Secure Broadcasting : The Secrecy Rate Region

Ghadamali Bagherikaram, Abolfazl S. Motahari, Amir K. Khandani
Coding and Signal Transmission Laboratory,
Department of Electrical and Computer Engineering,
University of Waterloo, Waterloo, Ontario, N2L 3G1
Emails: {gbagheri,abolfazl,khandani}@cst.uwaterloo.ca

[1] ***Abstract*— In this paper, we consider a scenario where a source node wishes to broadcast two confidential messages for two respective receivers, while a wire-tapper also receives the transmitted signal. This model is motivated by wireless communications, where individual secure messages are broadcast over open media and can be received by any illegitimate receiver. The secrecy level is measured by equivocation rate at the eavesdropper. We first study the general (non-degraded) broadcast channel with confidential messages. We present an inner bound on the secrecy capacity region for this model. The inner bound coding scheme is based on a combination of random binning and the Gelfand-Pinsker bining. This scheme matches the Marton's inner bound on the broadcast channel without confidentiality constraint. We further study the situation where the channels are degraded. For the degraded broadcast channel with confidential messages, we present the secrecy capacity region. Our achievable coding scheme is based on Cover's superposition scheme and random binning. We refer to this scheme as Secret Superposition Scheme. In this scheme, we show that randomization in the first layer increases the secrecy rate of the second layer. This capacity region matches the capacity region of the degraded broadcast channel without security constraint. It also matches the secrecy capacity for the conventional wire-tap channel. Our converse proof is based on a combination of the converse proof of the conventional degraded broadcast channel and Csiszar lemma.**

I. Introduction

The notion of information theoretic secrecy in communication systems was first introduced by Shannon in [1]. The information theoretic secrecy requires that the received signal of the eavesdropper does not provide even a single bit information about the transmitted messages. Shannon considered a pessimistic situation where both the intended receiver and the eavesdropper have direct access to the transmitted signal (which is called ciphertext). Under these circumstances, he proved a negative result showing that perfect secrecy can be achieved only when the entropy of the secret key is greater than or equal to the entropy of the message. In modern cryptography, all practical cryptosystems are based on Shannnon's pessimistic assumption. Due to practical constraints, secret keys are much shorter than messages. Therefore, these practical cryptosystems are theoretically susceptible of breaking by attackers. However, the goal of designing such practical ciphers is to guarantee that there exists no efficient algorithm for breaking them.

[1]Financial support provided by Nortel and the corresponding matching funds by the Natural Sciences and Engineering Research Council of Canada (NSERC), and Ontario Centres of Excellence (OCE) are gratefully acknowledged.

Wyner in [2] showed that the above negative result is a consequence of Shannon's restrictive assumption that the adversary has access to precisely the same information as the legitimate receiver. Wyner considered a scenario in which a wire-tapper receives the transmitted signal over a degraded channel with respect to the legitimate receiver's channel. He further assumed that the wire-tapper has no computational limitations and knows the codebook used by the transmitter. He measured the level of ignorance at the eavesdropper by its equivocation and characterized the capacity-equivocation region. Interestingly, a non-negative perfect secrecy capacity is always achievable for this scenario.

The secrecy capacity for the Gaussian wire-tap channel is characterized by Leung-Yan-Cheong in [3]. Wyner's work then is extended to the general (non-degraded) broadcast channel with confidential messages (BCC) by Csiszar and Korner [4]. They considered transmitting confidential information to the legitimate receiver while transmitting common information to both the legitimate receiver and the wire-tapper. They established a capacity-equivocation region of this channel.

The BCC is further studied recently in [5]–[7], where the source node transmits a common message for both receivers, along with two additional confidential messages for two respective receivers. The fading BCC is investigated in [8], [9] where the broadcast channels from the source node to the legitimate receiver and the eavesdropper is corrupted by multiplicative fading gain coefficients, in addition to additive white Gaussian noise terms. The Channel State Information (CSI) is assumed to be known at the transmitter. In [10], the perfect secrecy capacity is derived where the channels are slow fading. Moreover, the optimal power control policy is obtained for different scenarios regarding availability of CSI. In [11], the wire-tap channel is extended to the parallel broadcast channels and the fading channels with multiple receivers. Here, the secrecy constraint is a perfect equivocation for each messages, even if all the other messages are revealed to the eavesdropper. The secrecy sum capacity for a reverse broadcast channel is derived for this restrictive assumption. The notion of the wire-tap channel is also extended to multiple access channels [12]–[15], relay channels [16]–[19], parallel channels [20] and MIMO channels [21]–[26]. Some other related works on communication of confidential messages can be found in [27]–[31].

In this paper, we consider a scenario where a source node wishes to broadcast two confidential messages for two respec-

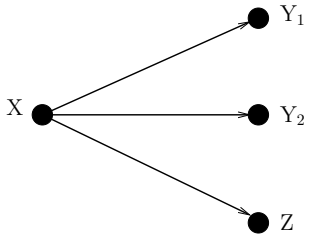

Fig. 1. Broadcast Channel with Confidential Messages

tive receivers, while a wire-tapper also receives the transmitted signal. This model is motivated by wireless communications, where individual secure messages are broadcast over shared media and can be received by any illegitimate receiver. In fact, we simplify the restrictive constraint imposed in [11] and assume that the eavesdropper does not have access to the other messages. We first study the general broadcast channel with confidential messages. We present an achievable rate region for this channel. Our achievable coding scheme is based on the combination of the random binning and the Gelfand-Pinsker bining [32]. This scheme matches the Marton's inner bound [33] on the broadcast channel without confidentiality constraint. We further study the situation where the channels are physically degraded and characterize the secrecy capacity region. Our achievable coding scheme is based on Cover's superposition coding [34] and the random binning. We refer to this scheme as Secret Superposition Coding. This capacity region matches the capacity region of the degraded broadcast channel without security constraint. It also matches the secrecy capacity of the wire-tap channel.

The rest of the paper is organized as follows. In section II we introduce the system model. In Section III, we provide an inner bound on the secrecy capacity region when the channels are not degraded. In section IV, we specialize our channel to the physically degraded and establish the secrecy capacity region. In Section V, we conclude the paper.

