).

Appendix F
Proof of the Converse for Theorem 3

We further derive the bounds (77), (78), (79), and (83) for the Gaussian channel. We start with (78) and obtain

$$\begin{aligned}
R_1 &\le \frac{1}{n}\sum_{i=1}^{n} I(U_i,X_{1,i};Z_i)\\
&= \frac{1}{n}\sum_{i=1}^{n}\Big[h(Z_i)-h(Z_i|U_i,X_{1,i})\Big]\\
&\le \frac{1}{2}\log 2\pi e\left(b^2P_1+P_2+\frac{2b}{n}\sum_{i=1}^{n}\mathrm{E}(X_{1,i}X_{2,i})+1\right)\\
&\quad-\frac{1}{n}\sum_{i=1}^{n}h(Z_i|U_i,X_{1,i}) && (98)
\end{aligned}$$

where (98) follows by applying the same steps as in (89) in Appendix E. For the term $\frac{1}{n}\sum_{i=1}^{n}h(Z_i|U_i,X_{1,i})$, we have

$$\begin{aligned}
\frac{1}{n}\sum_{i=1}^{n}h(Z_i|U_i,X_{1,i}) &\ge \frac{1}{n}\sum_{i=1}^{n}h(Z_i|U_i,X_{1,i},X_{2,i})\\
&= \frac{1}{2}\log 2\pi e && (99)
\end{aligned}$$

and

$$\begin{aligned}\frac{1}{n}\sum_{i=1}^{n} h(Z_i|U_i, X_{1,i}) &\le \frac{1}{n}\sum_{i=1}^{n} h(Z_i|X_{1,i}) \\ &\le \frac{1}{n}\sum_{i=1}^{n} h(X_{2,i}+N_{2,i}|X_{1,i}) \\ &\le \frac{1}{n}\sum_{i=1}^{n} \frac{1}{2}\log 2\pi e\left(\mathrm{E}\left[X_{2,i}^2\right]+1\right) \\ &\le \frac{1}{2}\log 2\pi e(P_2+1). \end{aligned} \tag{100}$$

Equations (99) and (100) imply that there exists a $|\rho'| \le 1$ such that

$$\frac{1}{n}\sum_{i=1}^{n} h(Z_i|U_i, X_{1,i}) = \frac{1}{2}\log 2\pi e\left((1-\rho'^2)P_2+1\right). \tag{101}$$

We can also obtain that

$$\begin{aligned}\frac{1}{n}\sum_{i=1}^{n} h(Z_i|U_i, X_{1,i}) &\le \frac{1}{n}\sum_{i=1}^{n} h(Z_i|X_{1,i}) \\ &\le \frac{1}{2}\log 2\pi e(P_2 - A + 1) \end{aligned} \tag{102}$$

where $A = \frac{1}{n}\sum_{i=1}^{n} \mathrm{E}\left[\mathrm{E}^2(X_{2,i}|X_{1,i})\right]$ and (102) follows from (97). Equations (101) and (102) imply that

$$A \le \rho'^2 P_2. \tag{103}$$

From (95) in Appendix E, we obtain

$$\left|\frac{1}{n}\sum_{i=1}^{n} \mathrm{E}[X_{1,i}X_{2,i}]\right| \le \sqrt{P_1 A} \le \sqrt{\rho'^2 P_1 P_2}. \tag{104}$$

Hence, if we choose a correct sign for ρ', there exists $0 \le \beta \le 1$ such that

$$\frac{1}{n}\sum_{i=1}^{n} \mathrm{E}[X_{1,i}X_{2,i}] = \rho'\sqrt{\beta P_1 P_2}. \tag{105}$$

Now applying (105) and (100) to (98), we obtain

$$R_1 \le \frac{1}{2}\log\frac{b^2 P_1 + P_2 + 2b\rho'\sqrt{\beta P_1 P_2}+1}{(1-\rho'^2)P_2+1}. \tag{106}$$

We next derive (79) to bound R_2

$$\begin{aligned} R_2 &\le \frac{1}{n}\sum_{i=1}^{n} I(X_{2,i}; Z_i|U_i, X_{1,i}) \\ &= \frac{1}{n}\sum_{i=1}^{n}\Big[H(Z_i|U_i, X_{1,i}) - H(Z_i|U_i, X_{1,i}, X_{2,i})\Big] \\ &\le \frac{1}{2}\log\left((1-\rho'^2)P_2+1\right) \end{aligned} \tag{107}$$

where (107) follows from (101).

