OPPORTUNISTIC SECRET COMMUNICATION IN WIRELESS SYSTEMS

by

ZANG LI

A dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Electrical and Computer Engineering

Written under the direction of

Prof. Wade Trappe and Prof. Roy Yates

and approved by

New Brunswick, New Jersey

October, 2009

ABSTRACT OF THE DISSERTATION

Opportunistic Secret Communication in Wireless Systems

By Zang Li

Dissertation Directors:

Prof. Wade Trappe and Prof. Roy Yates

This thesis examines the challenges of information-theoretic secret communication that exploits the temporal and spatial variations of the wireless medium to improve secret communication rates.

We first examine the secrecy capacity of a system consisting of independent parallel channels with one transmitter, one intended receiver and one eavesdropper. We show that the secrecy capacity of the system is the sum of the secrecy capacities of the individual subchannels. We further derive the optimal power allocation strategy for a system of parallel AWGN channels subject to a total power constraint, and also extend the results to random fading channels with additive Gaussian noise.

We then study the achievable secrecy rate with Gaussian random codes for the situation where the channel of the intended receiver is a constant AWGN channel, while the eavesdropper's channel is fast Rayleigh fading with unknown realizations but known statistics to the transmitter. The proposed method with artificial noise and bursting provides ways to achieve positive secrecy rate even when Bob's channel is worse than Eve's channel on average.

We also examine the achievable secrecy rate for a multiple antenna system, and the optimal input structure needed to achieve this rate. For the multiple input single output case, an analytical solution is derived. Multiple antenna systems provide extra degrees of freedom to the transmitter so that a beamforming-like approach can be used to provide advantage to the intended receiver against the eavesdropper.

Next we derive a secrecy capacity outer bound region for a class of one-sided interference channels. The outer bound is shown to be tight for a class of binary deterministic one-sided interference channels, and can be achieved within one bit for some Gaussian one-sided interference channels.

Finally, as Gaussian random codes are impractical, we evaluate achievable secrecy rates with discrete signaling. We observe that with discrete signaling, there exists an optimal power that maximizes the achievable secrecy rate. For the AWGN channel, larger constellation is always better. While for fading channel, the optimal constellation size varies with the power constraint, and discrete signaling can perform better than random Gaussian coding.

Acknowledgements

I would like to express my sincere gratitude to my advisor Prof. Wade Trappe, for his great guidance and support to me. Prof. Trappe offered me the opportunity to pursue PhD in WINLAB when I first came to Rutgers for a Master degree. He always provides me insightful ideas, and helps me to think from different perspectives when I met difficulties in research. He is always very patient to revise my drafts and give me many valuable comments to improve my work. I am very grateful to his consistent support to me, without which I would not have been here finishing this tough journey toward PhD.

I would also like to express my sincere gratitude to my co-advisor Prof. Roy Yates, for his great guidance and support to me. Prof. Yates led me into the information theory area, and taught me how to become a good researcher in this difficult field. He can always see the essence of a problem quickly, and he is always willing to spend time with me going over all those derivations. Talking with him is always very enjoyable and full of inspiring ideas. I deeply appreciate all the time and efforts he spent on me.

I would like to thank Prof. Narayan Mandayam and Dr. Ruoheng Liu to be my dissertation committee members. Thanks to them for reading my thesis and provide me many nice suggestions to improve the thesis.

I would like to thank all my colleagues for the helpful discussions we have had, and for making WINLAB a friendly place to work in. I want to especially thank Xiaojun Tang who helped me on many document issues when I was away from campus. I also want to thank

all my friends in WINLAB for the joy and help they gave to me in the last several years.

Finally, I want to thank my family for their support and care. It is their love that makes me strong and happy.

Table of Contents

List of Figures

Chapter 1

Introduction

Ensuring the confidentiality of communications is fundamental to securing any network. This requirement becomes particularly important for wireless systems, where eavesdropping is facilitated by the broadcast nature of the wireless medium. Rather than physically guard the communication medium to provide confidentiality, the traditional approach is to employ cryptographic algorithms, known as ciphers, that suitably obfuscate the communication between two entities so that only they can correctly interpret the messages, while all other entities fail to glean any useful information.

The question of how much information is too much to leak to an eavesdropping adversary is at the heart of modern cryptography, and two important schools of thought have emerged: information-theoretic and complexity-based security. The basics of information-theoretic encryption was first formulated by Shannon in 1949 [69], where the adversary is assumed to have unlimited computational resources and the cipher objective is to ensure that absolutely no information is released to the adversary. Thus, should the adversary observe an encrypted message (the ciphertext), the adversary is no better off than just randomly guessing the original message (the plaintext). Complexity-based cryptography, on the other hand, discards the notion that the adversary has infinite computing capabilities, and instead assumes the adversary has limitations on how much computation can be performed. Now, when an adversary witnesses a ciphertext, the necessary computations render it practically infeasible for the adversary to deduce the corresponding plaintext.

Common to both approaches, encryption algorithms are characterized by the existence of some form of information shared between the legitimate entities. This information, which is often colloquially referred to as a key, parameterizes specific realizations of the encryption service and must be kept private. This shared secret information is a further means to differentiate between these two forms of security. On the one hand, Shannon's fundamental result revealed the limits of information-theoretic security: a *perfectly secret* cipher requires that the legitimate participants share an amount of secret information (the key) that is as large as the message they wish to exchange securely. While, on the other hand, for complexity-based cryptography, the size of the key that must be shared can be significantly shorter than the size of the message or messages that will be exchanged.

This might suggest to some that complexity-based confidentiality is superior, while others might well draw the opposite conclusion. Our view is that the real issue in achieving confidentiality boils down to ensuring that the two communicating parties share the same, common key. Once this secret information is shared, then using an established encryption algorithm, such as AES [79], is possible. Unfortunately, establishing encryption keys is a problem that has plagued security systems for a long time, and inevitably some variation of the chicken-and-egg problem arises. One promising technique of modern cryptography that partially addresses this challenge is public key cryptography, where every entity has two keys: a private key that is closely guarded, and a public key that is publicly announced [59, 79]. An individual may securely send another entity a message by using that entity's public key to encrypt the message, which can only be decrypted using the corresponding private key. The asymmetry inherent in this protocol allows for one to use these messages to establish and distribute other keys, known as session keys, that can provide confidentiality to services requiring the processing of bulk amounts of data.

Unfortunately, there are several well-known problems with this formulation of public key cryptography. First, public key cryptography is reliant on the validity of unproven complexity assumptions, such as the difficulty of factoring or taking discrete logarithms. However, even if one accepts the intractability of such one-way primitives [4], there is still no guarantee as to the authenticity of the public key – in short, the public key might or might not belong to whom you think. The customary solution to this rather severe obstacle is the use of trusted third parties, such as the government or certificate authorities, e.g. as in X.509 [3], which are capable of securely distributing public keys. Again, we have the chicken-and-egg problem, plus now we face issues regarding the availability of these external entities.

Ideally, rather than require the assistance of trusted third parties, what we would like is for each communicating pair to take advantage of some physical resource that can facilitate the sharing of a key. For example, one such physical property that has received considerable attention over the past few decades is the quantum channel [10,83]. More recently, however, it has been realized that the wireless channel itself is another such resource for sharing keys [25, 27, 33, 54]. In fact, the wireless channel provides two distinct strategies for key formation: *extraction* and *dissemination*. Extraction techniques utilize the fact that in rich, multipath environments the reciprocal radio propagation characteristics between two entities are unique and decorrelate quickly with distance. This suggests that the wireless channel itself can be used as a source of common randomness for establishing keys for encryption without needing the involvement of trusted third parties. Several strategies have been proposed for extracting secret information from such common randomness [5, 16, 54]. Dissemination strategies, however, were originally cast in the context of the wiretap channel

[84], and take a different approach to secrecy. In dissemination, the communicating entity seeks to take advantage of mismatch between the primary channel and any adversarial channel in order to secretly convey shared bits. It is this second mode of sharing keys via the wireless channel that is the focus of this thesis.

The main scenario of interest to us is illustrated in Figure 1.1. Alice wants to secretly transmit a secret message to Bob utilizing the public wireless transmission medium. This corresponds to the dissemination mode mentioned earlier. Since the transmission medium is open, a passive eavesdropper Eve can overhear the transmission and guess what Alice is sending. Due to the complexity of the wireless environment, the channels between Alice-Bob and Alice-Eve are probably different. This difference can be exploited by proper coding techniques so that such secret communication is possible. The main focus of this thesis is to study the rate of such secret communication under various channel scenarios. We note that this rate can be very low, especially when Eve has a very good channel, such as may arise when Eve is closer to the transmitter than Bob. However, we may only need this process to build a key for subsequent communication with computationally efficient symmetric key algorithms, so even a low secrecy dissemination rate is still very valuable.

The rate at which bits can be securely shared was originally examined in [15, 84], where the notion of secrecy capacity was introduced to describe the rate (in bits per channel use) that a sender could communicate in an information-theoretically secure manner to an intended receiver in the presence of an eavesdropper. These early results on secrecy capacity were rather pessimistic in the sense that the underlying requirements were quite restrictive from a practical point of view. In particular, using the channel to communicate a secret to an intended receiver required the channel to the intended receiver to be better than the channel to the eavesdropper. In practical wireless settings, distance-dependent

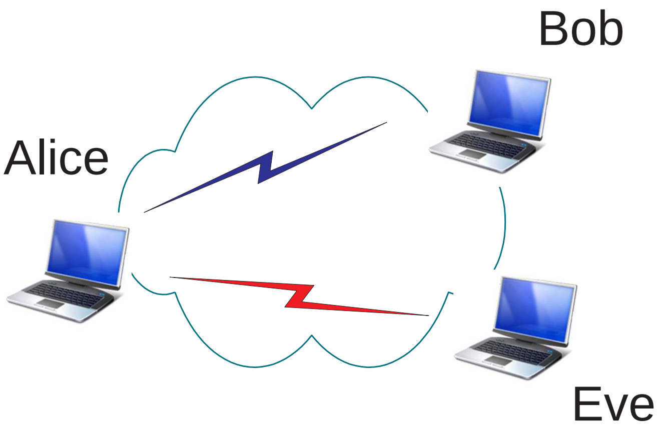


Figure 1.1: The wireless broadcast scenario.

attenuation and spatial variability of the channel make it unlikely that one can always meet the requirement that the intended channel is better.

The assumptions underlying this pessimism, however, do not reflect the design of modern communications systems, and in particular do not exploit the large number of degrees of freedom available to a modern wireless system. Notably, in order to achieve the performance of modern wireless systems, it is necessary to shift how we looked at the spectral, temporal, and spatial properties of the wireless environment. For example, even if channels are time-invariant, it is possible to use multiple subcarriers in order to provide a large number of parallel subchannels, as is utilized in OFDM transceivers, and the underlying frequency selectivity induced by multipath may provide a diversity advantage [80]. Further, even in a single narrowband subchannel, temporal variations due to fading can be exploited rather than avoided by transmitting during periods of good channel conditions, thereby resulting in enhanced performance [22]. Lastly, the dimensionality of the wireless system can be further expanded through the use of multiple antennas, as has been illustrated in recent MIMO communication systems [19, 76], in which multiple antennas improve the communication rates significantly. Overall, the past decade has seen a large and very successful effort by the wireless research community to exploit these degrees of freedom. Both diversity and capacity enhancing mechanisms have been proposed, analyzed and practically evaluated, and new capacity definitions have been proposed to characterize communication over time-varying channels.

Recently there has been a flurry of activity targeted at applying these strategies to the problem of enhancing the secrecy of communication between wireless devices. This literature is generally split into several different thrusts. There is a broad collection of work focused on establishing the secrecy capacity for a three party communication scenario (transmitter, receiver and eavesdropper) under varying assumptions on knowledge of the fading channel states [8,14,23,42,43,47,64]. Variations of the secrecy problem for broadcast and relay channels have been discussed in [32,35], while the achievable secrecy rate regions and outer bounds for multiple access channels with various secrecy requirements have been studied in [45,46,49,50,73,74].

The literature shows that there are many challenging directions for wireless secret communication that have yet to be explored. The overall objective of this thesis is to examine the challenges of information-theoretic secure communication that utilizes the temporal variations and spatial diversity advantages of the wireless medium to improve secret communication rates in presence of a passive eavesdropper. This thesis begins with a background review of information-theoretic secret communications over wireless channels in Chapter 2. The secrecy capacity of a system consisting of independent parallel channels is examined in Chapter 3. The secrecy capacity of the system is shown to be simply the summation of the secrecy capacities of the individual channels. The optimal power allocation strategy for a system with parallel AWGN channels subject to a total power constraint is derived, and the result is extended to random fading channels with additive Gaussian noise. Numerical evaluation shows that the diversity, either in frequency or in time, improves the rate of secret communication and allows secret communication even when the eavesdropper's channel is on average better than the legitimate party's channels.

Next, in Chapter 4, the achievable secrecy rate with Gaussian random codes is studied for the situation where the main channel is a constant AWGN channel, and Eve's channel is fast Rayleigh fading with unknown realizations but known statistics to the transmitter. The proposed method with artificial noise and bursting provides an approach to achieve positive secrecy rate even when Bob's channel is worse than Eve's channel on average. Then, in Chapter 5, we examine the achievable secrecy rate for a multiple antenna system, and the optimal input structure needed to achieve this rate. For the general multiple input multiple (MIMO) output case, the problem is not convex and is hard to solve. However, for the multiple input single output (MISO) case, the problem can be reformulated and solved. An analytical solution is derived for this simple case and the implication of the results are discussed. Multiple antennas provide extra degrees of freedom to the transmitter so that a beamforming-like approach can be used to provide advantage to the intended receiver against the eavesdropper.

In Chapter 6, we derive an outer bound of the secrecy capacity region for a class of one-sided interference channels. The outer bound is shown to be tight for a class of deterministic channels, and can be achieved within one bit for some Gaussian one-sided interference channels. Next, in Chapter 7, we evaluate the effect of discrete signaling on the achievable secrecy rate since the Gaussian random codes employed in information theoretical analysis are not practical for use in a real system. We observe that, with discrete signaling, there always exists an optimal power that maximizes the achievable secrecy rate. Extra power will only benefit the eavesdropper and hurt the secrecy. For the AWGN channel, larger constellations are always better. While for the fading channel, the optimal constellation size varies with the power constraint, and discrete signaling can perform better than random Gaussian coding. Finally, some discussion on future work is presented in Chapter 8.

Chapter 2

Background

In an information-theoretic secret communication system, a sender (Alice) wishes to reliably communicate a secret S to an intended receiver (Bob) in the presence of an eavesdropper (Eve). The secret S, a random integer from the set $\{1, 2, \ldots, 2^{nR}\}$, is transmitted in n channel uses. In this case, the secret has entropy $H(S) = nR$ bits and the secrecy communication rate is

$$R = H(S)/n$$

bits per channel use. In these n channel uses, Alice transmits the coded signal

$$X^n = X_1, \ldots, X_n,$$

Bob receives the channel output

$$Y^n = Y_1, \ldots, Y_n$$

and decodes $\hat{S}$ with error probability

$$P_e = \mathrm{P}r\Big[S \neq \hat{S}\Big].$$

From the reliable communication point of view, this error probability should be made as close to zero as possible with a large enough codeword length n. After Eve overhears the output

$$Z^n = Z_1, \ldots, Z_n$$

, her residual uncertainty regarding the secret message S is given by the conditional entropy $H(S|Z^n)$. The mutual information between S and Z^n is

$$I(S; Z^n) = H(S) - H(S|Z^n), \tag{2.1}$$

so the closer the residual uncertainty is to the original message entropy, the more confidential the message is. This secrecy level is generally expressed as a normalized equivocation rate $\Delta = H(S|Z^n)/H(S)$. From the perspective of both reliable and confidential communication, the system performance depends on both the communication rate R and the equivocation rate Δ. In particular, the rate tuple (R_0, Δ_0) is achievable if for any $\epsilon > 0$ there exists a rate R encoder and decoder with equivocation rate Δ such that for some n,

$$P_e \leq \epsilon, \qquad R \geq R_0 - \epsilon, \qquad \Delta \geq \Delta_0 - \epsilon. \tag{2.2}$$

In this thesis, we focus on the case $\Delta_0 = 1$, corresponding to the case where Eve's information per secret information bit regarding the secret S gained by the observation Z^n is given by

$$I(S; Z^n) = H(S) - H(S|Z^n) = (1 - \Delta)H(S) \leq \epsilon H(S). \tag{2.3}$$

That is, Eve learns arbitrarily little information regarding the secret S.