II. Preliminaries

In this paper, a random variable is denoted by a capital letter (e.g. X) and its realization is denoted by a corresponding lower case letter (e.g. x). The finite alphabet of a random variable is denoted by a script letter (e.g. $\mathcal{X}$) and its probability distribution is denoted by $P(x)$. Let $\mathcal{X}$ be a finite alphabet set and denote its cardinality by $|\mathcal{X}|$. The members of $\mathcal{X}^n$ will be written as $x^n = (x_1, x_2, ..., x_n)$, where subscripted letters denote the components and superscripted letters denote the vector. The notation x^{i-1} denotes the vector $(x_1, x_2, ..., x_{i-1})$. A similar notation will be used for random variables and random vectors.

Consider a Broadcast Channel with Confidential messages as depicted in fig.1. In this confidential setting, the transmitter (X) wants to broadcast some secret messages to the legitimated receivers (Y_1,Y_2), and prevent the eavesdropper (Z) from having any information about the messages. A discrete memoryless broadcast channel with confidential messages is described by finite sets $\mathcal{X}$, $\mathcal{Y}_1$,$\mathcal{Y}_2$,$\mathcal{Z}$, and a conditional distribution $P(y_1, y_2, z|x)$. The input of the channel is $x \in \mathcal{X}$ and the outputs are $(y_1, y_2, z) \in (\mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Z})$ for receiver 1, receiver 2, and the eavesdropper, respectively. The transmitter wishes to send independent messages (W_1, W_2) to the respective receivers in n uses of the channel while insuring perfect secrecy. The channel is discrete memoryless in the sense that

$$P(y_1^n, y_2^n, z^n|x^n) = \prod_{i=1}^{n} P(y_{1,i}, y_{2,i}, z_i|x_i). \quad (1)$$

A $((2^{nR_1}, 2^{nR_2}), n)$ code for a broadcast channel with confidential messages consists of a stochastic encoder

$$f : (\{1, 2, ..., 2^{nR_1}\} \times \{1, 2, ..., 2^{nR_2}\}) \rightarrow \mathcal{X}^n, \quad (2)$$

and two decoders,

$$g_1 : \mathcal{Y}_1^n \rightarrow \{1, 2, ..., 2^{nR_1}\} \quad (3)$$

and

$$g_2 : \mathcal{Y}_2^n \rightarrow \{1, 2, ..., 2^{nR_2}\}. \quad (4)$$

The average probability of error is defined as the probability that the decoded messages are not equal to the transmitted messages; that is,

$$P_e^{(n)} = P(g_1(Y_1^n) \neq W_1 \cup g_2(Y_2^n) \neq W_2). \quad (5)$$

The knowledge that the eavesdropper gets about W_1 and W_2 from its received signal Z^n is modeled as

$$I(Z^n, W_1) = H(W_1) - H(W_1|Z^n), \quad (6)$$
$$I(Z^n, W_2) = H(W_2) - H(W_2|Z^n), \quad (7)$$

and

$$I(Z^n, (W_1, W_2)) = H(W_1, W_2) - H(W_1, W_2|Z^n). \quad (8)$$

Perfect secrecy revolves around the idea that the eavesdropper cannot get even a single bit information about the transmitted messages. Perfect secrecy thus requires that

$$I(Z^n, W_1) = 0 \Leftrightarrow H(W_1) = H(W_1|Z^n), \quad (9)$$
$$I(Z^n, W_2) = 0 \Leftrightarrow H(W_2) = H(W_2|Z^n),$$

and

$$I(Z^n, (W_1, W_2)) = 0 \Leftrightarrow H(W_1, W_2) = H(W_1, W_2|Z^n). \quad (10)$$

The secrecy levels of confidential messages W_1 and W_2 are measured at the eavesdropper in terms of equivocation rates which are defined as follows.

Definition 1 *The equivocation rates R_{e1}, R_{e2} and R_{e12} for the Broadcast channel with confidential messages are:*

$$R_{e1} = \frac{1}{n} H(W_1|Z^n), \quad (11)$$
$$R_{e2} = \frac{1}{n} H(W_2|Z^n),$$
$$R_{e12} = \frac{1}{n} H(W_1, W_2|Z^n).$$

The perfect secrecy rates R_1 and R_2 are the amount of information that can be sent to the legitimate receivers not only reliably but also confidentially.

Definition 2 *A secrecy rate pair (R_1, R_2) is said to be achievable if for any $\epsilon > 0$, there exists a sequence of $((2^{nR_1}, 2^{nR_2}), n)$ codes, such that for sufficiently large n, we have:*

$$P_e^{(n)} \leq \epsilon, \tag{12}$$
$$R_{e1} \geq R_1 - \epsilon_1, \tag{13}$$
$$R_{e2} \geq R_2 - \epsilon_2, \tag{14}$$
$$R_{e12} \geq R_1 + R_2 - \epsilon_3. \tag{15}$$

In the above definition, the first condition concerns the reliability, while the other conditions guarantee perfect secrecy for each individual message and both messages as well. The capacity region is defined as follows.

Definition 3 *The capacity region of the broadcast channel with confidential messages is the closure of the set of all achievable rate pairs (R_1, R_2).*

III. General BCCs

In this section, we consider the general broadcast channel with confidential messages and present an achievable rate region. Our achievable coding scheme is based on a combination of the random binning and the Gelfand-Pinsker bining schemes [32]. The following theorem illustrates the achievable rate region for this channel.

Theorem 1 *Let $\mathbb{R}_I$ denote the union of all non-negative rate pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_1 &\leq I(V_1;Y_1) - I(V_1;Z), \\ R_2 &\leq I(V_2;Y_2) - I(V_2;Z), \\ R_1 + R_2 &\leq I(V_1;Y_1) + I(V_2;Y_2) - I(V_1,V_2;Z) - I(V_1;V_2). \end{aligned} \tag{16}$$

over all joint distributions $P(v_1, v_2)P(x|v_1, v_2)P(y_1, y_2, z|x)$. Then any rate pair $(R_1, R_2) \in \mathbb{R}_I$ is achievable for the broadcast channel with confidential messages.