We further derive (77) and obtain another bound on R_1

$$\begin{aligned} nR_1 &\le \sum_{i=1}^{n} I(U_i, X_{i,1}; Y_i) \\ &\le \sum_{i=1}^{n}\Big[h(Y_i) - h(Y_i|U_i, X_{1,i})\Big]. \end{aligned} \tag{108}$$

Now

$$\begin{aligned}&\sum_{i=1}^{n} h(Y_i) \\ &\quad\le \frac{1}{2}\log\left(P_1 + a^2 P_2 + \frac{2a}{n}\sum_{i=1}^{n}\mathrm{E}(X_{1,i}X_{2,i}) + 1\right) \quad (109) \\ &\quad= \frac{1}{2}\log\left(P_1 + a^2 P_2 + 2a\rho'\sqrt{\beta P_1 P_2} + 1\right) \quad (110)\end{aligned}$$

where (109) follows from the steps similarly to those in (89) in Appendix E, and (110) follows from (105).

We note that the capacity-equivocation region does not change if we consider the following output at receiver 1:

$$Y = X_1 + aX_2 + aN_2 + N' \tag{111}$$

where N' is a zero-mean Gaussian random variable with the variance $1-a^2$, and is independent of N_1 and N_2. We now use the entropy power inequality, and obtain

$$\begin{aligned}&2^{2h(Y_i|U_i=u_i, X_{1,i}=x_{1,i})} \\ &\quad= 2^{2h\left(aZ_i+N_i'|U_i=u_i, X_{1,i}=x_{1,i}\right)} \\ &\quad\ge 2^{2h(aZ_i|U_i=u_i, X_{1,i}=x_{1,i})} + 2^{2h\left(N_i'|U_i=u_i, X_{1,i}=x_{1,i}\right)} \\ &\quad= 2^{2h(Z_i|U_i=u_i, X_{1,i}=x_{1,i})+\log a^2} + 2\pi e(1-a^2).\end{aligned}$$

Hence

$$\begin{aligned}&h(Y_i|U_i=u_i, X_{1,i}=x_{1,i}) \\ &\quad\ge \frac{1}{2}\log\left(2^{2h(Z_i|U_i=u_i, X_{1,i}=x_{1,i})+\log a^2} + 2\pi e(1-a^2)\right).\end{aligned}$$

Thus

$$\begin{aligned}&\mathrm{E}\left[h(Y_i|U_i=u_i, X_{1,i}=x_{1,i})\right] \\ &\quad\ge \frac{1}{2}\mathrm{E}\left[\log\left(2^{2h(Z_i|U_i=u_i, X_{1,i}=x_{1,i})+\log a^2} + 2\pi e(1-a^2)\right)\right] \\ &\quad\ge \frac{1}{2}\log\left(2^{2\mathrm{E}[h(Z_i|U_i=u_i, X_{1,i}=x_{1,i})]+\log a^2} + 2\pi e(1-a^2)\right) \quad (112) \\ &\quad\ge \frac{1}{2}\log\left(2^{2h(Z_i|U_i, X_{1,i})+\log a^2} + 2\pi e(1-a^2)\right) \quad (113)\end{aligned}$$

where (112) follows because $\log(2^x + c)$ is a convex function of x. Therefore

$$\begin{aligned}&\frac{1}{n}\sum_{i=1}^{n} h(Y_i|U_i, X_{1,i}) \\ &\quad\ge \frac{1}{2n}\sum_{i=1}^{n}\log\left(2^{2h(Z_i|U_i, X_{1,i})+\log a^2} + 2\pi e(1-a^2)\right) \\ &\quad\ge \frac{1}{2}\log\left(2^{2\frac{1}{n}\sum_{i=1}^{n} h(Z_i|U_i, X_{1,i})+\log a^2} + 2\pi e(1-a^2)\right) \quad (114) \\ &\quad= \frac{1}{2}\log 2\pi e\left(a^2(1-\rho'^2)P_2+1\right) \quad (115)\end{aligned}$$

where (114) also follows because $\log(2^x + c)$ is a convex function of x, and (115) follows from (101).

Substituting (115) and (110) into (108), we obtain

$$nR_1 \le \frac{1}{2}\log\frac{P_1 + a^2 P_2 + 2a\rho'\sqrt{\beta P_1 P_2}+1}{a^2(1-\rho'^2)P_2+1}. \tag{116}$$

We finally apply (83) to bound R_e

$$\begin{aligned} R_e &\le \frac{1}{n}\sum_{i=1}^{n}\Big[I(X_{2,i};Z_i|X_{1,i},U_i) - I(X_{2,i};Y_i|X_{1,i},U_i)\Big] \\ &= \frac{1}{n}\sum_{i=1}^{n}\Big[h(Z_i|X_{1,i},U_i) - h(Y_i|X_{1,i},U_i)\Big] \\ &\le \frac{1}{2}\log\left((1-\rho'^2)P_2+1\right) - \frac{1}{2}\log\left(a^2(1-\rho'^2)P_2+1\right) \end{aligned} \tag{117}$$

where (117) follows from (101) and (115).