This model of information-theoretic secret communication started with Wyner's analysis of the discrete memoryless wiretap channel [84] in 1975. In Wyner's system, Eve hears a degraded version of Bob's received signal in that the channels are defined by a Markov chain $X \to Y \to Z$. Hence, Eve always has a worse channel than Bob no matter what the input is. The objective is to find an encoding and decoding scheme to maximize both the equivocation at the wire-tapper and the transmission rate of the main system. In this paper, Wyner found the trade-off curve between the equivocation Δ and the transmission rate R.

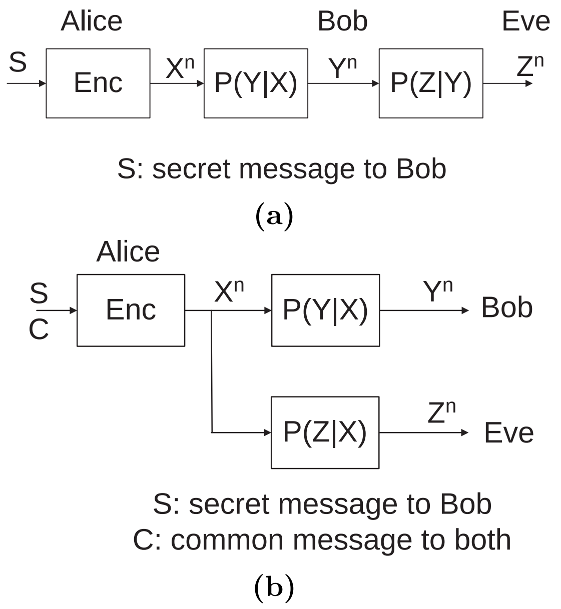


Figure 2.1: **(a)** Wiretap channel studied by Wyner [84]; **(b)** Broadcast channel studied by Csiszár and Körner [15]. The most important difference between the two is that in the wiretap channel model, Eve's received signal is a degraded version of Bob's, while in the broadcast channel model, this degradation assumption is not assumed. The degradation has a direct effect on the optimal coding strategy: with degradation, Alice only needs to encode directly in channel symbols X; without degradation, Alice might need to use a virtual channel from an auxiliary random variable V to X and encode in term of V to achieve secrecy capacity.

He defined the secrecy capacity C_s as the maximum rate R such that the uncertainty at the wiretapper is arbitrarily close to the entropy of the source. Wyner's results showed that there exists a $C_s > 0$ such that reliable transmission at a rate up to C_s in approximately perfect secrecy is possible for the wire-tap channel. The secrecy capacity is given by

$$\mathcal{C}_s = \max_X I(X;Y) - I(X;Z), \tag{2.4}$$

where the notation $\max_X$ for the random variable X is a shorthand for maximization over the choice of PMF $P_X(x)$ when X is discrete or the PDF $f_X(x)$ when X is continuous.

This information-theoretic secret communication framework was generalized by Csiszár and Körner [15] in 1978 to a broadcast system where the Markov condition does not need to hold (of course, Wyner's wiretap channel is a special case of a broadcast system). The differences between the two channel models are illustrated in Figure 2.1. In Csiszár and Körner's model, Alice transmits confidential messages to Bob at rate R as well as common messages to both Bob and Eve at rate R_0. The more important distinction between the two is that in the wiretap channel model, Eve's received signal is a degraded version of Bob's, while in the broadcast channel model, this degradation relationship is not assumed. The degradation has a direct effect on the optimal coding strategy: with degradation, Alice only needs to encode directly in channel symbols X; while without degradation, Alice might need to use a virtual channel from an auxiliary random variable V to X and encode in terms of V to achieve secrecy capacity.

The equivocation rate at Eve about the private message is R_e. Perfect secrecy is achieved when $R_e = R$. Csiszar and Korner derived the region for all achievable rate triples (R, R_e, R_0). When the rate of common messages is $R_0 = 0$, [15] defined the secrecy capacity $\mathcal{C}_s$ as the maximum rate R, such that the tuple $(R, R_e = R, R_0 = 0)$ is achievable and showed that

$$\mathcal{C}_s = \max_{V \to X \to YZ} I(V;Y) - I(V;Z). \tag{2.5}$$

In this case, given the discrete memoryless channel (DMC) $P_{YZ|X}$, secrecy capacity is achieved by maximizing over all joint distributions $P_{V,X}(v,x)$ such that the Markov chain $V \to X \to YZ$ holds.

In terms of coding realization, the underlying techniques involve stochastic encoding and joint typical decoding. The codebook used is illustrated in Figure 2.2, where each box in the grid represents a length n codeword vector, denoted as V^n. V^n is randomly generated as a sequence of iid symbols according to a probability distribution $P_V(v)$. For each secret message w, there is a total number of $2^{nR'}$ codewords, corresponding to the codewords in the w-th column in the codebook, where R' is a properly chosen parameter as we will

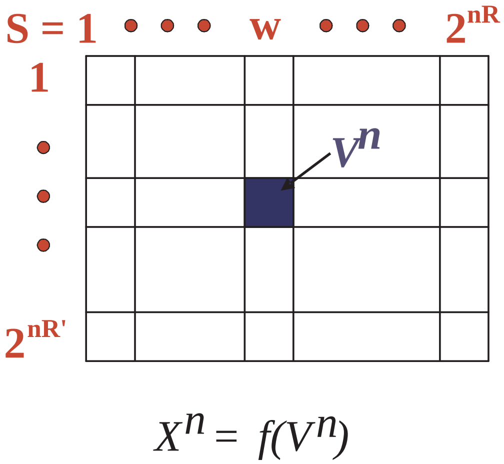


Figure 2.2: Codebook used to realize the perfect secret communication in Csiszár and Körner's paper [15]. Each box in the grid represents a length n codeword vector, denoted as V^n. V^n is randomly generated as a sequence of iid symbols according to a probability distribution $P_V(v)$. For each secret message w, there is a total number of $2^{nR'}$ codewords, corresponding to the codewords in the w-th column in the codebook, where R' is a properly chosen parameter. Thus, for 2^{nR} messages, the codebook has 2^{nR} columns with a total number of $2^{n(R+R')}$ codewords.

see later. Thus, for 2^{nR} messages, the codebook has 2^{nR} columns with a total number of $2^{n(R+R')}$ codewords.

To transmit a message with index w, the encoder first randomly picks a codeword V^n among its $2^{nR'}$ codewords in the w-th column, then maps it to the transmitted codes X^n using a predefined mapping function from V to X. After the transmitted signal passes through the channel, Bob receives Y^n and Eve receives Z^n. To decode the message, Bob finds a $\hat{V}^n$ from the entire codebook that's jointly typical with Y^n. Then he determines $\hat{w}$ to be the column index of $\hat{V}^n$. When the size of the codebook satisfies

$$2^{n(R+R')} \leq 2^{nI(V;Y)}, \tag{2.6}$$

it can be shown that with a probability close to 1, only the transmitted codeword is jointly typical with Y^n, so the error probability $P(\hat{w} \neq w)$ can be made arbitrarily small. On the other hand, to ensure the full equivocation of Eve, i.e. Eve has minimal knowledge of S

given her observation Z^n, the column size $2^{nR'}$ should satisfy

$$2^{nR'} > 2^{nI(V;Z)}, \tag{2.7}$$

so that there exists a codeword in every column that is jointly typical with Z^n. Thus, a decoder using joint typicality cannot give the eavesdopper any information on the message Alice sent. Combining the above two conditions, we get the achievable rate

$$R \leq I(V;Y) - I(V;Z).$$

The maximum achievable rate is obtained by maximizing over the choices of V and the preprocessing channel from V to X. Note that although the preprocessing $V \rightarrow X$ channel reduces the mutual information delivered to Bob, i.e. $I(V;Y) \leq I(X;Y)$, it reduces the mutual information delivered to Eve as well. So, it is possible that the auxiliary V and the auxiliary $V \rightarrow X$ channel creates more confusion for Eve than that for Bob. In other words, the loss on mutual information suffered by Eve is more severe than that suffered by Bob, and hence, the difference $I(V;Y) - I(V;Z)$ is increased. The above is only an intuitive sketch of the achievability proof. A rigorous proof of achievability and the converse can be found in [15].

To achieve secret transmission, both papers [15, 84] require the channel between Alice and Bob to be better than the channel between Alice and Eve, which is a hard condition to meet in practice. In 1993, Maurer [55] showed that secret key agreement between Alice and Bob can be achieved even when the channel between Alice and Bob is worse than the channel between Alice and Eve, as long as these two channels are different and public discussion is allowed. Bounds on the secret key rate were derived, and several examples of possible ways to realize secret key agreement were discussed. In these examples, public discussions help to build a virtual channel between Alice and Bob that is less noisy than the virtual channel between Alice and Eve. In this thesis, we do not consider this scenario. Secrecy capacity with feedback was considered in several recent works [36, 37, 71].

In subsequent work, Maurer and Wolf [56] showed that the secrecy condition (2.3) employed by Wyner and by Csiszár and Körner could be strengthened considerably through a technique called *privacy amplification* without reducing the secret capacity $\mathcal{C}_s$. In this thesis, we follow the traditional information-theoretic definitions of secrecy with a focus on the optimization of $\mathcal{C}_s$ while keeping in mind that an actual system would likely employ privacy amplification [9].

In theory, (2.5) is a complete characterization of the secrecy capacity $\mathcal{C}_s$; however, many questions remain unanswered. For example, there are no systematic methods to optimize over the auxiliary input V and the $P_{X|V}$ channel. It was shown that when channels satisfy the *less noisy* or *more capable* conditions, defined as follows following [34], V and the $P_{X|V}$ are not necessary.

Definition 1 (more capable) *The DMC $P_{Y|X}$ is more capable than $P_{Z|X}$ if $I(X;Y) - I(X;Z) \geq 0$ for all inputs X.*

Definition 2 (less noisy) *The DMC $P_{Y|X}$ is less noisy than $P_{Z|X}$ if $I(U;Y) - I(U;Z) \geq 0$ for all inputs U and DMCs $P_{X|U}$.*

It is known that less noisy implies more capable. However, for channels that do not satisfy the more capable conditions, it is not clear whether an auxiliary random variable and a preprocessing channel are beneficial to secret communication or not. Yet the auxiliary is often essential; an example of how the auxiliary can reshape the communication channel to enhance the secrecy rate is described below.

Example: Binary Asymmetric Channel

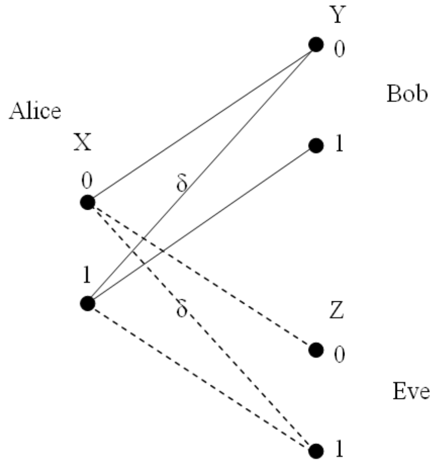


Figure 2.3: An example of binary asymmetric channel between Alice, Bob and Eve.

Consider the binary asymmetric channel shown in Figure 2.3. The crossover probabilities for Alice-Bob channel is $P(Y = 1|X = 0) = 0$, and $P(Y = 0|X = 1) = \delta$. The Alice-Eve channel has the opposite crossover probabilities, i.e. $P(Z = 1|X = 0) = \delta$, and $P(Z = 0|X = 1) = 0$. Without loss of generality, we assume $\delta \leq 1/2$. With one crossover probability equaling zero, the $X \to Y$ channel and the $X \to Z$ channel are commonly referred to as Z-channels because the channel transition diagram resembles the letter "Z". However, to avoid confusion with the $X \to Z$ channel of Eve, we refer to these as "Z" channels, where "Z" refers to the shape of the transition diagram, as distinct from Eve's receiver output Z.

Let $h(p)$ denotes the binary entropy function, i.e.

$$h(p) = -p\log(p) - (1-p)\log(1-p).$$

Also let $P(X = 1) = p$. Then, $P(Y = 1) = p(1-\delta)$, and

$$I(X;Y) = H(Y) - H(Y|X) = h(p(1-\delta)) - ph(\delta).$$

Similarly, $P(Z = 1) = p + (1-p)\delta$, and

$$I(X;Z) = H(Z) - H(Z|X) = h(p + (1-p)\delta) - (1-p)h(\delta).$$

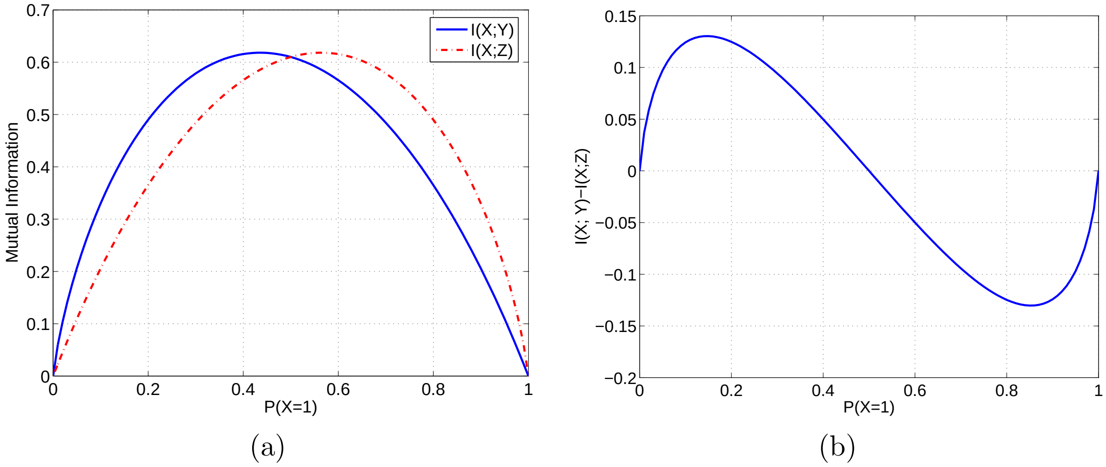


Figure 2.4: (a) $I(X;Y)$, $I(X;Z)$ and (b) $I(X;Y) - I(X;Z)$ for the binary asymmetric channel $X \rightarrow YZ$ with $\delta = 0.2$.