Remark 1 *If we remove the secrecy constraints by setting $\mathcal{Z} = \emptyset$, then the above rate region reduces to Marton's achievable region for the general broadcast channel.*

Remark 2 *If we remove one of the users by setting e.g., $\mathcal{Y}_2 = \emptyset$, then we get the Csiszar and Korner's secrecy capacity for the other user.*

Proof:

1) *Codebook Generation*: The structure of the encoder is depicted in Fig.2. Fix $P(v_1)$, $P(v_2)$ and $P(x|v_1, v_2)$. The stochastic encoder generates $2^{n(I(V_1;Y_1)-\epsilon)}$ independent and identically distributed sequences v_1^n according to the distribution $P(v_1^n) = \prod_{i=1}^n P(v_{1,i})$. Next, randomly distribute these sequences into 2^{nR_1} bins such that each bin contains

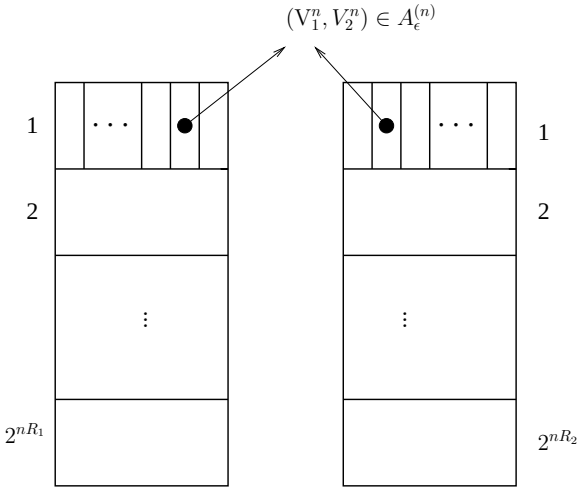

Fig. 2. The Stochastic Encoder

$2^{n(I(V_1;Z)-\epsilon)}$ codewords. Similarly, it generates $2^{n(I(V_2;Y_2)-\epsilon)}$ independent and identically distributed sequences v_2^n according to the distribution $P(v_2^n) = \prod_{i=1}^n P(v_{2,i})$. Next, randomly distribute these sequences into 2^{nR_2} bins such that each bin contains $2^{n(I(V_2;Z)-\epsilon)}$ codewords. Index each of the above bins by $w_1 \in \{1, 2, ..., 2^{nR_1}\}$ and $w_2 \in \{1, 2, ..., 2^{nR_2}\}$ respectively.

2) *Encoding*: To send messages w_1 and w_2, the transmitter looks for v_1^n in bin w_1 of the first bin set and looks for v_2^n in bin w_2 of the second bin set, such that $(v_1^n, v_2^n) \in A_\epsilon^{(n)}(P_{V_1,V_2})$ where $A_\epsilon^{(n)}(P_{V_1,V_2})$ denotes the set of jointly typical sequences v_1^n and v_2^n with respect to $P(v_1, v_2)$. The rates are such that there exist more than one joint typical pair, the transmitter randomly chooses one of them and then generates x^n according to $P(x^n|v_1^n, v_2^n) = \prod_{i=1}^n P(x_i|v_{1,i}, v_{2,i})$. This scheme is equivalent to the scenario in which each bin is divided into subbins and the transmitter randomly chooses one of the subbins of bin w_1 and one of the subbins of bin w_2. It then looks for a joint typical sequence (v_1^n, v_2^n) in the corresponding subbins and generates x^n.

3) *Decoding*: The received signals at the legitimate receivers, y_1^n and y_2^n, are the outputs of the channels $P(y_1^n|x^n) = \prod_{i=1}^n P(y_{1,i}|x_i)$ and $P(y_2^n|x^n) = \prod_{i=1}^n P(y_{2,i}|x_i)$, respectively. The first receiver looks for the unique sequence v_1^n such that (v_1^n, y_1^n) is jointly typical and declares the index of the bin containing v_1^n as the message received. The second receiver uses the same method to extract the message w_2.

4) *Error Probability Analysis*: Since the region of (12) is a subset of Marton's region then, error probability analysis is the same as [33].

5) *Equivocation Calculation*: The proof of secrecy requirement for each individual message (13) and (14) is straightforward and may therefore be omitted.

To prove the requirement of (15) consider $H(W_1, W_2|Z^n)$, we have

$$\begin{aligned}
nR_{e12} &= H(W_1, W_2|Z^n) \\
&\geq H(W_1, W_2, Z^n) - H(Z^n) \\
&= H(W_1, W_2, V_{1^n}, V_2^n, Z^n) \\
&- H(V_1^n, V_2^n|W_1, W_2, Z^n) - H(Z^n) \\
&= H(W_1, W_2, V_1^n, V_2^n) \\
&+ H(Z^n|W_1, W_2, V_1^n, V_2^n) \\
&- H(V_1^n, V_2^n|W_1, W_2, Z^n) - H(Z^n) \\
&\overset{(a)}{\geq} H(W_1, W_2, V_1^n, V_2^n) \\
&+ H(Z^n|W_1, W_2, V_1^n, V_2^n) - n\epsilon_n - H(Z^n) \\
&\overset{(b)}{=} H(W_1, W_2, V_1^n, V_2^n) + H(Z|V_1^n, V_2^n) - n\epsilon_n \\
&- H(Z^n) \\
&\overset{(c)}{\geq} H(V_1^n, V_2^n) + H(Z^n|V_1^n, V_2^n) - n\epsilon_n - H(Z^n) \\
&\overset{(d)}{=} H(V_1^n) + H(V_2^n) - I(V_1^n; V_2^n) \\
&- I(V_1^n, V_2^n; Z^n) - n\epsilon_n \\
&\overset{(e)}{=} I(V_1^n; Y_1^n) + I(V_2^n; Y_2^n) - I(V_1^n; V_2^n) \\
&- I(V_1^n, V_2^n; Z^n) - n\epsilon_n \\
&\geq nR_1 + nR_2 - n\epsilon_n,
\end{aligned}$$

where (a) follows from Fano's inequality which states that for sufficiently large n we have $H(V_1^n, V_2^n|W_1, W_2, Z^n) \leq h(P_{we}^{(n)}) + nP_{we}^n I(V_1, V_2; Z) \leq n\epsilon_n$. Here P_{we}^n denotes the wiretapper's error probability of decoding (v_1^n, v_2^n) in the case that the bin numbers w_1 and w_2 are known to the eavesdropper. Since the sum rate is less than $I(V_1, V_2; Z)$, then $P_{we}^n \to 0$ for sufficiently large n. (b) follows from the following Markov chain: $(W_1, W_2) \to (V_1, V_2) \to Z$. Hence, we have $H(Z^n|W_1, W_2, V_1^n, V_2^n) = H(Z^n|V_1^n, V_2^n)$. (c) follows from the fact that $H(W_1, W_2, V_1^n, V_2^n) \geq H(V_1^n, V_2^n)$. (d) follows from that fact that $H(V_1^n) = I(V_1^n; Y_1^n)$ and $H(V_2^n) = I(V_2^n; Y_2^n)$.