REFERENCES

[1] A. B. Carleial, "Interference channels," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 1, pp. 60–70, Jan. 1978.

[2] T. S. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 1, pp. 49–60, Jan. 1981.

[3] I. Sason, "On achievable rate regions for the Gaussian interference channel," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1345–1356, Jun. 2004.

[4] H. F. Chong, M. Motani, H. K. Garg, and H. El Gamal, "On a simplification of the Han–Kobayashi rate region for the interference channel," *IEEE Trans. Inf. Theory*, submitted for publication.

[5] G. Kramer, "Review of rate regions for interference channels," in *Proc. Int. Zurich Seminar on Communications*, Zurich, Switzerland, Feb. 2006, pp. 162–165.

[6] R. Etkin, D. N. C. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *IEEE Trans. Inf. Theory*, submitted for publication.

[7] E. Telatar and D. Tse, "Bounds on the capacity region of a class of interference channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, Jun. 2007, pp. 2871–2874.

[8] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[9] N. Devroye, P. Mitran, and V. Tarokh, "Achievable rates in cognitive channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 1813–1827, May 2006.

[10] N. Devroye, P. Mitran, and V. Tarokh, "Limits on communications in a cognitive radio channel," *IEEE Commun. Mag.*, vol. 44, no. 6, pp. 44–49, Jun. 2006.

[11] W. Wu, S. Vishwanath, and A. Arapostathis, "Capacity of a class of cognitive radio channels: Interference channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4391–4399, Nov. 2007.

[12] A. Jovicic and P. Viswanath, "Cognitive radio: An information-theoretic perspective," *IEEE Trans. Inf. Theory*, submitted for publication.

[13] J. Jiang, Y. Xin, and H. K. Garg, "Interference channels with common information," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 171–187, Jan. 2008.

[14] Y. Zhong, F. Alajaji, and L. L. Campbell, "Error exponents for asymmetric two-user discrete memoryless source-channel systems," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, 2007, pp. 1736–1740.

[15] I. Maric, A. Goldsmith, G. Kramer, and S. Shamai, "On the capacity of interference channels with a cognitive transmitter," in *Proc. Information Theory and Applications Workshop*, La Jolla, CA, Jan./Feb. 2007.

[16] I. Maric, A. Goldsmith, G. Kramer, and S. Shamai (Shitz), "On the capacity of interference channels with partially cognitive transmitters," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, Jun. 2007, pp. 2156–2160.

[17] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

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

[19] A. Schrijver, *Theory of Linear and Integer Programming*. New York: Wiley, 1998.

[20] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 1, pp. 60–64, Jan. 1977.

[21] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Budapest, Hungary: Akadémiai Kiadó, 1981.

[22] V. V. Prelov, "Transmission over a multiple-access channel with a special source heirarchy," *Probl. Inf. Transm.*, vol. 20, no. 4, pp. 3–10, Oct.-Dec. 1984.

[23] D. Slepian and J. K. Wolf, "A coding theorem for multiple access channels with correlated sources," *Bell Syst. Tech. J.*, vol. 52, pp. 1037–1076, 1973.

[24] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley, 2006.

Yingbin Liang (S'01–M'05) received the Ph.D. degree in electrical engineering from the University of Illinois at Urbana-Champaign, Urbana, in 2005.

From 2005 to 2007, she was working as a Postdoctoral Research Associate at Princeton University, Princeton, NJ. Since January 2008, she has been an Assistant Professor in the Department of Electrical Engineering at the University of Hawaii, Honolulu. Her research interests include information security, wireless communications, mobile *ad hoc* wireless networks, and information theory.

Dr. Liang was a Vodafone Fellow at the University of Illinois at Urbana-Champaign during 2003–2005, and received the Vodafone-U.S. Foundation Fellows Initiative Research Merit Award in 2005. She also received the M. E. Van Valkenburg Graduate Research Award from the Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, in 2005.

Anelia Somekh-Baruch (S'01–M'03) received the B.Sc. degree from Tel-Aviv University, Tel-Aviv, Israel, in 1996 and the M.Sc. and Ph.D. degrees from the Technion–Israel Institute of Technology, Haifa, Israel, in 1999 and 2003, respectively, all in electrical engineering.