Therefore,

$$I(X;Y) - I(X;Z) = h(p(1-\delta)) - ph(\delta) - h(p + (1-p)\delta) + (1-p)h(\delta).$$

The expression is a function of p, and is plotted in Figure 2.4, for $\delta = 0.2$. Since $I(X;Y)$ is not always greater than $I(X;Z)$, this channel does not satisfy the more capable condition. The technical question is can we find a joint distribution $P(V,X) = P(V)P(X|V)$ such that

$$\max_{V\rightarrow X\rightarrow YZ}[I(V;Y) - I(V;Z)] > \max_{X\rightarrow YZ}[I(X;Y) - I(X;Z)]?$$

Let us make a binary "Z" channel from V to X as shown in Figure 2.5(a), with the crossover probability $P(X=0|V=1) = \gamma$, and $P(X=1|V=0) = 0$. Then, the resulting $V \rightarrow Y$ channel has the crossover probabilities

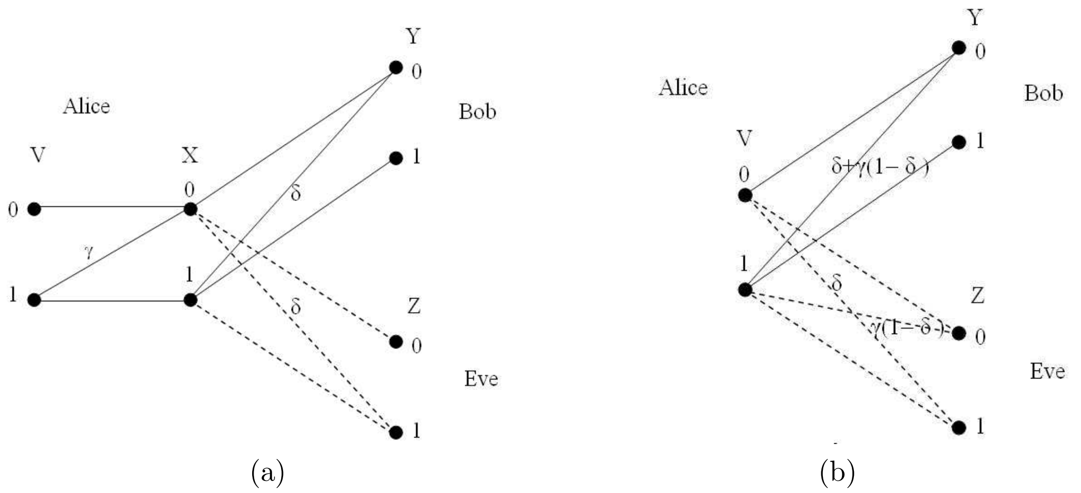
$$P(Y=1|V=0) = 0$$

$$P(Y=0|V=1) = \gamma + (1-\gamma)\delta = \delta + \gamma(1-\delta),$$

and the $V \rightarrow Z$ channel has

$$P(Z=1|V=0) = \delta$$

$$P(Z=0|V=1) = \gamma(1-\delta).$$



(a) (b)

Figure 2.5: (a) The virtual $V \rightarrow X$ preprocessing “Z” channel. (b) The effective $V \rightarrow YZ$ channel after adding the virtual “Z” channel.

The new binary asymmetric channels between V and YZ with different crossover probabilities are illustrated in Figure 2.5(b).

Note that the additional “Z” channel renders the crossover probability from $V = 1$ to $Y = 0$ greater than the crossover probability from $X = 1$ to $Y = 0$, as well as the crossover probability from $V = 1$ to $Z = 0$ greater than that from $X = 1$ to $Z = 0$. Since $X = 1$ is the better symbol in terms of decoding for Eve, but the worse symbol for Bob, the additional “Z” channel effectively degrades Eve's channel for its best symbol at the price of hurting Bob's channel for its worst symbol.

Let $P(V = 1) = q$. With the virtual $V \rightarrow X$ channel, we have

$$P(Y = 1) = q(1 - \gamma)(1 - \delta),$$

and

$$I(V; Y) = H(Y) - H(Y|X) = h(q(1 - \gamma)(1 - \delta)) - qh((1 - \gamma)(1 - \delta)).$$

Similarly,

$$P(Z = 1) = q(1 - \gamma(1 - \delta)) + (1 - q)\delta,$$

and

$$I(V; Z) = H(Z) - H(Z|X) = h(q(1 - \gamma(1 - \delta)) + (1 - q)\delta) - (1 - q)h(\delta) - qh(\gamma(1 - \delta)).$$

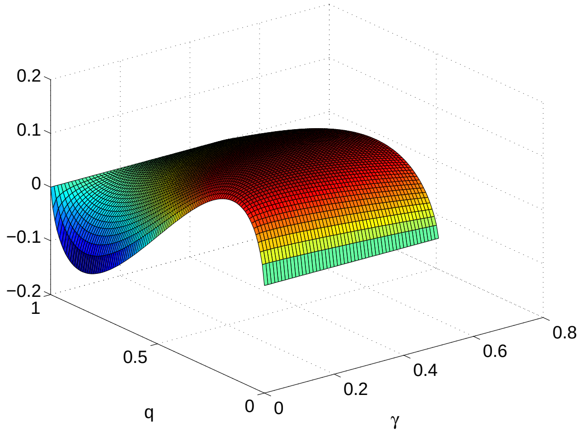
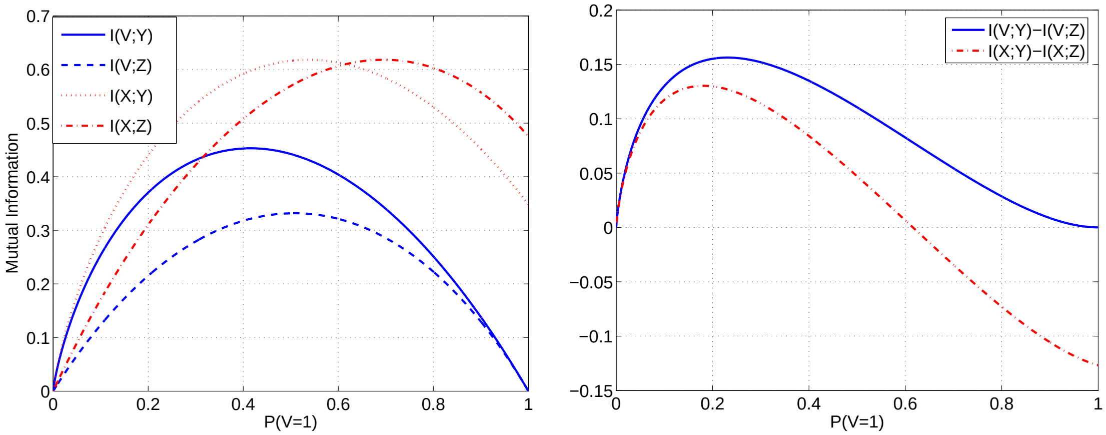


Figure 2.6: $I(V;Y) - I(V;Z)$ as a function of γ and q. $\delta = 0.2$.



(a) (b)

Figure 2.7: (a) $I(V;Y)$, $I(V;Z)$ and the corresponding $I(X;Y)$, $I(X;Z)$, (b) $I(V;Y) - I(V;Z)$ and the corresponding $I(X;Y) - I(X;Z)$ for the binary asymmetric channel $V \to X \to YZ$, with $\delta = 0.2$ and $\gamma = 0.231$. Introducing a virtual channel from V to X enhances the achievable secrecy rate.

Now to maximize the achievable secrecy rate with the help of the auxiliary channel $V \to X$, we would like to solve the following optimization problem:

$$\begin{aligned} &\text{maximize} \qquad I(V;Y) - I(V;Z) \\ &\text{subject to} \qquad 0 \le q \le 1, \quad 0 \le \gamma \le 1. \end{aligned}$$

With the same setting of $\delta = 0.2$, we can plot the objective function $I(V;Y) - I(V;Z)$ as a function of q and the crossover probability γ as in Figure 2.6. Unfortunately, the objective function is not convex with respect to the two parameters. Nevertheless, the maximum value is obtained at a non-zero γ, which indicates that the virtual $V \to X$ channel improves the achievable secrecy rate.

Choosing $\gamma = 0.231$, which produces the largest $I(V;Y) - I(V;Z)$, we can plot $I(V;Y)$ and $I(V;Z)$ as a function of $q = P(V = 1)$ in Figure 2.7(a) along with the corresponding $I(X;Y)$ and $I(X;Z)$. Since varying q from 0 to 1 also changes $P(X = 1)$ from 0 to $1 - \gamma$, $I(X;Y)$ and $I(X;Z)$ have a similar shape as before. We then plot $I(V;Y) - I(V;Z)$ and $I(X;Y) - I(X;Z)$ together in Figure 2.7b. Although $I(V;Y) < I(X;Y)$ and $I(V;Z) < I(X;Z)$, $\max[I(V;Y) - I(V;Z)]$ is greater than $\max[I(X;Y)-I(X;Z)]$. In other words, introducing V with joint probability $P(V, X) = P(V)P(X|V)$ using the above "Z" channel allows a larger secrecy rate.

We note that although one can add a non-zero crossover probability from $V = 0$ to $X = 1$ in the virtual channel, this addition would only hurt the achievable secrecy rate. Intuitively, such addition hurts Bob's channel for its best symbol but Eve's channel for its worst symbol, so that the loss on mutual information is greater for Bob that that for Eve. On the other hand, this "Z" channel is just one possible strategy that allows the secrecy rate to be higher than $\max[I(X;Y) - I(X;Z)]$, and may not be the best one.

As mentioned earlier, it was shown in [15] that if Bob's channel is *more capable* than Eve's channel, the secrecy rate $\mathcal{C}_s$ is achieved with $V = X$. Thus, when Bob has a more capable channel,

$$\mathcal{C}_s = \max_X I(X;Y) - I(X;Z). \tag{2.8}$$

Nevertheless, it remains to find the optimal input X that achieves $\mathcal{C}_s$ for common channels. A fundamental difficulty is that $I(X;Y)$ and $I(X;Z)$ are both concave functions in the input distribution P_X. Thus the difference $I(X;Y)-I(X;Z)$ is, in general, neither concave nor convex in P_X and may have multiple local maxima. In this case, convex optimization procedures are not guaranteed to find the optimal input distribution [11]. We do note that the case that Bob's channel is less noisy than Eve's is an exception since van Dijk [17] has shown that $P_{Y|X}$ is less noisy than $P_{Z|X}$ if and only if $I(X;Y) - I(X;Z)$ is a concave function of P_X.

The memoryless discrete-time AWGN channel is an important example for which the secrecy capacity is known. In this model, at time t, Alice's transmitted signal is X_t and the received signals of Bob and Eve are

$$Y_t = \sqrt{b}X_t + W_{1,t}, \qquad\qquad Z_t = \sqrt{g}X_t + W_{2,t}. \tag{2.9}$$

The independent additive noises $W_{i,t}$ are assumed to have unit variance and b and g represent real link gains normalized by the power spectral density of the additive noise. When $b < g$, we can construct an equivalent system in which Y_t and Z_t have the same conditional marginal distributions but Bob's signal Y_t is a degraded version of Z_t. It follows that $I(X;Y) - I(X;Z) \leq 0$ for all inputs X. In this case, the secrecy capacity is zero, which is achieved by any input X with entropy $H(X) = 0$. When $b > g$, Bob's channel is more capable, and the secrecy capacity is given by (2.8). Here the complication is that while $I(X;Y)$ is maximized under an average power constraint by a Gaussian input X so too is $I(X;Z)$ maximized. Nevertheless, Leung-Yan-Cheong and Hellman [38] verified that a Gaussian input X also maximizes the secret capacity $\mathcal{C}_s$. In this case, $I(X;Y)$ and $I(X;Z)$ are given by AWGN Shannon capacity. Thus, for a real channel, an average power P for the input X yields a secrecy capacity of

$$\mathcal{C}_s^{\text{AWGN}}(b,g,P) = \frac{1}{2}\big(\log\left(1+bP\right) - \log\left(1+gP\right)\big)^+, \tag{2.10}$$

where $(x)^+ = \max(x, 0)$. This result is subject to a quite negative interpretation. First, $b \leq g$ yields zero secrecy capacity. Second, even if Bob's channel is more capable, the capacity is power limited; for arbitrarily large power P, the capacity is upper bounded by

$(1/2)\log(b/g)$, which may be quite small.

The assumptions underlying this pessimism, however, do not reflect the design of modern communications systems, and in particular do not exploit the large number of degrees of freedom available to a modern wireless system. Due to fading and shadowing, channel gains vary significantly across space, frequency and time, and these variations can be exploited for secret communication. For example, it is possible to use multiple subcarriers to provide a large number of parallel subchannels, as is utilized in OFDM transceivers, and the underlying frequency selectivity induced by multipath may provide a diversity advantage [80].

On the other hand, the time-varying wireless channel provides an opportunity for secret communication. For a wiretap channel with additive white Gaussian interference known non-causally to the transmitter, a perfect-secrecy-achieving coding strategy (which is optimal in certain situations) was proposed in [60]. A rate equivocation achievable region for the discrete memoryless wiretap channel with side information was given in [14]. When the broadcast channels are fading, Bob's channel can be better than Eve's at one time but worse at another. Outage calculations for Rayleigh fading channels were performed in [8]. When the fading channel states are known to all parties, the secrecy capacity was derived in [23, 42, 47] and is achievable with Gaussian random codes with optimal power adaptation. When the eavesdropper's channel is unknown but is slow block fading, the secrecy capacity of the channel is derived in [23]. However, an important assumption there is that Eve's channel is constant during each fading block. In [43], we considered the scenario that the Alice→Bob channel is AWGN, while the Alice→Eve channel is Rayleigh fading whose channel statistics (instead of the exact channel realizations) are known to Alice. In particular, Eve's channel randomly changes over each symbol time, or equivalently, the codeword is long enough to see an ergodic realization of Eve's channels. Strategies with Gaussian random coding, additive artificial noise and bursting were discussed. The work showed that a positive secrecy rate is always achievable regardless of whether Bob's channel is worse than Eve's channel on average or not.

Multiple-input Multiple-output (MIMO) systems have been shown to improve the communication rate due to its multiplexing gain. MIMO can facilitate secret communication as well. The secret communication problem for MIMO systems was studied in [26], where it was shown that proper exploitation of space-time diversity at the transmitter can enhance information security and information hiding capabilities. In particular, for information security, Hero showed that when the eavesdropper is uninformed about his channel, the transmitter can enforce a zero information rate to the eavesdropper while delivering a positive information rate to the intended receiver by restricting the space-time modulation to a class of complex transmit matrices whose spatial inner product is a constant matrix. The channel capacity under this perfect secrecy condition, when both the transmitter and the intended receiver have channel information, was derived. The secrecy capacity of single-input multiple-output channel under Gaussian noise was studied in [64] by transforming the channel into scalar wiretap channels. Negi et al. [61, 62] studied secrecy capacity with MIMO channels when artificial noise is injected. They showed that injecting artificial noise in the nullspace of the intended receiver's channel can degrade Eve's channel and allow positive secrecy capacity even when Eve's channel was better before artificial noise injection. Practical schemes for secret transmission with MIMO using randomization were proposed in [39, 40]. In [41], we derived an achievable secrecy rate for MISO systems. A similar result was derived independently in [67]. Results for MIMO channel with two transmit antennas, two receive antennas and one eavesdropping antenna were presented in [66]. The secrecy capacity for the general MIMO systems was derived later by [31, 53, 63], and the capacity for MISO systems coincides with the achievable rate we derived earlier.

Secret communication amongst multiple users has also been an active research field in recent years. In [48], the fading broadcast channel with confidential messages was investigated, where a source node has common information for two receivers (receivers 1 and 2), and has confidential information intended only for receiver 1. The confidential information needs to be kept as secret as possible from receiver 2. The broadcast channel from the source node to receivers 1 and 2 is corrupted by multiplicative fading gain coefficients in addition to additive Gaussian noise terms. The channel state information (CSI) is assumed to be known at both the transmitter and the receivers. The secret capacity region was established for parallel broadcast channels and Gaussian fading channels. The problem of broadcasting information to one or more receivers in the presence of potential eavesdroppers was considered in [30, 32]. The sender might broadcast either a common secret message or independent secret messages to the intended receivers. Upper and lower bounds on the secrecy rate were derived for both cases and the results were also extended to fading channels. The Gaussian broadcast channel with multiple transmitting antennas was studied in [52], where the secrecy capacity region was achieved with dirty paper coding. Besides the broadcast channel, multiple access channels also have received much attention. The achievable secrecy rate regions and outer bounds for multiple access channels with various secrecy requirements were studied in [45, 46, 49, 50, 73, 74].

User cooperation to facilitate secret communication was first proposed in [35], where a four-terminal relay eavesdropper channel was introduced. The achievable rate equivocation region with several cooperation strategies, including decode-and-forward, amplify-and-forward and noise-forward, were discussed and an outer bound on the optimal equivocation region was derived. It was shown that the relay was able to facilitate secret communications while being totally ignorant of the transmitted messages. In [72], using an independent helping interferer to facilitate the secret communication was proposed. A Gaussian example in which the interferer has a better channel to the intended receiver than to the eavesdropper was considered. The interferer can send a (random) codeword at a rate that ensures that it can be decoded and subtracted from the received signal by the intended receiver but cannot be decoded by the eavesdropper. Hence, only the eavesdropper is interfered with and the secrecy level of the confidential message is increased.