■

IV. The secrecy capacity Region of the Degraded BCCs

In this section, we consider the degraded broadcast channel with confidential messages and establish its secrecy capacity region.

Definition 4 *A broadcast channel with confidential messages is said to be physically degraded, if $X \to Y_1 \to Y_2 \to Z$ forms a Markov chain. In the other words, we have*

$$P(y_1, y_2, z|x) = P(y_1|x)P(y_2|y_1)P(z|y_2). \tag{17}$$

Definition 5 *A broadcast channel with confidential messages is said to be stochastically degraded if its conditional marginal distributions are the same as that of a physically degraded broadcast channel, i.e., if there exist two distributions $P^{'}(y_2|y_1)$ and $P^{'}(z|y_2)$ such that*

$$\begin{aligned}
P(y_2|x) &= \sum_{y_1} P(y_1|x)P^{'}(y_2|y_1) \qquad (18)\\
P(z|x) &= \sum_{y_2} P(y_2|x)P^{'}(z|y_2)
\end{aligned}$$

Lemma 1 *The secrecy capacity region of a broadcast channel with confidential messages depends only on the conditional marginal distributions $P(y_1|x)$, $P(y_2|x)$ and $P(z|x)$.*

Proof: The proof is very similar to [34] and may therefore be omitted here. ■

In the following theorem, we fully characterize the capacity region of the physically degraded broadcast channel with confidential messages.

Theorem 2 *The capacity region for transmitting independent secret information over the degraded broadcast channel is the convex hull of the closure of all (R_1, R_2) satisfying*

$$R_1 \leq I(X; Y_1|U) + I(U; Z) - I(X; Z), \tag{19}$$
$$R_2 \leq I(U; Y_2) - I(U; Z). \tag{20}$$

for some joint distribution $P(u)P(x|u)P(y_1, y_2, z|x)$.

Remark 3 *If we remove the secrecy constraints by setting $\mathcal{Z} = \emptyset$, then the above theorem reduces to the capacity region of the degraded broadcast channel.*

Proof:

Achievability: The coding scheme is based on Cover's superposition coding and the random bining. We refer to this scheme as Secure Superposition Coding scheme. The available resources at the encoder are used for two purposes: to confuse the eavesdropper so that perfect secrecy can be achieved for both layers, and to transmit the messages in the main channels. To satisfy confidentiality, the randomization used in the first layer is again used in the second layer. This makes a shift of $I(U; Z)$ in the bound of R_1. The formal proof of the achievability is as follows:

1) *Codebook Generation*: The structure of the encoder is depicted in Fig.3. Let us fix $P(u)$ and $P(x|u)$. The stochastic encoder generates $2^{n(I(U;Y_2)-\epsilon)}$ independent and identically distributed sequences u^n according to the distribution $P(u^n) = \prod_{i=1}^n P(u_i)$. Next, we randomly distribute these sequences into 2^{nR_2} bins such that each bin contains $2^{n(I(U;Z)-\epsilon)}$ codewords. We index each of the above bins by $w_2 \in \{1, 2, ..., 2^{nR_2}\}$. For each codeword of u^n, it also generates $2^{n(I(X;Y_1|U)-\epsilon)}$ independent and identically distributed sequences x^n according to the distribution $P(x^n|u^n) = \prod_{i=1}^n P(x_i|u_i)$. We randomly distribute these sequences into 2^{nR_1} bins such that each bin contains $2^{n(I(X;Z)-I(U;Z)-\epsilon)}$ codewords. We index each of the above bins by $w_1 \in \{1, 2, ..., 2^{nR_1}\}$.

2) *Encoding*: To send messages w_1 and w_2, the transmitter randomly chooses one of the codewords in bin w_2, say u^n.

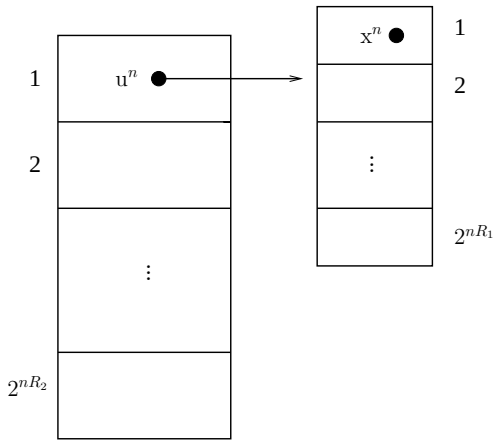

Fig. 3. Secret Superposition structure

Then given u^n, the transmitter randomly chooses one of x^n in bin w_1 of the second layer and sends it.

3) *Decoding*: The received signal at the legitimate receivers, y_1^n and y_2^n, are the outputs of the channels $P(y_1^n|x^n) = \prod_{i=1}^n P(y_{1,i}|x_i)$ and $P(y_2^n|x^n) = \prod_{i=1}^n P(y_{2,i}|x_i)$, respectively. Receiver 2 determines the unique u^n such that (u^n, y_2^n) are jointly typical and declares the index of the bin containing u^n as the message received. If there is none of such or more than of one such, an error is declared. Receiver 1 looks for the unique (u^n, x^n) such that (u^n, x^n, y_1^n) are jointly typical and declares the indexes of the bins containing u^n and x^n as the messages received. If there is none of such or more than of one such, an error is declared.

4) *Error Probability Analysis*: Since each rate pair of (19) is in the capacity region of the degraded broadcast channel without confidentiality constraint, then it can be readily shown that the error probability is arbitrarily small, c.f. [34].