During 2003–2004, she was with the Technion Electrical Engineering Department. Since 2005, she has been a Visiting Research Associate at the Electrical Engineering Department, Princeton University, Princeton, NJ. Her research interests include topics in information theory, communication theory, and data-hiding systems.

Dr. Somekh-Baruch received the Tel-Aviv University program for outstanding B.Sc. students scholarship, the Viterbi scholarship, the Rothschild foundation scholarship for postdoctoral studies, and the Marie Curie Outgoing International Fellowship.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in electrical engineering and computer science from Princeton University, Princeton, NJ, in 1977.

From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990, he has been on the faculty at Princeton, where he is the Dean of Engineering and Applied Science, and the Michael Henry Strater University Professor of Electrical Engineering. His research interests are in the areas of stochastic analysis, statistical signal processing and their applications in wireless networks, and related fields. Among his publications in these areas are the recent books *MIMO Wireless Communications* (Cambridge University Press, 2007), coauthored with Ezio Biglieri *et al*., and *Quickest Detection* (Cambridge University Press, 2009), coauthored with Olympia Hadjiliadis.

Dr. Poor is a member of the National Academy of Engineering, a Fellow of the American Academy of Arts and Sciences, and a former Guggenheim Fellow. He is also a Fellow of the Institute of Mathematical Statistics, the Optical Society of America, and other organizations. In 1990, he served as President of the IEEE Information Theory Society, and from 2004 to 2007, as the Editor-in-Chief of these TRANSACTIONS. He is the recipient of the 2005 IEEE Education Medal. Recent recognition of his work includes the 2007 IEEE Marconi Prize Paper Award, the 2007 Technical Achievement Award of the IEEE Signal Processing Society, and the 2008 Aaron D. Wyner Distinguished Service Award of the IEEE Information Theory Society.

Shlomo Shamai (Shitz) (S'80–M'82–SM'88–F'94) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Technion–Israel Institute of Technology, Haifa, Israel, in 1975, 1981, and 1986 respectively.

During 1975–1985, he was with the Communications Research Labs in the capacity of a Senior Research Engineer. Since 1986, he has with the Department of Electrical Engineering, Technion, where he is now the William Fondiller Professor of Telecommunications. His research interests encompasses a wide spectrum of topics in information theory and statistical communications.

Dr. Shamai (Shitz) is a member of the Union Radio Scientifique Internationale (URSI). He is the recipient of the 1999 van der Pol Gold Medal of URSI, and a corecipient of the 2000 IEEE Donald G. Fink Prize Paper Award, the 2003, and the 2004 joint IT/COM societies paper award, and the 2007 IEEE Information Theory Society Paper Award. He is also the recipient of 1985 Alon Grant for distinguished young scientists and the 2000 Technion Henry Taub Prize for Excellence in Research. He has served as Associate Editor for the Shannon Theory of the IEEE TRANSACTIONS ON INFORMATION THEORY, and also serves on the Board of Governors of the IEEE Information Theory Society.

Sergio Verdú (S'80–M'84–SM'88–F'93) received the Telecommunications Engineering degree from the Universitat Politècnica de Barcelona, Barcelona, Spain, in 1980 and the Ph.D. degree in electrical engineering from the University of Illinois at Urbana-Champaign, Urbana, in 1984.

Since 1984, he has been a member of the faculty of Princeton University, Princeton, NJ, where he is the Eugene Higgins Professor of Electrical Engineering.

Prof. Verdú is the recipient of the 2007 Claude E. Shannon Award and the 2008 IEEE Richard W. Hamming Medal. He is a member of the National Academy of Engineering and was awarded a Doctorate *Honoris Causa* from the Universitat Politècnica de Catalunya, Barcelona, in 2005. He is a recipient of several paper awards from the IEEE: the 1992 Donald Fink Paper Award, the 1998 Information Theory Outstanding Paper Award, an Information Theory Golden Jubilee Paper Award, the 2002 Leonard Abraham Prize Award, and the 2006 Joint Communications/Information Theory Paper Award. In 1998, Cambridge University Press published his book *Multiuser Detection*, for which he received the 2000 Frederick E. Terman Award from the American Society for Engineering Education. He served as President of the IEEE Information Theory Society in 1997 and as Associate Editor for Shannon Theory of the IEEE TRANSACTIONS ON INFORMATION THEORY. He is currently Editor-in-Chief of *Foundations and Trends in Communications and Information Theory*.