It is natural to extend secret communication research to the network scenario, which is often modeled using an interference channel. In interference channel models, multiple transmitter-receiver pairs co-exist in the space. Due to the interference nature of the multiple transmissions, the secrecy capacity depends on the strategy used by each user. Transmissions by one user can create interference that enhances the secrecy afforded to the other user. The secrecy capacity of the two-user interference channels was studied in [49,51]. The concept of robust secrecy capacity was proposed for the interference channel in [85], where robust means secrecy is not harmed by unilateral strategy deviations by the other users, given that the alternative strategy chosen by the other users still guarantee the reliability of all transmissions and secrecy of their own messages. Secrecy without this robust requirement is called semi-secrecy. However, the robust secrecy region for the general interference channel is still elusive. We studied the semi-secrecy capacity region for a class of one-sided interference channels in [44]. The derived secrecy capacity outer bound region was shown to be tight for a class of binary deterministic one-sided channels, and is achievable within a constant gap for a class of Gaussian one-sided channels. More details on these works are provided in Chapter 6.

Chapter 3

Secrecy Capacity of Independent Parallel Channels

Independent parallel channels refer to a class of channels that can be decomposed into multiple independent components. For example, a wide-band frequency selective channel can be decomposed into a number of narrow-band channels, each with a flat frequency magnitude response, and the noise across the channels are independent due to the white noise assumption. This decomposition is the basis of the orthogonal frequency division system (OFDM) communication systems. Mathematically, a system with independent parallel channels has M inputs, denoted as

$$X^M = X_1, \ldots, X_M$$

and M outputs, denoted as

$$Y^M = Y_1, \ldots, Y_M.$$

Moreover, the transition probability can be written as

$$P(Y^M|X^M) = \prod_{m=1}^{M} P(Y_m|X_m). \tag{3.1}$$

Independent parallel channels can also be used to model memoryless fading channels, where the sub-channels are across time instead of frequency as in OFDM.

For the class of additive white Gaussian noise independent parallel scalar channels, the channel model can be written as

$$Y_{i,t} = \sqrt{b_i} X_{i,t} + W_{i,t} \qquad i = 1, \cdots, M \tag{3.2}$$

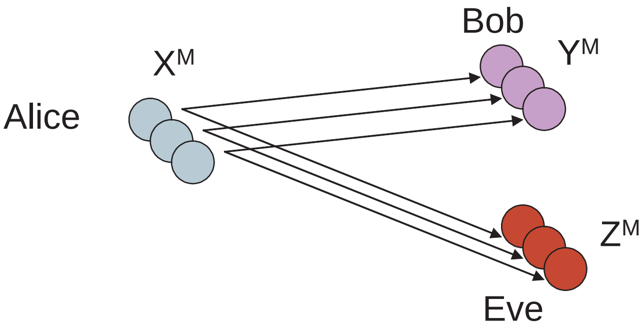


Figure 3.1: The independent parallel channel scenario.

where $W_{i,t}$ is the white Gaussian noise, and b_i is the channel gain for the i-th subchannel. For simplicity of notation, we would omit the time index t for now. The capacity of the AWGN independent parallel channels with an average power constraint P is given by the well-known waterfilling solution [80].

In this chapter, we consider the secrecy capacity of a system composed of independent parallel channels. The system model is described in the next section, followed by the main results in Section 3.2, with the corresponding proof presented in Section 3.5 at the end of this chapter. We show that the secrecy capacity of the system is simply the summation of the secrecy capacities of the individual channels. We further derive the optimal power allocation strategy for a system with parallel AWGN channels subject to a total power constraint. The results can be extended to random fading channels with additive Gaussian noise. Secrecy capacity under various channel conditions and the benefits of the optimal power allocation strategy are evaluated numerically in Section 3.3.

3.1 Problem formulation

Consider a system with M independent parallel subchannels as illustrated in Figure 3.1. Alice's channel input is $X^M = X_1, \ldots, X_M$. Bob and Eve receive $Y^M = Y_1, \ldots, Y_M$ and $Z^M = Z_1, \ldots, Z_M$, respectively. The channel is characterized by the transition probability

$$P(Y^M Z^M | X^M) = \prod_{m=1}^{M} P(Y_m Z_m | X_m). \tag{3.3}$$

Note that Bob's channel $P_{Y^M|X^M}$ is, in general, not more capable than Eve's channel $P_{Z^M|X^M}$. When there exists a subchannel $\hat{m}$ satisfying $I(X_{\hat{m}}; Y_{\hat{m}}) \leq I(X_{\hat{m}}; Z_{\hat{m}})$ for some input $X_{\hat{m}}$, the *more capable* condition is violated. A natural question raised here is what is the secrecy capacity of the system and how to achieve this capacity.

From (2.5), the secrecy capacity of the system is

$$\mathcal{C}_s^M = \max_{V \to X^M \to Y^M Z^M} I(V; Y^M) - I(V; Z^M), \tag{3.4}$$

where V is some auxiliary random variable, and the maximization is over both the distribution of V and the virtual channel from V to X. Since the more capable condition is not satisfied in general, it is not clear what V is optimal. In this work, we show that the system can be decomposed to the sum of each individual channels, thus independent coding in each sub channel is enough to achieve the secrecy capacity. This is analogous to the well-known results on ordinary capacity of independent parallel channels. Our main results are presented in the following subsection.

3.2 Main results

Theorem 3.1 *The secrecy capacity (3.4) of the system with M independent parallel subchannels is given by*

$$\mathcal{C}_s^M = \sum_{m=1}^{M} \max_{V_m \to X_m \to Y_m Z_m} I(V_m; Y_m) - I(V_m; Z_m), \tag{3.5}$$

where V_m is an auxiliary variable designed just for subchannel m.

The method of the proof is essentially the same as that used in [15] to derive a single letter characterization of the secrecy capacity and is presented in the Appendix at the end of this chapter. Theorem 3.1 shows that we can code for each subchannel independently without losing secrecy rate, and thus can choose the optimal V_m for each subchannel independently. The secrecy capacity of the system is simply the summation of the secrecy capacities of the individual subchannels. Note that (3.5) holds for any collection of M independent parallel subchannels, regardless of the model for each subchannel.

When all subchannels are AWGN channels, X^M, Y^M and Z^M satisfy

$$Y_m = \sqrt{b_m} X_m + W_{1,m}, \qquad Z_m = \sqrt{g_m} X_m + W_{2,m}, \qquad m = 1, \ldots, M. \tag{3.6}$$

where m is the channel index, b_m is the normalized gain of Bob's m-th channel , and g_m is the normalized gain of Eve's m-th channel. The power of the Gaussian white noise $W_{1,m}$ and $W_{2,m}$ are normalized to 1. We can represent the normalized channel gains for the Alice-Bob and Alice-Eve subchannels by the vectors $\mathbf{b} = [b_1, \cdots, b_M]^T$ and $\mathbf{g} = [g_1, \cdots, g_M]^T$. For the AWGN case, $b_m \leq g_m$ implies subchannel m has zero secrecy capacity, while $b_m > g_m$ implies Bob has a more capable subchannel, and hence the optimal $V_m = X_m$. Therefore, the secrecy capacity of a system of M orthogonal AWGN channels is

$$\mathcal{C}_s^M = \sum_{\{m | b_m > g_m\}} \max_{X_m \to Y_m Z_m} I(X_m; Y_m) - I(X_m; Z_m), \tag{3.7}$$

where the summation is over all subchannels on which Bob is more capable than Eve. Moreover, because each subchannel is just an AWGN channel, capacity is achieved using a Gaussian input on each subchannel. Thus, a subchannel m with transmit power P_m contributes $\mathcal{C}_s^{\mathrm{AWGN}}(b_m, g_m, P_m)$, given in (2.10), to the secrecy capacity

$$\mathcal{C}_s^M(\mathbf{b}, \mathbf{g}, \mathbf{P}) = \sum_{\{m|b_m > g_m\}} \mathcal{C}_s^{\mathrm{AWGN}}(b_m, g_m, P_m). \tag{3.8}$$

A fundamental question is how $\mathcal{C}_s^M(\mathbf{b}, \mathbf{g}, \mathbf{P})$ depends on the power allocation $\mathbf{P} = [P_1, \cdots, P_M]$, particularly when we are subject to the total power constraint $\sum_{m=1}^M P_m \leq P_{\mathrm{tot}}$. Our second result gives the optimal power allocation $\mathbf{P}$ that maximizes the secrecy capacity under this situation.

Theorem 3.2 *The secrecy capacity of a system of M orthogonal AWGN subchannels, with normalized link gain $\mathbf{b} = [b_1, \cdots, b_M], \mathbf{g} = [g_1, \cdots, g_M]$, and under the total power constraint $\sum_{m=1}^M P_m \leq P_{tot}$ is*

$$\mathcal{C}_s^M(\mathbf{b}, \mathbf{g}, P_{tot}) = \sum_{m=1}^M \mathcal{C}_s^{AWGN}(b_m, g_m, P_{AWGN}(b_m, g_m, \lambda)). \tag{3.9}$$

If $b_m \leq g_m$ for every m, the secrecy capacity is zero regardless of the power allocation strategy. Otherwise, $P_{AWGN}(b_m, g_m, \lambda)$ is given by

$$P_{AWGN}(b, g, \lambda) = \frac{1}{2}\left(f(b, g, \lambda) - (\frac{1}{b} + \frac{1}{g})\right)^+, \tag{3.10}$$

where

$$f(b, g, \lambda) = \sqrt{\left(\frac{1}{b} + \frac{1}{g}\right)^2 + 4\left[\frac{1}{\lambda}\left(\frac{1}{g} - \frac{1}{b}\right) - \frac{1}{gb}\right]}, \tag{3.11}$$

and $\lambda > 0$ is chosen such that we satisfy the total power constraint

$$\sum_{m=1}^M P_{AWGN}(b_m, g_m, \lambda) = P_{tot}. \tag{3.12}$$

The proof uses the well-known Lagrangian method, which gives the optimal power allocation solution here due to the convexity of the AWGN channel secrecy capacity. We note that in the optimal power allocation (3.10), $P_m > 0$ if and only if $b_m - g_m > \lambda$. Since λ is positive, subchannel m will go unused if $b_m \leq g_m$. This is expected as $\mathcal{C}_s^{\text{AWGN}}(b_m, g_m, P_m) = 0$ no matter what power is used when $b_m \leq g_m$. For the subchannels with $b_m > g_m$, they are ranked according to the differences $b_m - g_m$. For very small P_{tot}, only the subchannel with the largest difference is used. As P_{tot} increases, λ decreases and additional subchannels are employed in the order given by $b_m - g_m$. This solution is conceptually similar to the familiar capacity-achieving waterfilling solution in that the power level P_m is determined by the channel parameters and the Lagrange multiplier λ that is used to meet the power constraint. However, in the secrecy capacity power allocation (3.10) the subchannels are ranked not by the gain b_m but rather by the gain differences $b_m - g_m$.

The result above can be extended to the fading channel scenario when the channel realizations are known to all parties. Consider a discrete-time memoryless channel with normalized stationary and ergodic time-varying gains $\sqrt{b_i}$ and $\sqrt{g_i}$ at the ith time unit for Bob and Eve, respectively. For convenience, we use $\gamma_i = (b_i, g_i)$ to denote the joint channel state. The noise is assumed to be AWGN, with unit power spectral density. Let $S(\gamma)$ denote the transmit signal power, and $\bar{S}$ denote the average transmit signal power. Let W denote the received signal bandwidth, which is assumed to be the same for both Bob and Eve. The instantaneous received signal-to-noise ratio (SNR) is then $S(\gamma_i)b_i/W$ and $S(\gamma_i)g_i/W$. Given the knowledge of the channel states, the sequence of fading channels is just a special case of a system of independent parallel channels. With similar methods, we can show the following theorem.

Theorem 3.3 *When the channel side information $\gamma = (b, g)$ is known to all parties, the* *secrecy capacity of a discrete-time memoryless fading channel with additive unit Gaussian noise subject to an average power constraint $\bar{S}$ is*

$$\mathcal{C}_s = \max_{S(\gamma): E_\gamma[S(\gamma)] = \bar{S}} E_\gamma\big[\mathcal{C}_s\big(\gamma, S(\gamma)\big)\big], \tag{3.13}$$

where

$$\mathcal{C}_s\big(\gamma, S(\gamma)\big) = W\left[\log\left(1 + \frac{S(\gamma)b}{W}\right) - \log\left(1 + \frac{S(\gamma)g}{W}\right)\right]. \tag{3.14}$$

The optimal power allocation to achieve the secrecy capacity (3.13) is

$$S^*(\gamma) = \frac{W}{2}\left(f(b,g,\lambda) - (\frac{1}{b} + \frac{1}{g})\right)^+, \tag{3.15}$$

where $f(b,g,\lambda)$ is given by (3.11), and λ is chosen such that the average transmit signal power satisfies the constraint

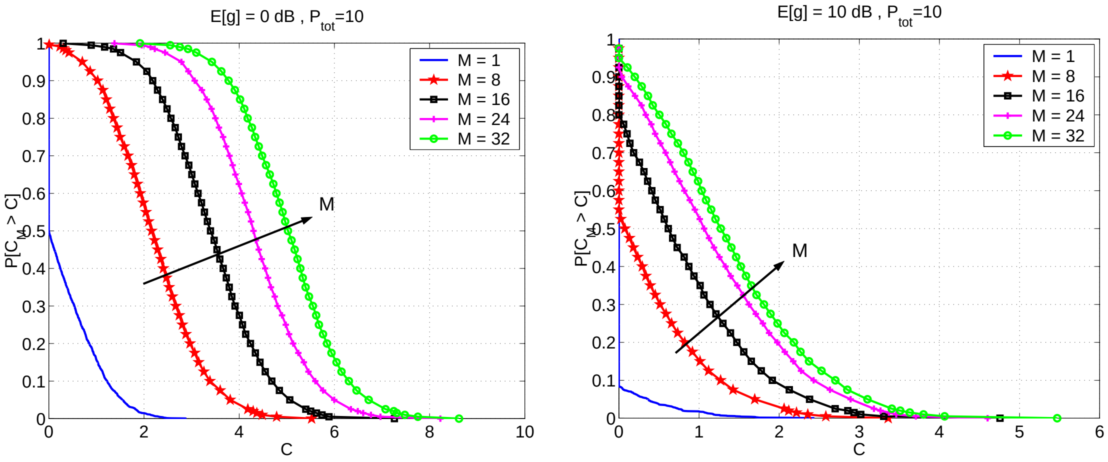
$$E_\gamma[S^*(\gamma)] = \bar{S}. \tag{3.16}$$

Moreover, a single codebook with the dynamic power adaptation (3.15) is sufficient to achieve the secrecy capacity.

Although a multiplexing codebook scheme similar to that proposed in [22] can be deployed to achieve the secrecy capacity (3.13), we show that it is not necessary. Just as in the case of ordinary capacity, a single codebook with optimal power adaptation is sufficient to achieve the capacity [13], it is also enough to achieve the secrecy capacity. The transmitter transmits only when Bob's channel gain is greater than Eve's channel by at least λ, and the transmitted power is adapted to the variation of channel gains.