5) *Equivocation Calculation*: To prove the secrecy requirement of (13), we have

$$\begin{aligned}
nR_{e1} &= H(W_1|Z^n) \\
&\geq H(W_1|Z^n, U^n) \\
&= H(W_1, Z^n|U^n) - H(Z^n|U^n) \\
&= H(W_1, X^n, Z^n|U^n) - H(Z^n|U^n) \\
&- H(X^n|W_1, Z^n, U^n) \\
&\overset{(a)}{=} H(W_1, X^n|U^n) + H(Z^n|W_1, U^n, X^n) \\
&- H(Z^n|U^n) - n\epsilon_n \\
&\overset{(b)}{\geq} H(X^n|U^n) + H(Z^n|X^n) \\
&- H(Z^n|U^n) - n\epsilon_n \\
&\overset{(c)}{=} I(X^n; Y_1^n|U^n) + I(U^n; Z^n) \\
&- I(X^n; Z^n) - n\epsilon_n \\
&\geq nR_1 - n\epsilon_n,
\end{aligned}$$

where (a) follows from Fano's inequality which states that $H(X^n|W_1, Z^n, U^n) \leq h(P_{we}^{(n)}) + nP_{we}^n I(X;Z) \leq n\epsilon_n$ for sufficiently large n. Here P_{we}^n denotes the wiretapper's error probability of decoding x^n given the bin number and the codeword u^n are known to the eavesdropper. Since the rate is less than $I(X;Z)$, then $P_{we}^n \to 0$ for sufficiently large n. (b) follows from the fact that $(W_1, U) \to X \to Z$ forms a Markov chain. Thus we have $I(W_1, U^n; Z^n|X^n) = 0$, where it is implied that $H(Z^n|W_1, U^n, X^n) = H(Z^n|X^n)$. (c) follows from two identities: $H(X^n|U^n) = I(X^n; Y_1^n|U^n)$ and $H(Z^n|X^n) - H(Z^n|U^n) = I(U^n; Z^n) - I(X^n; Z^n)$. Since the proof of the requirement (14) is straightforward, we need to prove the requirement of (15).

$$\begin{aligned}
nR_{e12} &= H(W_1, W_2|Z^n) \\
&\geq H(W_1, W_2, Z^n) - H(Z^n) \\
&= H(W_1, W_2, U^n, X^n, Z^n) \\
&- H(U^n, X^n|W_1, W_2, Z^n) - H(Z^n) \\
&= H(W_1, W_2, U^n, X^n) + H(Z^n|W_1, W_2, U^n, X^n) \\
&- H(U^n, X^n|W_1, W_2, Z^n) - H(Z^n) \\
&\overset{(a)}{\geq} H(W_1, W_2, U^n, X^n) \\
&+ H(Z^n|W_1, W_2, U^n, X^n) - n\epsilon_n - H(Z^n) \\
&\overset{(b)}{=} H(W_1, W_2, U^n, X^n) + H(Z|U^n, X^n) \\
&- n\epsilon_n - H(Z^n) \\
&\overset{(c)}{\geq} H(U^n, X^n) + H(Z^n|U^n, X^n) - n\epsilon_n - H(Z^n) \\
&= H(U^n) + H(X^n|U^n) - I(U^n, X^n; Z^n) - n\epsilon_n \\
&\overset{(d)}{=} I(U^n; Y_2^n) + I(X^n; Y_1^n|U^n) - I(X^n; Z^n) \\
&- I(U^n; Z^n|X^n) - n\epsilon_n \\
&\geq nR_1 + nR_2 - n\epsilon_n,
\end{aligned}$$

where (a) follows from Fano's inequality that $H(U^n, X^n|W_1, W_2, Z^n) \leq h(P_{we}^{(n)}) + nP_{we}^n I(U, X; Z) \leq n\epsilon_n$ for sufficiently large n. Here P_{we}^n denotes the wiretapper's error probability of decoding (u^n, x^n) in the case that the bin numbers w_1 and w_2 are known to the eavesdropper. The eavesdropper first looks for the unique u^n in bin w_2 of the first layer, such that it is jointly typical with z^n. Since the number of candidate codewords is less than $I(U;Z)$, then the probability of error is arbitrarily small for a sufficiently large n. Next, given u^n, the eavesdropper looks for the unique x^n in bin w_1 which is jointly typical with z^n. Similarly, since the number of available candidates is less than $I(X;Z)$, then the probability of error decoding is arbitrarily small. (b) follows from the fact that $(W_1, W_2) \to U \to X \to Z$ forms a Markov chain. Therefore, we have $I(W_1, W_2; Z^n|U^n, X^n) = 0$, where it is implied that $H(Z^n|W_1, W_2, U^n, X^n) = H(Z^n|U^n, X^n)$. (c) follows from the fact that $H(W_1, W_2, U^n, X^n) \geq H(U^n, X^n)$. (d) follows from that fact that $H(U^n) = I(U^n; Y_2^n)$ and $H(X^n|U^n) = I(X^n; Y_1^n|U^n)$.

Converse: The transmitter sends two independent secret messages W_1 and W_2 to receiver 1 and receiver 2 respectively. Let us define $U_i = (W_2, Y_1^{i-1})$. The following chain of

inequality clarifies the proof:

$$\begin{aligned}
nR_1 &\overset{(a)}{\leq} \sum_{i=1}^{n} I(W_1;Y_{1,i}|W_2,Z_i,Y_1^{i-1},\widetilde{Z}^{i+1}) \\
&+ n\delta_1 + n\epsilon_3 \\
&= \sum_{i=1}^{n} I(W_1;Y_{1,i}|U_i,Z_i,\widetilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&\overset{(b)}{\leq} \sum_{i=1}^{n} I(X_i;Y_{1,i}|U_i,Z_i,\widetilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&\overset{(c)}{=} \sum_{i=1}^{n} I(X_i;Y_{1,i},U_i,Z_i|\widetilde{Z}^{i+1}) - I(X_i;Z_i|\widetilde{Z}^{i+1}) \\
&- I(X_i;U_i|Z_i,\widetilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&\overset{(d)}{=} \sum_{i=1}^{n} I(X_i;Y_{1,i}|U_i,\widetilde{Z}^{i+1}) + I(X_i;U_i|\widetilde{Z}^{i+1}) \\
&- I(X_i;Z_i|\widetilde{Z}^{i+1}) - I(X_i;U_i|Z_i,\widetilde{Z}^{i+1}) \\
&+ n\delta_1 + n\epsilon_3 \\
&\overset{(e)}{=} \sum_{i=1}^{n} I(X_i;Y_{1,i}|U_i,\widetilde{Z}^{i+1}) - I(X_i;Z_i|\widetilde{Z}^{i+1}) \\
&+ I(Z_i;U_i|\widetilde{Z}^{i+1}) - I(Z_i;U_i|X_i,\widetilde{Z}^{i+1}) \\
&+ n\delta_1 + n\epsilon_3 \\
&\overset{(f)}{=} \sum_{i=1}^{n} I(X_i;Y_{1,i}|U_i,\widetilde{Z}^{i+1}) - I(X_i;Z_i|\widetilde{Z}^{i+1}) \\
&+ I(Z_i;U_i|\widetilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3
\end{aligned}$$