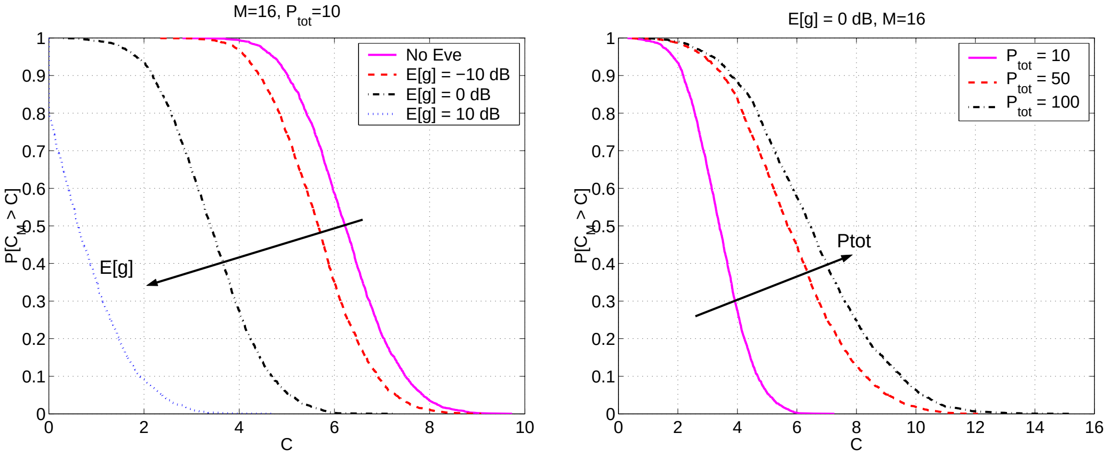
3.3 Numerical evaluation

Our results can be easily applied to an OFDM system with independent Rayleigh fading AWGN subchannels. We start by noting that the secrecy capacity (3.9) is determined by



(a) **(b)**

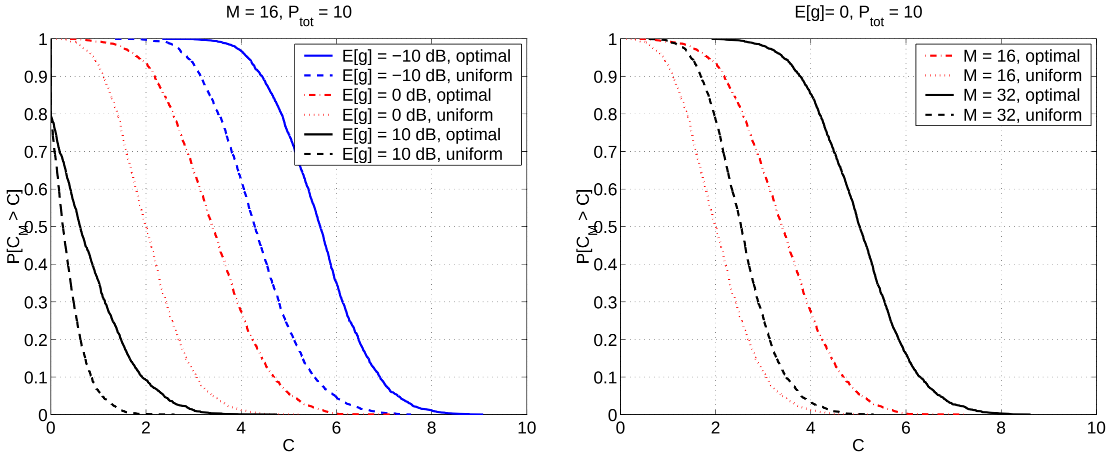
Figure 3.2: Change in the secrecy capacity CCDF versus the number of channels M for (a) $E[g] = 0$ dB, and (b) $E[g] = 10$ dB. We fix $P_{\text{tot}} = 10$ and $E[b] = 1$.



(a) **(b)**

Figure 3.3: Change in the secrecy capacity CCDF versus (a) $E[g]$ for $P_{\text{tot}} = 10$, and (b) P_{tot} for $E[g] = 0$ dB. We fix $M = 16$ and $E[b] = 1$.

M, the total number of channels, Bob and Eve's channel gain vectors $\mathbf{b}$ and $\mathbf{g}$, and the power constraint P_{tot}. In an OFDM system with fixed frequency spacing of subchannels, M will be proportional to the transmission bandwidth. For Rayleigh fading, Bob and Eve's channel gain vectors $\mathbf{b}$ and $\mathbf{g}$ can be modeled as independent random vectors (assuming Bob and Eve are separated by a distance of more than a wavelength) with i.i.d. exponentially



(a) **(b)**

Figure 3.4: Comparison between optimal power allocation and uniform power allocation for (a) varying $E[g]$ with $M = 16$, and (b) varying M with $E[g] = 0$ dB. We fix $P_{\text{tot}} = 10$, and $E[b] = 1$.

distributed components, and is characterized by their mean $E[b]$ and $E[g]$. Therefore, an interesting question is how the secrecy capacity varies with M, $E[b]$, $E[g]$ and P_{tot}. In this section, we will study the effect of these factors on the secrecy capacity through numerical evaluations.

The secrecy capacity depends on the exact channel realizations. For a given set of parameters $\{M, E[b], E[g], P_{\text{tot}}\}$, since channel gains are randomly drawn from their distributions, $\mathcal{C}_s^M$ is a random variable. To characterize the distribution of $\mathcal{C}_s^M$ under each setting, we choose to show its *Complementary Cumulative Distribution Function* (CCDF), i.e. $\Pr\left[\mathcal{C}_s^M > C\right]$ for increasing C, estimated from numerical methods. For simplicity, we fix $E[b] = 1$ for all settings. Let us first look at how the secrecy capacity changes with M. Intuitively, due to the randomness of the channel gains, the larger M is, the more good subchannels Bob may have relative to Eve's subchannels. As a result, the secrecy capacity increases with M. This is illustrated in Figure 3.2 under two levels of $E[g]$. The secrecy rate improvement from the single channel to multiple channels is significant. The intersection of the curve to the vertical axis represents the probability that Bob has at least one subchannel better than Eve, given by [1]

$$1 - \Pr[b \leq g]^M = 1 - \big(E[g]/(E[b] + E[g])\big)^M, \tag{3.17}$$

which increases rapidly with M. The improvement gets smaller as M gets larger because the total power is fixed. Even though more good channels are available as M increases, only a few best are used due to the power limitation.

The change in secrecy capacity with the average Alice-Eve channel gain is plotted in Figure 3.3(a). As Eve's channel gets better on average, the secrecy capacity becomes smaller. For comparison purposes, the ordinary non-secure capacity is also plotted in the same figure. Obviously, this is an upper bound to the secrecy capacity. We note that if Eve's channel is significantly worse than Bob's channel on average, the capacity reduction due to the secrecy requirement is quite small. This is as expected, since as $E[\mathbf{g}] \rightarrow 0$, we should approach the ordinary capacity. Moreover, even when Eve's channel is much better on average, we can still obtain positive secrecy capacity because of the availability of multiple independent random channels. We also plot the change in secrecy capacity versus the total power in Figure 3.3(b). Larger power budget improves the secrecy capacity, but will not cause an unbounded increase because the secrecy capacity of each subchannel is upper bounded by $1/2\log(b_m/g_m)$ no matter how large the power is.

To assess the benefits of the optimal power allocation, we can compare against the non-adaptive uniform power allocation $\mathbf{P} = \overline{\mathbf{P}} = (P_{\text{tot}}/M)[1, \cdots, 1]$. This uniform allocation yields the secrecy rate

$$\mathcal{C}_s^M(\mathbf{b}, \mathbf{g}, \overline{\mathbf{P}}) = \sum_{m=1}^{M} \mathcal{C}_s^{\text{AWGN}}(b_m, g_m, P_{\text{tot}}/M). \tag{3.18}$$

[1] A similar derivation is provided by J. Barros and M. R. D. Rodrigues in [8].

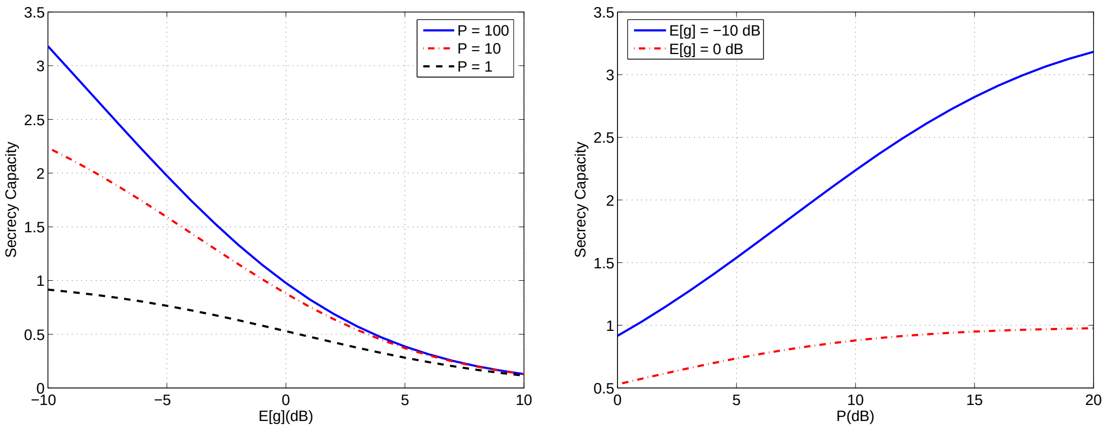
The uniform power allocation forfeits power when a subchannel is bad; however, it does take advantage of good (for secrecy capacity) subchannels. In addition, the uniform power allocation is easy to analyze since it is a sum of M independent random variables. With the approximation of $\log(1+x) \approx x/\ln 2$ for small x, we can derive from (3.18) and (2.10) that

$$\lim_{M\to\infty} \mathcal{C}_s^M(\mathbf{b},\mathbf{g},\overline{\mathbf{P}}) = \frac{P_{\text{tot}}}{2\ln 2} E[(b-g)^+] \tag{3.19}$$

$$= \frac{P_{\text{tot}}}{2\ln 2} \frac{E[b]^2}{(E[b]+E[g])} \tag{3.20}$$

for the uniform power allocation. The secrecy capacity with the optimal power allocation and the non-adaptive uniform power allocation are compared in Figure 3.4. The result shows that there is a significant capacity loss due to the non-optimal power allocation. The penalty becomes increasingly severe as M increases. Thus, optimal power allocation is crucial for fully exploiting the advantage brought by multiple random channels when the power budget is tight. On the other hand, the benefits of the simpler power allocation may be overstated. The fundamental binning code method of Csiszár and Körner [15] demands knowledge of the channel states. If this requirement is unavoidable, then the residual complexity of channel-dependent codebooks will likely outweigh any complexity reduction associated with uniform power allocation. Moreover, OFDM channels become increasingly difficult to estimate as the average power per subchannel P_{tot}/M goes to zero. For traditional data communication, these same issues are addressed in [58, 77, 81, 82].

We also evaluated the secrecy capacity for the Rayleigh fading channels with the optimal power allocation. Figure 3.5(a) shows how the secrecy capacity in bits per channel use varies with the average eavesdropper's channel gain at several average power levels P. Bob's average channel gain is always fixed at 1. Figure 3.5(b) shows how the secrecy capacity



(a) **(b)**

Figure 3.5: Change in the secrecy capacity with (a) $E[g]$ for different P, and (b) P for different $E[g]$. $E[b] = 1$.

increases with the average power at two levels for the average eavesdropper's channel gain. When the eavesdropper's channel is good, the secrecy capacity is mainly limited by the channel conditions, and increasing power would not increase the secrecy capacity very much. Nevertheless, unlike the constant AWGN channel, fading allows a positive probability that an instantaneous realization of Bob's channel is better than that of Eve's, so that secret communication is still possible even when eavesdropper's channel is on average better. When the eavesdropper's channel is bad, the secrecy capacity is mainly power limited, and significant secrecy rate can be achieved with 20dB SNR for Bob.

3.4 Discussion

In this work, we derived the secrecy capacity of a system consisting of multiple independent parallel channels. We show that the secrecy capacity of the system is simply the summation of the secrecy capacities of the individual channels. We further derive the optimal power allocation strategy for a system with parallel AWGN channels subject to a total power constraint, and also extend the results to random fading channels with additive Gaussian noise. Secrecy capacity was evaluated numerically for OFDM system and Rayleigh fading channels, which shows that the diversity, either in frequency or in time, improves the rate of secret communication and allow secret communication even when the eavesdropper's channel is better on average.

In this work, we assume that the transmitter knows both Bob's channel and Eve's channel. This assumption is impractical if Eve is an adversary that the transmitter is not even aware of or has no idea on its channel state. However, consider a scenario with one transmitter and two receivers, as shown in Figure 3.6. All users belong to the same network and do communicate with each other. The transmitter wants to convey individual secret information to each of the receiver without leaking information to the non-intended receiver, who can overhear the communication. Then, the assumption that all parties know the channel state information is valid since both receivers are legitimate members of the network. The results in this chapter can be applied when the channels are composed of independent parallel channels. In particular, to convey message to both receivers secretly, the transmitter will check all subchannels, and use the subchannels that receiver 1 is better to convey secret information to receiver 1, and use the rest subchannels for receiver 2. Then, the transmitter can do independent coding for each subchannel without hurting the secrecy rate, and do optimal power allocation among the subchannels. Note that the optimal power allocation will depend on both the objective function, i.e. the weighted sum rate, and the channel realizations. Some subchannel might end up unused under the optimal power allocation. This model is one example of secure broadcast channel, and more results on secure broadcasting with various settings can be found in [30, 52].

The decomposition of the system into subchannels with independent coding is valid only with a single eavesdropper, and cannot be directly extended to the multiple receiver case. In

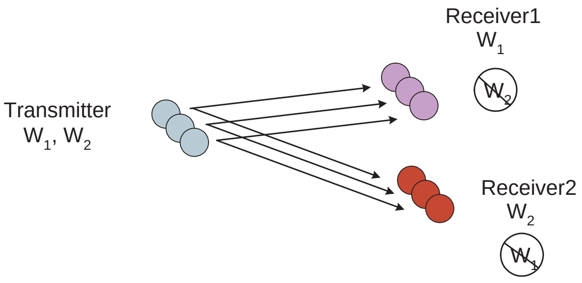


Figure 3.6: The independent parallel broadcast channel scenario.

other words, when there are multiple eavesdroppers, independent coding across subchannels are likely to be non-optimal. To see this, we can look at a simple binary channel example

$$Y = \begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix} = \begin{bmatrix} X_1 \\ X_2 \end{bmatrix} \tag{3.21}$$

$$Z^1 = X_1 \tag{3.22}$$

$$Z^2 = X_2, \tag{3.23}$$

where there are two independent 1-bit channels, and two eavesdroppers. The intended receiver gets both bits perfectly, while eavesdropper 1 gets first bit perfectly, and eavesdropper 2 gets the second bit perfectly. With independent coding, no secrecy can be achieved for the intended receiver. However, with X_1 be random binary noise, while $X_2 = W + X_1$, the intended receiver can get the information bit perfectly by doing $\hat{W} = Y_1 + Y_2 = W$, while the eavesdropper gets no information by observing X_1 or X_2 but not both. Clearly, $R = 1$ is also the secrecy capacity of the system. So joint coding might be necessary in presence of multiple non-colluding eavesdroppers.