(a) follows from the following lemma (2). (b) follows from the data processing theorem. (c) follows from the chain rule. (d) follows from the fact that $I(X_i;Y_{1,i},U_i,Z_i|\widetilde{Z}^{i+1}) = I(X_i;U_i|\widetilde{Z}^{i+1}) + I(X_i;Y_{1,i}|U_i,\widetilde{Z}^{i+1}) + I(X_i;Z_i|Y_{1,i},U_i,\widetilde{Z}^{i+1})$ and from the fact that $\widetilde{Z}^{i+1}U_i \rightarrow X_i \rightarrow Y_{1,i} \rightarrow Y_{2,i} \rightarrow Z_i$ forms a Markov chain, which means that $I(X_i;Z_i|Y_{1,i},U_i,\widetilde{Z}^{i+1}) = 0$. (e) follows from the fact that $I(X_i;U_i|\widetilde{Z}^{i+1}) - I(X_i;U_i|Z_i,\widetilde{Z}^{i+1}) = I(Z_i;U_i|\widetilde{Z}^{i+1}) - I(Z_i;U_i|X_i,\widetilde{Z}^{i+1})$. (f) follows from the fact that $\widetilde{Z}^{i+1}U_i \rightarrow X_i \rightarrow Z_i$ forms a Markov chain. Thus $I(Z_i;U_i\widetilde{Z}^{i+1}|X_i) = 0$ which implies that $I(Z_i;U_i|X_i,\widetilde{Z}^{i+1}) = 0$.

Lemma 2 *: For the broadcast channel with confidential messages of $(W_1,W_2) \rightarrow X^n \rightarrow Y_1^nY_2^nZ^n$, the perfect secrecy rates are bounded as follows,*

$$\begin{aligned}
nR_1 &\leq \sum_{i=1}^{n} I(W_1;Y_{1i}|W_2,Z_i,Y_1^{i-1},\widetilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3, \\
nR_2 &\leq \sum_{i=1}^{n} I(W_2;Y_{2i}|Z_i,Y_2^{i-1},\widetilde{Z}^{i+1}) + n\delta_1 + n\epsilon_2.
\end{aligned}$$

Proof: We need to prove the first bound. The second bound can similarly be proven. nR_1 is bounded as follows:

$$\begin{aligned}
nR_1 &\overset{(a)}{\leq} H(W_1|W_2,Z^n) + n\epsilon_3 \\
&\overset{(b)}{\leq} H(W_1|W_2,Z^n) - H(W_1|Y_1^n,W_2) + n\delta_1 + n\epsilon_3 \\
&= I(W_1;Y_1^n|W_2) - I(W_1;Z^n|W_2) + n\delta_1 + n\epsilon_3
\end{aligned}$$

where (a) follows from the secrecy constraint that $H(W_1,W_2|Z^n) \geq H(W_1,W_2) - n\epsilon_3$, the fact that $H(W_2|Z^n) \leq H(W_2)$ and the fact that two messages are independent. (b) follows from Fano's inequality that $H(W_1|Y_1^n,W_2) \leq n\delta_1$. Next, we expand $I(W_1;Y_1^n|W_2)$ and $I(W_1;Z^n|W_2)$ starting with $I(W_1;Y_1|W_2)$ and $I(W_1;\widetilde{Z}^n|W_2)$, respectively.

$$\begin{aligned}
I(W_1;Y_1^n|W_2) &= \sum_{i=1}^{n} I(W_1;Y_{1i}|W_2,Y_1^{i-1}) \\
&= \sum_{i=1}^{n} I(W_1,\widetilde{Z}^{i+1};Y_{1i}|W_2,Y_1^{i-1}) \\
&- I(\widetilde{Z}^{i+1};Y_{1i}|W_1,W_2,Y_1^{i-1}) \\
&= \sum_{i=1}^{n} I(W_1;Y_{1i}|W_2,Y_1^{i-1},\widetilde{Z}^{i+1}) \\
&+ I(\widetilde{Z}^{i+1};Y_{1i}|W_2,Y_1^{i-1}) \\
&- I(\widetilde{Z}^{i+1};Y_{1i}|W_1,W_2,Y_1^{i-1}) \\
&= \sum_{i=1}^{n} I(W_1;Y_{1i}|W_2,Y_1^{i-1},\widetilde{Z}^{i+1}) \\
&+ \Delta_1 - \Delta_2,
\end{aligned}$$

where, $\Delta_1 = \sum_{i=1}^{n} I(\widetilde{Z}^{i+1};Y_{1i}|W_2,Y_1^{i-1})$ and $\Delta_2 = \sum_{i=1}^{n} I(\widetilde{Z}^{i+1};Y_{1i}|W_1,W_2,Y_1^{i-1})$. Similarly, we have,

$$\begin{aligned}
I(W_1;Z^n|W_2) &= \sum_{i=1}^{n} I(W_1;Z_i|W_2,\widetilde{Z}^{i+1}) \\
&= \sum_{i=1}^{n} I(W_1,Y_1^{i-1};Z_i|W_2,\widetilde{Z}^{i+1}) \\
&- I(Y_1^{i-1};Z_i|W_1,W_2,\widetilde{Z}^{i+1}) \\
&= \sum_{i=1}^{n} I(W_1;Z_i|W_2,Y_1^{i-1},\widetilde{Z}^{i+1}) \\
&+ I(Y_1^{i-1};Z_i|W_2,\widetilde{Z}^{i+1}) \\
&- I(Y_1^{i-1};Z_i|W_1,W_2,\widetilde{Z}^{i+1}) \\
&= \sum_{i=1}^{n} I(W_1;Z_i|W_2,Y_1^{i-1},\widetilde{Z}^{i+1}) \\
&+ \Delta_1^* - \Delta_2^*,
\end{aligned}$$

where, $\Delta_1^* = \sum_{i=1}^{n} I(Y_1^{i-1};Z_i|W_2,\widetilde{Z}^{i+1})$ and $\Delta_2^* = \sum_{i=1}^{n} I(Y_1^{i-1};Z_i|W_1,W_2,\widetilde{Z}^{i+1})$. According to lemma 7 of