3.5 Proof

Proof: Theorem 1

We follow the method used in [15] to derive a single-letter characterization in the secrecy capacity converse. Denote $Y^m = Y_1 \cdots Y_m$, and $Z_m^M = Z_m \cdots Z_M$. From the chain rule, we can write

$$I(V;Y^M) - I(V;Z^M) = \sum_{m=1}^{M} I(V;Y_m|Y^{m-1}) - \sum_{m=1}^{M} I(V;Z_m|Z_{m+1}^M). \tag{3.24}$$

Moreover, we can obtain

$$\begin{aligned}
I(V;Y_m|Y^{m-1}) &= H(Y_m|Y^{m-1}) - H(Y_m|VY^{m-1}) && (3.25)\\
&= H(Y_m|Y^{m-1}) - H(Y_m|VY^{m-1}Z_{m+1}^M) + H(Y_m|VY^{m-1}Z_{m+1}^M)\\
&\quad - H(Y_m|VY^{m-1}) && (3.26)\\
&= I(VZ_{m+1}^M;Y_m|Y^{m-1}) - I(Z_{m+1}^M;Y_m|VY^{m-1}) && (3.27)\\
&= I(Z_{m+1}^M;Y_m|Y^{m-1}) + I(V;Y_m|Y^{m-1}Z_{m+1}^M)\\
&\quad - I(Z_{m+1}^M;Y_m|VY^{m-1}) && (3.28)\\
&= \sum_{j=m+1}^{M} I(Z_j;Y_m|Y^{m-1}Z_{j+1}^M) + I(V;Y_m|Y^{m-1}Z_{m+1}^M)\\
&\quad - \sum_{j=m+1}^{M} I(Z_j;Y_m|VY^{m-1}Z_{j+1}^M). && (3.29)
\end{aligned}$$

Similarly,

$$\begin{aligned}
I(V;Z_m|Z_{m+1}^M) &= H(Z_m|Z_{m+1}^M) - H(Z_m|VZ_{m+1}^M) && (3.30)\\
&= H(Z_m|Z_{m+1}^M) - H(Z_m|VY^{m-1}Z_{m+1}^M)\\
&\quad + H(Z_m|VY^{m-1}Z_{m+1}^M) - H(Z_m|VZ_{m+1}^M) && (3.31)\\
&= I(VY^{m-1};Z_m|Z_{m+1}^M) - I(Y^{m-1};Z_m|VZ_{m+1}^M) && (3.32)\\
&= I(Y^{m-1};Z_m|Z_{m+1}^M) + I(V;Z_m|Y^{m-1}Z_{m+1}^M)\\
&\quad - I(Y^{m-1};Z_m|VZ_{m+1}^M) && (3.33)
\end{aligned}$$

With the chain rule, we can further write

$$I(V;Z_m|Z_{m+1}^M) = \sum_{j=1}^{m-1} I(Y_j;Z_m|Z_{m+1}^M Y^{j-1}) \\ + I(V;Z_m|Y^{m-1}Z_{m+1}^M) - \sum_{j=1}^{m-1} I(Y_j;Z_m|VZ_{m+1}^M Y^{j-1}). \tag{3.34}$$

Note that

$$\sum_{m=1}^{M}\sum_{j=m+1}^{M} I(Z_j;Y_m|Y^{m-1}Z_{j+1}^M) = \sum_{m=1}^{M}\sum_{j=1}^{m-1} I(Y_j;Z_m|Z_{m+1}^M Y^{j-1}) \tag{3.35}$$

and

$$\sum_{m=1}^{M}\sum_{j=m+1}^{M} I(Z_j;Y_m|VY^{m-1}Z_{j+1}^M) = \sum_{m=1}^{M}\sum_{j=1}^{m-1} I(Y_j;Z_m|VZ_{m+1}^M Y^{j-1}). \tag{3.36}$$

Combining (3.24) to (3.36), we get

$$I(V;Y^M) - I(V;Z^M) = \sum_{m=1}^{M} I(V;Y_m|Y^{m-1}) - \sum_{m=1}^{M} I(V;Z_m|Z_{m+1}^M) \tag{3.37}$$

$$= \sum_{m=1}^{M} [I(V;Y_m|Y^{m-1}Z_{m+1}^M) - I(V;Z_m|Y^{m-1}Z_{m+1}^M)]. \tag{3.38}$$

Denote $U_m = Y^{m-1}Z_{m+1}^M$, $\hat{V}_m = VU_m$, then

$$I(V;Y^M) - I(V;Z^M) = \sum_{m=1}^{M} [I(V;Y_m|U_m) - I(V;Z_m|U_m)] \tag{3.39}$$

$$= \sum_{m=1}^{M} [I(VU_m;Y_m|U_m) - I(VU_m;Z_m|U_m)] \tag{3.40}$$

$$= \sum_{m=1}^{M} [I(\hat{V}_m;Y_m|U_m) - I(\hat{V}_m;Z_m|U_m)] \tag{3.41}$$

$$\leq \sum_{m=1}^{M} \max_{\hat{V}_m \to X_m \to Y_m Z_m} [I(\hat{V}_m;Y_m) - I(\hat{V}_m;Z_m)]. \tag{3.42}$$

Note that the term inside the sum is just the secrecy capacity of each parallel independent channel, thus is achievable. The equality holds if and only if each channel achieves its individual secrecy capacity. □

Proof: Theorem 2

To prove Theorem 2, we need to resort to the secrecy capacity results for AWGN channels, as characterized by (2.10). We observe that if $b_m \leq g_m$, channel m will go unused since its secrecy capacity is zero, and no power will be allocated to this channel. Thus we can simplify the subsequent proof by assuming that channels $1, \cdots, \bar{M}$ satisfy $b_m > g_m$, and only consider the power allocation to these channels. In this case, it is easily verified that $b_m > g_m$ implies $\mathcal{C}_s^{\text{AWGN}}(b_m, g_m, P_m)$ is concave in P_m. In terms of the vector $\mathbf{P} = [P_1 \cdots P_{\bar{M}}]^T$, we use (2.10) and form the Lagrangian

$$\mathcal{L}(\lambda, \mathbf{P}) = \sum_{m=1}^{\bar{M}} [\log(1 + b_m P_m) - \log(1 + g_m P_m) - \lambda P_m], \tag{3.43}$$

where $\lambda > 0$. Maximization of the Lagrangian requires that $\partial\mathcal{L}/\partial P_m = 0$ if $P_m > 0$ or $\partial\mathcal{L}/\partial P_m \leq 0$ if $P_m = 0$. This implies that the nonzero P_m satisfy the quadratic equation

$$\left(P_m + \frac{1}{g_m}\right)\left(P_m + \frac{1}{b_m}\right) - \frac{1}{\lambda}\left(\frac{1}{g_m} - \frac{1}{b_m}\right) = 0. \tag{3.44}$$

We can solve for non-negative P_m and express the general solution as $P_m = P_{\text{AWGN}}(b_m, g_m, \lambda)$ described by (3.10). It follows that $P_m > 0$ if and only if $b_m - g_m > \lambda$. The Lagrange multiplier λ is chosen so that the power constraint is met. Since (3.10) already implies that $P_{\text{AWGN}}(b, g, \lambda) = 0$ for $b \leq g$, we have proved Theorem 2 for a general system with M independent parallel AWGN channels. □

Proof: Theorem 3

We will prove the converse of the theorem first, and show the achievability afterwards.

Denote $W \in \{1, \cdots, 2^{nR}\}$ as the secret message index. To prove the converse, we note that

$$
\begin{aligned}
nR &= H(W|\gamma^n) && (3.45)\\
&\leq H(W|Z^n,\gamma^n)+\epsilon && (3.46)\\
&= H(W|Y^n,\gamma^n)+I(W;Y^n|\gamma^n)-I(W;Z^n|\gamma^n)+\epsilon && (3.47)\\
&\leq I(W;Y^n|\gamma^n)-I(W;Z^n|\gamma^n)+\eta+\epsilon, && (3.48)
\end{aligned}
$$

where (3.46) is due to the perfect secrecy requirement and (3.48) is due to the capacity requirement.

Using the same method as in proof for Theorem 1, we can show that

$$
\begin{aligned}
I(W;Y^n|\gamma^n)-I(W;Z^n|\gamma^n) &= \sum_{i=1}^{n}\big(I(W;Y_i|U_i,\gamma^n)-I(W;Z_i|U_i,\gamma^n)\big) && (3.49)\\
&= \sum_{i=1}^{n}\big(I(V_i;Y_i|U_i,\gamma^n)-I(V_i;Z_i|U_i,\gamma^n)\big) && (3.50)\\
&\leq \sum_{i=1}^{n}\max_{V_i\to X_i\to Y_iZ_i}\big(I(V_i;Y_i|\gamma_i)-I(V_i;Z_i|\gamma_i)\big) && (3.51)
\end{aligned}
$$

Since the channel at time i is an AWGN channel with unit noise for a given γ_i, we can write

$$
\max_{V_i\to X_i\to Y_iZ_i} I(V_i;Y_i|\gamma_i)-I(V_i;Z_i|\gamma_i)=\mathcal{C}_s\big(\gamma_i,S(\gamma_i)\big), \qquad (3.52)
$$

where $\mathcal{C}_s\big(\gamma,S(\gamma)\big)$ is the secrecy capacity for channel with gain γ and power $S(\gamma)$, and is given by (3.14).

Assume that the channel state is a discrete random variable, perhaps derived from quantization of a continuous channel state, and takes values from $\{\gamma_1,\cdots,\gamma_M\}$. Denote N_m to be the number of appearance that $\gamma=\gamma_m$ during the n transmissions, we then have

$$
\begin{aligned}
I(W;Y^n|\gamma^n)-I(W;Z^n|\gamma^n) &\leq \sum_{i=1}^{n}\mathcal{C}_s\big(\gamma_i,S(\gamma_i)\big) && (3.53)\\
&= \sum_{m=1}^{M}\mathcal{C}_s\big(\gamma_m,S(\gamma_m)\big)N_m. && (3.54)
\end{aligned}
$$

Combining all above, we see that

$$R \le \frac{1}{n}\big(I(W;Y^n|\gamma^n) - I(W;Z^n|\gamma^n) + \eta + \epsilon\big), \tag{3.55}$$

$$\le \sum_{m=1}^{M} \mathcal{C}_s\big(\gamma_m, S(\gamma_m)\big)\frac{N_m}{n} + \frac{\eta}{n} + \frac{\epsilon}{n}. \tag{3.56}$$

As n increases, N_m/n approaches $p(\gamma_m)$, implying

$$R \le E_\gamma\big[\mathcal{C}_s\big(\gamma, S(\gamma)\big)\big] + \frac{\eta}{n} + \frac{\epsilon}{n}. \tag{3.57}$$

Maximizing the right hand side over $S(\gamma)$ subject to the average power constraint using the method in the proof of Theorem 2, we get the optimal power allocation (3.15). This completes the converse for Theorem 3.3.

As for the achievability, we note that a multiplexing codebook scheme similar to that proposed in [22] can achieve the secrecy rate $E_\gamma\big[\mathcal{C}_s\big(\gamma, S(\gamma)\big)\big]$. Combining with (3.57), this ends the proof of (3.13). On the other hand, using similar arguments as in [13], we can show that a multiplexing codebook is actually not necessary, as detailed below.

Suppose Alice chooses $X = \tilde{S}(\gamma)V$, where $\tilde{S}(\gamma)$ is a power function adapted to the channel state γ, and V is a unit power Gaussian random variable independent of γ. In this case, Bob receives

$$Y = \sqrt{b}\tilde{S}(\gamma)V + W_1, \tag{3.58}$$

and Eve receives

$$Z = \sqrt{g}\tilde{S}(\gamma)V + W_2. \tag{3.59}$$

Since all parties know γ and in turn $\tilde{S}(\gamma)$, we can consider the random channel state Γ as an output of the channel. Thus, with the coding procedure in [15], a single codebook can be used to achieve the secrecy rate of

$$I(V;Y\Gamma) - I(V;Z\Gamma) = I(V;Y|\Gamma) - I(V;Z|\Gamma) \tag{3.60}$$

$$= E_\gamma\big[\mathcal{C}_s\big(\gamma, \tilde{S}(\gamma)\big)\big]. \tag{3.61}$$

When $\tilde{S}(\gamma) = S^*(\gamma)$, the optimum power allocation strategy, we achieve the secrecy capacity (3.13). □

Chapter 4

Ergodic Secrecy Rate of Rayleigh Fading Channels

In the previous chapter, we studied the secrecy capacity of fading channels when the channel states are known at all parties. In the scenarios where the eavesdropper's instantaneous channel realization is not known, but only the channel statistics are known to the transmitter, the optimal power allocation derived in previous chapter does not apply. It is interesting to study the achievable secrecy rate in such cases, which is the topic of this chapter.

When the eavesdropper's channel is unknown but is slow block fading, the secrecy capacity of the channel is derived in [23]. However, an important assumption there is that Eve's channel is constant during each fading block, and each fading block is long enough for sending Gaussian codes with almost zero error probability. With this assumption, a two-tier coding scheme is proposed which contains a sub-codebook used for each fading block, and a super-codebook across an ergodic realization of fading blocks. The key is that for each fading block, the eavesdropper cannot get more information on what has been sent than the intended receiver. In this work, we consider the situation when the block fading assumption does not hold. In particular, Eve's channel randomly changes over each symbol time, while Bob's channel is a constant AWGN channel. Note that although in this model the main channel has a constant gain, not the more general fading gain, it is clear that the latter is a temporal concatenation of our simple model with various main channel gains. Thus, power allocation over time can be used to obtain secrecy rates of the more general model with fading on both the main channel and the eavesdropper's channel, and the main channel state known by Bob. On the other hand, although our channel model is simple, as we will show later that it already exhibits some intriguing behavior. Moreover, an optimal solution for this channel remains elusive.

4.1 Problem formulation

In this chapter, we consider the situation when Bob's channel is an AWGN channel with a fixed SNR, while Eve has a Rayleigh fading channel with the channel statistics (not the realizations) known to the other parties. Mathematically,

$$Y_i = \sqrt{\tilde{b}}\tilde{X}_i + W_{1,i}, \tag{4.1a}$$

$$Z_i = \sqrt{\tilde{G}_i}\tilde{X}_i + W_{2,i}, \tag{4.1b}$$

where i is the time index, $W_{1,i}, W_{2,i}$ are independent white Gaussian noise with normalized variance 1, and $\tilde{b}$ is the constant channel gain for Bob. Eve's time varying channel gain $\tilde{G}_i$ is an exponential random variable due to the Rayleigh fading model, and is perfectly observable by Eve. Alice knows Eve's average channel gain $\bar{G}$, but not the exact realization. This is the major difference of the current model from the one studied in last chapter. By making these assumptions, we have considered a quite powerful adversarial model as Eve has a more complete information of the system.

We can further normalize the channel gain of Bob by the average channel gain of Eve through the transformation

$$Y_i = \sqrt{\tilde{b}/\bar{G}}\sqrt{\bar{G}}\tilde{X}_i + W_{1,i} \tag{4.2a}$$

$$Z_i = \sqrt{\tilde{G}_i/\bar{G}}\sqrt{\bar{G}}\tilde{X}_i + W_{2,i}. \tag{4.2b}$$

Define $b = \tilde{b}/\bar{G}$ and $G_i = \tilde{G}_i/\bar{G}$, then we have the simplified channel model

$$Y_i = \sqrt{b}X_i + W_{1,i}, \tag{4.3a}$$

$$Z_i = \sqrt{G_i}X_i + W_{2,i}. \tag{4.3b}$$

Now, the normalized channel gain G_i follows exponential distribution with mean 1 and b is the relative gain of Bob against Eve, and the signal power is scaled by $\bar{G}$. From now on, we will use this model, and refer b as Bob's channel gain, and $P = E\big[X_i^2\big]$ as the average power of X.

If we consider the random channel observation G_i at Eve as an output, Eve's channel is equivalent to a channel with output (G, Z) and the channel transition probability is $\Pr(GZ|X) = \Pr(G)\Pr(Z|XG)$. Following Csiszár and Körner's arguments [15], the secrecy capacity of the channel model (4.3)is

$$\mathcal{C}_s = \max_{V \to X \to YGZ} I(V;Y) - I(V;GZ) \tag{4.4}$$

$$= \max_{V \to X \to YGZ} I(V;Y) - I(V;G) - I(V;Z|G) \tag{4.5}$$

$$= \max_{V \to X \to YGZ} I(V;Y) - I(V;Z|G), \tag{4.6}$$

where (4.6) follows from the independence of V and G since Alice does not know G and cannot choose V according to G. This channel does not satisfy the more capable condition, and it appears to be hard to obtain the optimal V and $P(X|V)$. Instead, in this work, we study the achievable secrecy rates that are possible with random Gaussian codes as this is a natural approach for attacking the problem. The main result of this work is that with Gaussian random codes, artificial noise injection and power bursting, positive secrecy rate is achievable even when Bob' channel is arbitrarily worse than Eve's average channel.

4.2 Achievable secrecy rates

4.2.1 Gaussian random codes with constant power

First, we assume the use of Gaussian random codes with a constant power P. We also assume that no auxiliary random variable is used, or equivalently, $X = V$. With these two simplifications, we can achieve the secrecy rate

$$\mathcal{R}_x(P,b) = I(X;Y) - I(X;Z|G) \tag{4.7}$$

$$= \log(1+bP) - E\big[\log(1+GP)\big], \tag{4.8}$$

where E denotes the expectation over the unit mean exponential random variable g. To simplify the subsequent analysis, we employ the natural log and use nats per channel use as our units. Note that $\mathcal{R}_x(P,b)$ can be negative, which means that simple Gaussian signaling with power P can not achieve positive rate, and the achievable secrecy rate is zero. However, we will allow the negative $\mathcal{R}_x(b,P)$ since it is useful to the scheme proposed in next subsection. Also, since we view $\mathcal{R}_x(P,b)$ as a function of P for fixed b, we remove b from the parameter list from now on to simplify the notation.

We can calculate the second term in (4.8) as

$$E\big[\log(1+GP)\big] = \int_0^\infty \log(1+GP)\exp(-G)dG \tag{4.9}$$

$$= \int_0^\infty e^{-G}\left(\log(G+1/P) + \log(P)\right)dG \tag{4.10}$$

$$= \int_{1/P}^\infty e^{-t}\log t\, dt \cdot e^{1/P} + \log(P). \tag{4.11}$$

Note that

$$\int_{1/P}^\infty e^{-t}\log t dt = -e^{-t}\log t|_{1/P}^\infty + \int_{1/P}^\infty \frac{e^{-t}}{t}dt \tag{4.12}$$

$$= e^{-1/P}\log(1/P) + E_1(1/P), \tag{4.13}$$

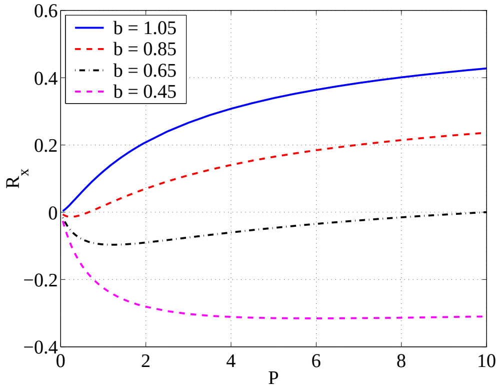


Figure 4.1: The secrecy rate $\mathcal{R}_x(P)$ of (4.17) versus power P at different levels of b.

where $E_1(x)$, the En-function for $n = 1$, is given by

$$E_1(x) = \int_x^\infty \frac{e^{-t}}{t} dt = \int_1^\infty \frac{e^{-xt}}{t} dt \tag{4.14}$$

$$= -\gamma - \ln(x) - \sum_{n=1}^{\infty} \frac{(-1)^n x^n}{n!n}, \tag{4.15}$$

and $\gamma = 0.57721566\cdots$ is the Euler-Mascheroni constant. More detail on the En-function and Euler-Mascheroni constant can be found in [1, 2, 70]. Substituting (4.13) into (4.11) , we obtain

$$E\big[\log(1 + GP)\big] = e^{1/P} E_1(1/P). \tag{4.16}$$

Therefore, we can write

$$\mathcal{R}_x(P) = \log(1 + bP) - e^{1/P} E_1(1/P). \tag{4.17}$$

Evaluating $\mathcal{R}_x(P)$, we can see how the secrecy rate changes with P at different levels of b, as shown in Figure 4.1. Clearly, the shape of the curve is strongly affected by b and is not always concave.

We observe from (4.8) that $\mathcal{R}_x(P) > 0$ if and only if the main channel SNR satisfies

$$b > \frac{1}{P}\big(e^{E\left[\log(1+GP)\right]} - 1\big) \triangleq f_{pos}(P). \tag{4.18}$$

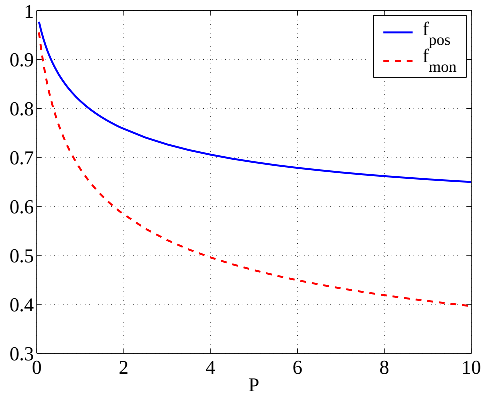


Figure 4.2: $f_{pos}(P)$ defined in (4.18) and $f_{mon}(P)$ defined in (4.28).

We plot $f_{pos}(P)$ with P as the solid line in Figure 4.2. Note that due to the concavity of the log function, an upper bound on $f_{pos}(P)$ is given by

$$f_{pos}(P) \leq \frac{1}{P}\big(e^{\log(1+E[G]P)} - 1\big) = 1. \tag{4.19}$$

Moreover, it can be shown that $\lim_{P\to 0} f_{pos}(P) = 1$ and that $f_{pos}(P)$ decreases monotonically with power P. In addition, we can calculate the minimum of $f_{pos}(P)$ as

$$\begin{aligned}
\lim_{P\to\infty} f_{pos}(P) &= \lim_{P\to\infty} \frac{e^{E\big[\log(1+GP)\big]}}{P} && (4.20)\\
&= \lim_{P\to\infty} \exp\big(E\big[\log(1+GP) - \log(P)\big]\big) && (4.21)\\
&= \lim_{P\to\infty} \exp\left(E\big[\log(\frac{1}{P} + G)\big]\right) && (4.22)\\
&= \lim_{P\to\infty} \exp\Big(\int_0^\infty e^{-G}\log(\frac{1}{P} + G)\, dG\Big) && (4.23)\\
&= \lim_{P\to\infty} \exp\Big(e^{1/P}\int_{1/P}^\infty e^{-t}\log t\, dt\Big) && (4.24)\\
&= e^{-\gamma} \approx 0.56146, && (4.25)
\end{aligned}$$

where we used the substitution $t = G + 1/P$ and the property of the Euler-Mascheroni constant $\gamma = -\int_0^\infty e^{-t}\log t\, dt$.

The result above implies that if Bob's relative channel gain b is less than 0.56146, Alice cannot achieve positive secrecy rate with simple random Gaussian codes, no matter how large P is.

Because (4.8) is essential to our analysis later on, we will look at its properties in more detail. Let us look at its first derivative with respect to P to see whether the secrecy rate increases with P monotonically.

$$\mathcal{R}_x'(P) = \frac{b}{(1+bP)} - E\big[\frac{G}{1+GP}\big] \tag{4.26}$$

$$= \frac{1}{(1+bP)} E\big[\frac{b-G}{1+GP}\big]. \tag{4.27}$$

This implies that $\mathcal{R}_x'(P) > 0$ if and only if

$$b > \frac{E\big[G/(1+GP)\big]}{E\big[1/(1+GP)\big]} \triangleq f_{mon}(P). \tag{4.28}$$

It's easy to see that $\lim_{P\to 0} f_{mon}(P) = E[G] = 1$. From (4.16), an alternative representation of $f_{mon}(P)$ can be found to be

$$f_{mon}(P) = \frac{1}{e^{1/P}E_1(1/P)} - \frac{1}{P}. \tag{4.29}$$

Evaluating $f_{mon}(P)$, we obtain the dashed line in Figure 4.2, which shows that $f_{mon}(P)$ decreases monotonically with P. In particular, (4.29) implies $\lim_{P\to\infty} f_{mon}(P) = 0$. Thus, for $b \in (0,1)$, we can find $P_0(b) = f_{mon}^{-1}(b)$ as the value of P that minimizes $\mathcal{R}_x(P)$. The secrecy rate (4.8) decreases in P monotonically for $P < P_0(b)$, and increases for $P > P_0(b)$. Since the minimum value is always non-positive here, $f_{mon}(P) \leq f_{pos}(P)$, with equality if and only if $P = 0$. For $b \geq 1$, the secrecy rate (4.8) increases with P monotonically.

4.2.2 Constant power transmission with noise injection

The previous scheme is simple, but cannot obtain positive secrecy rate when $b < e^{-\gamma}$. Can we do better for the case with small b? Recall that the auxiliary random variable V and the virtual $V \to X$ channel can be used to confuse Eve. A simple virtual channel is the AWGN channel $X = V + W$, where W is an artificial additive noise. The idea of adding artificial noise for secrecy is not completely new, and was explored in [62], in the context of a multiple antenna system in which the noise is chosen to be orthogonal to the information bearing signal. In our case, it follows from (4.3) that AWGN $V \to X$ channel yields the $V \to YZ$ channel

$$Y_i = \sqrt{b}V_i + \sqrt{b}W_i + W_{1,i}, \tag{4.30a}$$

$$Z_i = \sqrt{G_i}V_i + \sqrt{G_i}W_i + W_{2,i}. \tag{4.30b}$$

We assume V and W are independent Gaussian random variables with mean 0 and variance P_v and P_w respectively. The transmit power constraint becomes $P_x = P_v + P_w \leq P$.

The secrecy rate achieved by this modified channel is

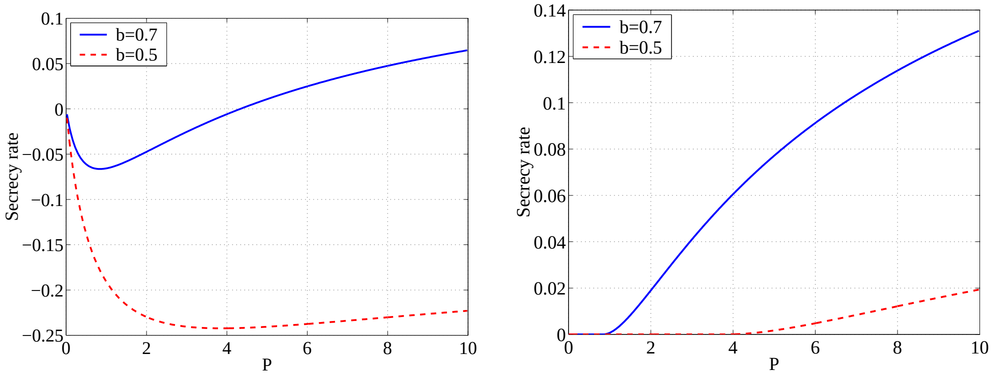
$$\begin{aligned}\mathcal{R}_v(P) &= I(V;Y) - I(V;Z|G)\\ &= \log\left(1 + \frac{bP_v}{bP_w + 1}\right) - E\left[\log\left(1 + \frac{GP_v}{GP_w + 1}\right)\right]\\ &= \log\left(1 + bP_w + bP_v\right) - E\left[\log(1 + GP_w + GP_v)\right]\\ &\quad - \left(\log\left(1 + bP_w\right) - E\left[\log(1 + GP_w)\right]\right). \end{aligned} \tag{4.31}$$

It follows from (4.8) that

$$\mathcal{R}_v(P) = \mathcal{R}_x(P_w + P_v) - \mathcal{R}_x(P_w) \tag{4.32}$$

$$= \mathcal{R}_x(P_x) - \mathcal{R}_x(P_w). \tag{4.33}$$

An important observation from (4.33) is that if $\mathcal{R}_x(P_w) < 0$, we actually gain by injecting the artificial Gaussian noise W. When $b < 1$, $\mathcal{R}_x(P) < 0$ for $P < f_{pos}^{-1}(b)$. In other words, $P_w \in [0, f_{pos}^{-1}(b))$ will produce negative $\mathcal{R}_x(P_w)$. Denote $P_w^*(b)$ as the noise power giving the



(a) $\mathcal{R}_x(P)$ **(b)** $\mathcal{R}_v(P)$

Figure 4.3: Secrecy rate with additive Gaussian white noise.

most negative $\mathcal{R}_x(P_w)$ for Bob's channel gain b. To find $P_w^*(b)$, we set the derivative of $\mathcal{R}_x$ in (4.8) to zero, and find the zero-yielding solution to be $P_w^*(b) = f_{mon}^{-1}(b)$. If $P > P_w^*(b)$, we maximize $\mathcal{R}_v$ by choosing $P_w = P_w^*(b)$ to get the most negative $\mathcal{R}_x(P_w)$, and choosing $P_x = P$ to maximize $\mathcal{R}_x(P_x)$, as $\mathcal{R}_x'(P) > 0$ for $P > f_{mon}^{-1}(b) = P_w^*(b)$. When $P \leq P_w^*(b)$, $\mathcal{R}_x(P_x)$ is negative, and $\mathcal{R}_x(P_w) > \mathcal{R}_x(P_x)$ for $P_w < P_x < P_w^*(b)$. In this case, injecting noise is not sufficient to boost the secrecy rate above zero. In summary, with this strategy of injecting artificial additive independent Gaussian noise, the achievable secrecy rate is

$$\mathcal{R}_v(P) = \begin{cases} \mathcal{R}_x(P) - \mathcal{R}_x(P_w^*(b)), & P > P_w^*(b), \\ 0, & P \leq P_w^*(b). \end{cases} \tag{4.34}$$

Note that $P_w^*(b) = f_{mon}^{-1}(b)$, which is zero for $b \geq 1$. Thus noise injection does not improve the secrecy rate for $b \geq 1$. Also note that even though $\mathcal{R}_x(P) < 0$ for $b < e^{-\gamma}$, we can still obtain a positive rate as long as $P > P_w^*(b)$ because $\mathcal{R}_x(P) > \mathcal{R}_x(P_w^*(b))$ due to the positive slope of $\mathcal{R}_x(P)$ after $P_w^*(b)$. Although there is no analytical solution for $P_w^*(b)$, we observe that

$$\mathcal{R}_x'(P) = \frac{b}{(1+bP)} - \Big(e^{1/P}E_1(1/P)\Big)' \tag{4.35}$$

$$= \frac{1}{P^2}\Big(e^{1/P}E_1(1/P) - \frac{P}{1+bP}\Big) \tag{4.36}$$

$$> \frac{1}{P^2}\Big(E_1(1/P) - \frac{1}{b}\Big) \tag{4.37}$$

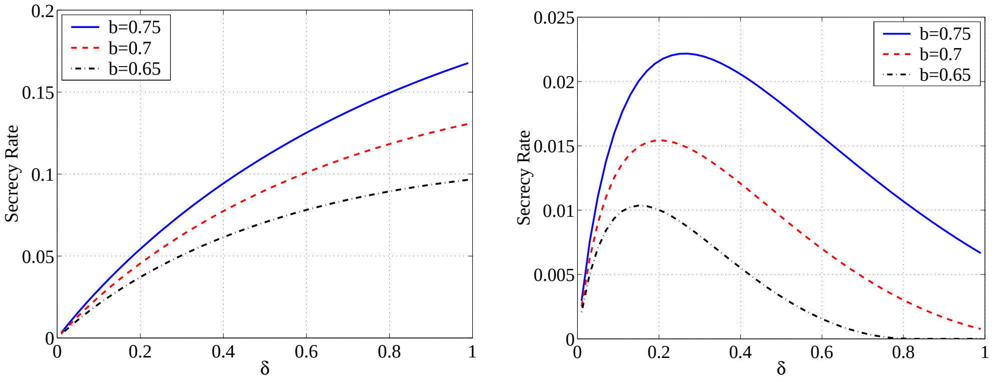
$$> \frac{1}{P^2}\Big(-\gamma + \log(P) - \frac{1}{b}\Big) \qquad \text{for } P > 1. \tag{4.38}$$

Thus for any $b \in (0,1)$, $P > e^{\gamma+1/b}$ implies that $\mathcal{R}_x'(P) > 0$, which guarantees that $P > P_w^*(b)$ and $\mathcal{R}_v(P) > 0$. In short, power $e^{\gamma+1/b}$ can serve as a rule of thumb estimate of the power needed to achieve a positive secrecy rate using noise injection.

To see the effect of injecting artificial noise, we plot $\mathcal{R}_x$ and $\mathcal{R}_v$ versus power budget P at $b = 0.7$ and $b = 0.5$ in Figure 4.3. Introducing artificial noise achieves positive secrecy rate even when b is less than $e^{-\gamma}$. This result looks surprising at first sight, since artificial noise degrades the Alice→Bob channel, and reduces the mutual information conveyed through this channel. The key point here is that the properly chosen artificial noise limits the SNR of Eve's channel even when Eve's random channel gain is very large. In our case, we inject white Gaussian noise with power $P_w^*(b)$ to make a positive secrecy rate achievable for very small b.

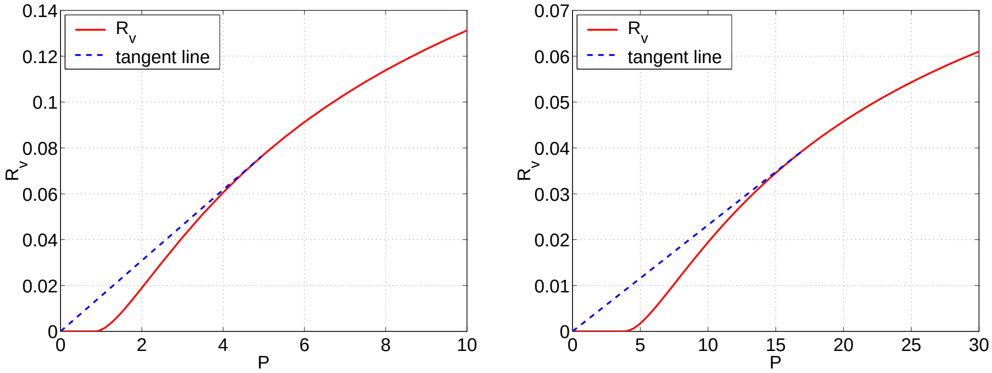
4.2.3 Bursting transmission with noise injection

The previous schemes show that, when $b \geq 1$, simple Gaussian codes can achieve a positive secrecy rate regardless of power budget; when $0 < b < 1$, the Gaussian codes with artificial noise method can achieve positive secrecy rate with sufficiently large P no matter how small b is. However, for small b, the given power budget may not be sufficient. To obtain positive secrecy rate with any average power budget $\bar{P}$, we can use a burst transmission method



(a) $\bar{P} = 10$ **(b)** $\bar{P} = 1$

Figure 4.4: Change of the average secrecy rate (4.39) with δ.