[4], $\Delta_1 = \Delta_1^*$ and $\Delta_2 = \Delta_2^*$. Thus, we have,

$$\begin{aligned}
nR_1 &\leq \sum_{i=1}^{n} I(W_1; Y_{1i}|W_2, Y_1^{i-1}, \widetilde{Z}^{i+1}) \\
&- I(W_1; Z_i|W_2, Y_1^{i-1}, \widetilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&= \sum_{i=1}^{n} H(W_1|W_2, Z_i, Y_1^{i-1}, \widetilde{Z}^{i+1}) \\
&- H(W_1|W_2, Y_{1i}, Y_1^{i-1}, \widetilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&\overset{(a)}{\leq} \sum_{i=1}^{n} H(W_1|W_2, Z_i, Y_1^{i-1}, \widetilde{Z}^{i+1}) \\
&- H(W_1|W_2, Y_{1i}, Z_i, Y_1^{i-1}, \widetilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3 \\
&= \sum_{i=1}^{n} I(W_1; Y_{1i}|W_2, Z_i, Y_1^{i-1}, \widetilde{Z}^{i+1}) + n\delta_1 + n\epsilon_3,
\end{aligned}$$

where (a) follows from the fact that conditioning always decreases the entropy. ■

For the second receiver, we have

$$\begin{aligned}
nR_2 &\overset{(a)}{\leq} \sum_{i=1}^{n} I(W_2; Y_{2,i}|Y_2^{i-1}, Z_i, \widetilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&= \sum_{i=1}^{n} H(Y_{2,i}|Y_2^{i-1}, Z_i, \widetilde{Z}^{i+1}) \\
&- H(Y_{2,i}|W_2, Y_2^{i-1}, Z_i, \widetilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&\overset{(b)}{\leq} \sum_{i=1}^{n} H(Y_{2,i}|Z_i, \widetilde{Z}^{i+1}) \\
&- H(Y_{2,i}|W_2, Y_1^{i-1}, Y_2^{i-1}, Z_i, \widetilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&\overset{(c)}{=} \sum_{i=1}^{n} H(Y_{2,i}|Z_i, \widetilde{Z}^{i+1}) \\
&- H(Y_{2,i}|U_i, Z_i, \widetilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&= \sum_{i=1}^{n} I(Y_{2,i}; U_i|Z_i, \widetilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&= \sum_{i=1}^{n} I(Y_{2,i}; U_i|\widetilde{Z}^{i+1}) + I(Y_{2,i}; Z_i|U_i, \widetilde{Z}^{i+1}) \\
&- I(Y_{2,i}; Z_i|\widetilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&= \sum_{i=1}^{n} I(Y_{2,i}; U_i|\widetilde{Z}^{i+1}) - I(Z_i; U_i|\widetilde{Z}^{i+1}) \\
&+ I(Z_i; U_i|Y_{2,i}, \widetilde{Z}^{i+1}) + n\delta_2 + n\epsilon_1 \\
&\overset{(d)}{=} \sum_{i=1}^{n} I(Y_{2,i}; U_i|\widetilde{Z}^{i+1}) - I(Z_i; U_i|\widetilde{Z}^{i+1}) \\
&+ n\delta_2 + n\epsilon_1,
\end{aligned}$$

where (a) follows from the lemma (2). (b) follows from the fact that conditioning always decreases the entropy. (c) follows from the fact that $Y_2^{i-1} \rightarrow W_2\widetilde{Z}^{i+1}Y_1^{i-1} \rightarrow Y_{2i} \rightarrow Z_i$ forms a Markov chain. (d) follows from the fact that $\widetilde{Z}^{i+1}U_i \rightarrow Y_{2,i} \rightarrow Z_i$ forms a Markov chain. Thus $I(Z_i; U_i\widetilde{Z}^{i+1}|Y_{2i}) = 0$ which implies that $I(Z_i; U_i|Y_{2i}, \widetilde{Z}^{i+1}) = 0$. Now, following [34], let us define the time sharing random variable Q which is uniformly distributed over $\{1, 2, ..., n\}$ and independent of $(W_1, W_2, X^n, Y_1^n, Y_2^n)$. Let us define $U = U_Q$, $V = (\widetilde{Z}^{Q+1}, Q)$, $X = X_Q$, $Y_1 = Y_{1,Q}$, $Y_2 = Y_{2,Q}$, $Z = Z_Q$, then we can bound R_1 and R_2 as follows

$$R_1 \leq I(X; Y_1|U, V) + I(U; Z|V) - I(X; Z|V), \quad (21)$$

$$R_2 \leq I(U; Y_2|V) - I(U; Z|V). \quad (22)$$

Since Conditional mutual informations are average of unconditional ones, the maximum region is achieved when V is a constant. This proves the converse part. ■

V. Conclusion

A generalization of the wire-tap channel to the case of two receivers and one eavesdropper is considered. We established an inner bound for the general (non-degraded) case. This bound matches Marton's bound on broadcast channels without security constraint. Furthermore, we considered the scenario in which the channels are degraded. We established the perfect secrecy capacity region for this case. The achievability coding scheme is a secret superposition scheme where randomization in the first layer helps the secrecy of the second layer. The converse proof combines the converse proof for the degraded broadcast channel without security constraint and the perfect secrecy constraint.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, pp. 656-715, Oct. 1949.

[2] A. Wyner, "The Wire-tap Channel,"*Bell System Technical Journal*, vol. 54, pp. 13551387, 1975

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian Wiretap Channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451456, July 1978.

[4] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339348, May 1978.

[5] R. Liu, I. Maric, P. Spasojevic and R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels with Confidential Messages," *IEEE Trans. Inform. Theory*, Vol. 54, Issue: 6, pp.2493-2507, Jun 2008.

[6] J. Xu and B. Chen, "Broadcast Confidential and Public Messages," *in Proc. 42nd Conf. Information Sciences and Systems (CISS)*, Princeton, NJ, Mar. 2008.

[7] J. Xu, Y. Cao, and B. Chen ,"Capacity Bounds for Broadcast Channels with Confidential Messages", available at `http://arxiv.org/PS_cache/arxiv/pdf/0805/0805.4374v1.pdf`.

[8] Y. Liang and H. V. Poor, "Secure Communication Over Fading Channels," *in Proc. 44th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, pp. 817823, Sep. 2006.

[9] Y. Liang, H. V. Poor and S. Shamai (Shitz), " Secure Communication Over Fading Channels", *IEEE Trans. Inform. Theory*, Volume 54, Issue 6, pp.2470 - 2492, June 2008.

[10] P. K. Gopala, L. Lai and H. El-Gamal, " On the Secrecy Capacity of Fading Channels", available at `http://arxiv.org/PS_cache/cs/pdf/0610/0610103v1.pdf`.

[11] A. Khisti, A. Tchamkerten and G. W. Wornell, "Secure Broadcasting," available at `http://arxiv.org/PS_cache/cs/pdf/0702/0702093v1.pdf`.

[12] E. Tekin, S. Serbetli, and A. Yener, "On secure Signaling for the Gaussian Multiple Access Wire-tap Channel," *in Proc. 2005 Asilomar Conf. On Signals, Systems, and Computers*, Asilomar, CA, November 2005.

[13] E. Tekin and A. Yener, "The Gaussian Multiple Access Wiretap Channel with Collective Secrecy Constraints," *in Proc. Int. Symp. On Inf. Theory (ISIT)*, Seattle, WA, July 914, 2006.

[14] Y. Liang and V. Poor, "Generalized Multiple Access Channels with Confidential Messages," *in Proc. Of IEEE Int. Symp. Inf. Theory (ISIT)*, 2006.

[15] E. Tekin and A. Yener, "The General Gaussian Multiple Access and Two-Way wire-Tap Channels: Achievable Rates and Cooerative Jamming,", available at http://arxiv.org/PS_cache/cs/pdf/0702/0702112v2.pdf.
[16] Y. Oohama, "Coding for Relay Channels with Confidential messages," *in Proc. Of IEEE Information Theory Workshop*, pp. 87 89,2001.
[17] Y. Oohama, "Relay channels with confidential messages," *IEEE Trans. on Information Theory*, Submitted, available at http://arxiv.org/PS_cache/cs/pdf/0611/0611125v7.pdf.
[18] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *IEEE Trans. Inf. Theory*, submitted, available at http://arxiv.org/PS_cache/cs/pdf/0612/0612044v1.pdf.
[19] M. Yuksel and E. Erkip., "The Relay Channel with a Wiretapper," *in Proc. Forty-First Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, USA, Mar. 2007.
[20] Z. Li, R. Yates, and W. Trappe, "Secrecy Capacity of Independent Parallel Channels," *in Proc. 44th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, pp. 841848,Sep. 2006.
[21] F. Oggier, B. Hassibi, " The MIMO Wiretap Channel", *Communications, Control and Signal Processing, 2008. ISCCSP 2008. 3rd International Symposium on.*,12-14 March 2008 Page(s):213 - 218
[22] S. Shafiee, L. Nan and S. Ulukus, "Secrecy Capacity of the 2-2-1 Gaussian MIMO Wire-tap Channel", *Communications, Control and Signal Processing, 2008. ISCCSP 2008. 3rd International Symposium on.*,12-14 March 2008 Page(s):207 - 212
[23] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO Wiretap Channel," *in Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 24-29, 2007.
[24] A. Khisti and G. Wornell, "Secure Transmission with Multiple Antennas: The MISOME Wiretap Channel," *IEEE Trans. Inf. Theory*, submitted, available at http://arxiv.org/PS_cache/arxiv/pdf/0708/0708.4219v1.pdf.
[25] T. Liu and S. Shamai (Shitz), "A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel," *IEEE Trans. Inf. Theory*, available at http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.4105v1.pdf.
[26] R. Liu and H. V. Poor, "Secrecy Capacity Region of a Multi-antenna Gaussian Broadcast Channel with Confidential Messages," available at http://arxiv.org/PS_cache/arxiv/pdf/0709/0709.4671v1.pdf.
[27] X. Tang, R. Liu, P. spasojevic and V. Poor, "The Gaussian Wiretap Channel with a Helping Interferer," *Proceedings of the 2008 IEEE International Symposium on Information Theory*, Toronto, ON, Canada, July 6-11, 2008
[28] C. Chan, "Success Exponent of Wiretapper: A Tradeoff between Secrecy and Reliability," available at http://arxiv.org/PS_cache/arxiv/pdf/0805/0805.3605v4.pdf.
[29] X. Tang, R. Liu, P. Spasojevic and V.Poor, "Interference-Assisted Secret Communication," available at http://arxiv.org/PS_cache/arxiv/pdf/0804/0804.1382v1.pdf.
[30] L.Lai, H. El-Gamal, V. Poor, "Secrecy Capacity of the Wiretap Channel with Noisy Feedback," available at http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.0865v1.pdf.
[31] O.Ozan Koyluoglu, H.El-Gamal, "On the Secure Degrees of Freedom in the K-User Gaussian Interference Channel," *Proceedings of the 2008 IEEE International Symposium on Information Theory*, Toronto, ON, Canada, July 6-11, 2008
[32] S. I. Gelfand and M. S. Pinsker, "Coding for Channel with Random Parameters," *Problemy Peredachi Informatsii*, vol. 9, no. 1, pp. 1931, 1980.
[33] K. Marton, "A Coding Theorem for the Discrete Memoryless Broadcast Channel," *IEEE Trans. on Inf. Theory*, vol. 25, no. 1, pp. 306311, May 1979.
[34] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley Sons, Inc., 1991.