(a) $b = 0.7$ **(b)** $b = 0.5$

Figure 4.5: $\mathcal{R}_v(P)$ and the tangent line passing $\tilde{P}$.

that allows a large power for short periods of time. A simple bursting strategy that uses power $\bar{P}/\delta$ for δ fraction of time and zero power otherwise achieves the average secrecy rate

$$\bar{\mathcal{R}}_s(\bar{P}, \delta) = \delta \mathcal{R}_v(\bar{P}/\delta). \tag{4.39}$$

Evaluating this average secrecy rate for $\delta \in (0, 1]$ at several different b, we obtain Figure 4.4. The figure shows that for some configurations of $\{\bar{P}, b\}$, a bursting strategy ($\delta < 1$) is better than the constant power transmission ($\delta = 1$).

To find the optimal δ for a given power P and b, we can take a derivative of (4.39) with respective to δ. Obviously, to achieve positive secrecy rate, we only consider the portion of $\mathcal{R}_v(P,b)$ with $P > P_w^*(b)$, which is differentiable.

$$\frac{\partial\bar{\mathcal{R}}_s(\bar{P},\delta)}{\partial\delta} = \mathcal{R}_v(\bar{P}/\delta) + \delta\frac{\partial\mathcal{R}_v(\bar{P}/\delta)}{\partial P}\cdot\left(\frac{-\bar{P}}{\delta^2}\right) \tag{4.40}$$

$$= \mathcal{R}_v(\bar{P}/\delta) - (\bar{P}/\delta)\frac{\partial\mathcal{R}_v(\bar{P}/\delta)}{\partial P}. \tag{4.41}$$

If there is a $\delta^* \in (0,1)$ that maximizes $\bar{\mathcal{R}}_s(\delta)$, it must make the above derivative be zero. In other words,

$$\mathcal{R}_v(\bar{P}/\delta^*) = (\bar{P}/\delta^*)\frac{\partial\mathcal{R}_v(\bar{P}/\delta)}{\partial P}. \tag{4.42}$$

Define $\tilde{P}$ be the positive power that satisfies

$$\mathcal{R}_v(\tilde{P}) = \tilde{P}\frac{\partial\mathcal{R}_v(\tilde{P})}{\partial P}. \tag{4.43}$$

Note that $\tilde{P}$ is actually a function of b, Bob's relative channel gain. We are interested in $\tilde{P}$ with positive $\mathcal{R}_v(\tilde{P})$. The above equation is equivalent to

$$\frac{\partial\mathcal{R}_v(\tilde{P})}{\partial P} = \frac{\mathcal{R}_v(\tilde{P})}{\tilde{P}}. \tag{4.44}$$

In other words, the tangent line at $\tilde{P}$ passes through the origin with positive slope. For example, when $b = 0.7$, $\tilde{P}(b = 0.7) = 4.9447$. We plot $\mathcal{R}_v(P)$ and the tangent line at $P = \tilde{P}(b = 0.7)$ together on Figure 4.5(a). The tangent line passes the origin. Another example for $\mathcal{R}_v(P)$ and the origin-passing tangent line at $b = 0.5$ is showed in Figure 4.5(b). The value of $\tilde{P}(b)$ is plotted in Figure 4.6. $\tilde{P}(b)$ increases fast as b decreases.

When the power budget $\bar{P} < \tilde{P}(b)$, the optimal $\delta^* = \bar{P}/\tilde{P}(b) \in (0,1)$, and the secrecy rate achieved is

$$\bar{\mathcal{R}}_s(\bar{P},\delta^*) = \frac{\bar{P}}{\tilde{P}(b)}\mathcal{R}_v(\tilde{P}(b)) = \bar{P}\mathcal{R}_v'(\tilde{P}), \tag{4.45}$$

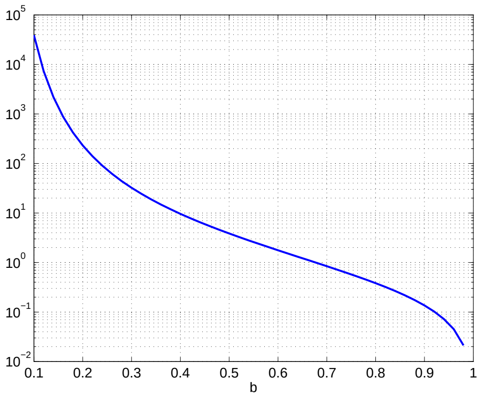


Figure 4.6: $\tilde{P}(b)$ that satisfies (4.43).

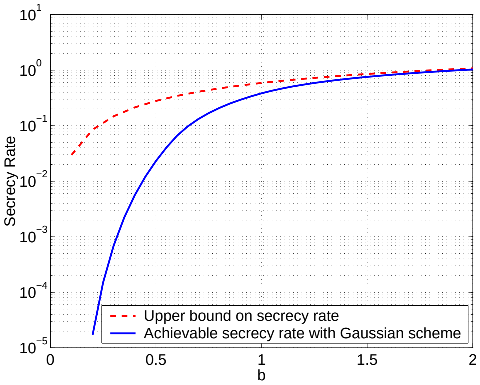


Figure 4.7: The achievable secrecy rate and the upper bound (4.46) at $\bar{P} = 10$.

which is exactly the tangent line. When the power budget $\bar{P} > \tilde{P}(b)$, the optimal $\delta^* = 1$. No bursting is needed in this case, and we achieve rate $\mathcal{R}_v(\bar{P})$. With this selection of the δ^*, we can achieve the upper envelope of the curves in Figure 4.5. Since this is actually the convex envelope of $\mathcal{R}_v(\bar{P})$, no more complicated power allocation strategy can achieve better secrecy rate.

4.3 Numerical evaluation

The scheme introduced above shows that it is possible to achieve positive secrecy rate even when Bob's channel is arbitrarily worse than Eve's average channel. We plot the achievable secrecy rate $\bar{\mathcal{R}}_s(\bar{P}, \delta^*)$ for the proposed scheme at power $\bar{P} = 10$ for varying b as the solid line in Figure 4.7. For each value of b, the achievable secrecy rate is obtained by evaluating $\bar{\mathcal{R}}_s(\bar{P}, \delta^*)$ with the optimal noise injection power $P_w^*(b)$ and bursting parameter δ^*.

An upper bound on the achievable rate for our model is the capacity result with slow block fading given in [23] as

$$E\left[(\log(1+b\bar{P}) - \log(1+G\bar{P}))^+\right] = \log(1+b\bar{P}) - e^{1/\bar{P}}\left(E_1(1/\bar{P}) - E_1(b+1/\bar{P})\right). \tag{4.46}$$

This bound appears as the dashed curve in Figure 4.7. There is a large gap between the upper bound and the achievable secrecy rate when b is small. However, this upper bound is likely not tight because it is achieved with the assumption that the timing of channel state change is known to Alice, which is not assumed in our model. On the other hand, it is clear that when Bob's channel gain gets large, the secrecy rate achieved by a Gaussian random codes in our model approaches this upper bound.

4.4 Discussion

We study the achievable secrecy rate with Gaussian random codes for the situation where the main channel is a constant AWGN channel, and Eve's channel is Rayleigh fading with unknown realizations but known statistics to the transmitter. The proposed method with artificial noise and bursting provides ways to achieve positive secrecy rate even when Bob's channel is much worse than Eve's average channel gain. Note that this secrecy rate is achieved without knowing when Eve's channel is bad or assumptions on the rate of Eve's channel changes.

We note that the proposed scheme with Gaussian random codes, artificial noise injection, and bursting transmission is not likely to be optimal. Actually, as we will show in the later chapter on discrete input, discrete input signaling such as QAM could provide larger secrecy rate than Gaussian signaling for some configurations. The key is still to limit the information the eavesdropper can gain when his channel is good, similar to our artificial noise approach. Nevertheless, the method presented in this chapter illustrates how the temporal variation of the channel facilitates secret communication even when the eavesdropper's channel realizations are unknown to the transmitter. The results are also very interesting in that they show that careful design of the preprocessing $V \rightarrow X$ channel can enable better secrecy rate.

Chapter 5

Secrecy Rate for Multi-antenna Systems

In previous chapters, we showed that the diversity introduced by fading can facilitate secret communication. It is easy to speculate that the extra spatial dimensions brought by multiple antennas can also be exploited for secret communication. Multiple antenna systems have been a popular field in both research and industry in the last decade. The capacity of the multiple antenna systems was derived in [20, chapter 8], [78], and the rate gain mainly depends on the rank of the channel matrix. When the channel matrix is known at both the transmitter and the receiver, the channel can be decomposed into independent parallel channels, and waterfilling over these channels achieves the capacity. When the channel matrix is time-varying and unknown at the transmitter but known at the receiver, input with unit covariance matrix achieves the ergodic capacity.

The secure communication problem for Multiple-input Multiple-output (MIMO) systems was first studied in [26], where it was shown that proper exploitation of space-time diversity at the transmitter can enhance information security and information hiding capabilities. In particular, for information security, Hero showed that when the eavesdropper is uninformed about his channel, the transmitter can enforce a zero information rate to the eavesdropper while delivering a positive information rate to the intended receiver by restricting the space-time modulation to a class of complex transmit matrices whose spatial inner product is a constant matrix. The channel capacity under this perfect secrecy condition, when both the transmitter and the intended receiver have channel information, was derived. However, the restriction to an eavesdropper uninformed about his channel is quite unrealistic. The secrecy capacity of single-input multiple-output channel under Gaussian noise was studied in [64] by transforming the channel into scalar wiretap channels. Negi et al. [61,62] studied secrecy capacity with MIMO channels when artificial noise is injected. They showed that injecting artificial noise in the nullspace of the intended receiver's channel can degrade Eve's channel and allow positive secrecy capacity even when Eve's channel was better before artificial noise injection. Practical schemes for secret transmission with MIMO using randomization were proposed in [39, 40].

In this work, we examine what kind of input structure should we use to achieve the secrecy rate for a multiple antenna broadcast channel. Although the secrecy capacity of the simple Alice-Bob-Eavesdropper channel model is always given by the well-known result derived by Csiszar and Korner [15], since the MIMO channel does not satisfy the more capable or less noisy conditions, the key issue is the structure of an appropriate auxiliary random variable V. However, $\max_X I(X;Y) - I(X;Z)$ can be considered as a lower bound to the achievable secrecy rate, and it is instructive to study this achievable secrecy rate under the MIMO scenario. To make the problem simpler, we assume Gaussian random codes are used at the transmitter and both Bob's and Eve's channels are known to Alice. The problem is formulated in Section 5.1. A simplified version of the problem for the Multiple-Input Single-Output (MISO) case is solved in Section 5.2.

5.1 Problem formulation

In the general broadcast channel scenario, Alice broadcasts her message to Bob, while Eve eavesdrops and tries to figure out the information communicated between Alice and

Bob. Let C_{sec} be the largest rate that Alice can transmit with perfect secrecy, denote the transmitted signal by Alice as X, and the received signal at Bob and Eve as Y and Z respectively. In [15], it was shown that the secrecy capacity under this case is

$$C_{sec} = \max_{V \to X \to YZ} I(V;Y) - I(V;Z),$$

where V is an auxiliary random variable. When Bob's channel is more capable than Eve's channel, the secrecy capacity is reduced to $C_{sec} = \max_X I(X;Y) - I(X;Z)$. In general, $\max_X I(X;Y) - I(X;Z)$ can be considered as a lower bound to the achievable secrecy rate, and it is instructive to study this achievable secrecy rate under the MIMO scenario. So our goal here is to find the optimal input structure that maximizes the achievable secrecy rate

$$\mathcal{R}_x = I(X;Y) - I(X;Z).$$

When the broadcast channels are MIMO, the outputs at Bob and Eve are modeled as

$$\mathbf{y} = H\mathbf{x} + \mathbf{w}_1, \tag{5.1a}$$

$$\mathbf{z} = G\mathbf{x} + \mathbf{w}_2, \tag{5.1b}$$

where H is the channel matrix between Alice and Bob, G is the channel matrix between Alice and Eve, and $\mathbf{w}_1$ and $\mathbf{w}_2$ are the corresponding noise vectors.

To make the problem simpler, we assume zero mean Gaussian random codes are used at the transmitter and both Bob's and Eve's channels are known to all parties. We further assume that the noise $\mathbf{w}_1$ and $\mathbf{w}_2$ are independent Gaussian white noise with the covariance matrix normalized to identity matrix. The distribution of the input $\mathbf{x}$ is characterized by its covariance matrix $Q = E[\mathbf{x}\mathbf{x}^\dagger]$. The mutual information between the transmitter and the receiver with channel matrix H under this MIMO model was shown to be $\log\det(I_r + HQH^\dagger)$ in [78], where I_r is the identity matrix with size r, the number of receiving antennas.

Therefore, to maximize the achievable secrecy rate $\mathcal{R}_x(Q)$, we need to

$$\begin{aligned} \text{maximize} \quad & \log\det(I_r + HQH^\dagger) - \log\det(I_r + GQG^\dagger) \\ \text{subject to} \quad & \operatorname{tr}(Q) \leq P, \ \ Q \succeq 0, \ Q = Q^\dagger, \end{aligned} \tag{5.2}$$

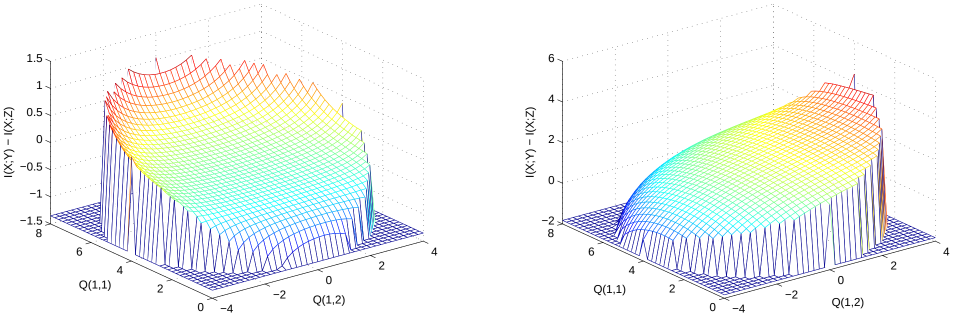
with the optimization variable Q, where $\succeq 0$ implies positive semidefiniteness. The channel input is required to satisfy the transmission power constraint P. Here we assume Bob and Eve have the same number of antennas, which we will extend in later work.

The objective function of the above optimization problem is not convex. This can be easily seen by noting that $\log\det(I_r + HQH^\dagger)$ is a concave function of Q. So, the objective function is a difference of two concave functions. For Q's that make the second term of the objective function zero, the objective function is concave, while for Q's that make the first term of the objective function zero, the objective function is convex. For a simple 2×2 MIMO case, we plot the $I(X;Y) - I(X;Z)$ as a function of $Q(1,1)$ and $Q(1,2)$ for two random channel realizations (assumed real here to allow plotting $Q(1,2)$) in Figure 5.1, with the power constraint satisfied with equality. From the figure, it is clear that maximizing $I(X;Y) - I(X;Z)$ is not easy even for this simple example, and a simple Newton method could be trapped in a local maximum.

By introducing an auxiliary variable t, we can reformulate the problem as

$$\begin{aligned} \text{maximize} \quad & t - \log\det(I_r + GQG^\dagger) \\ \text{subject to} \quad & \log\det(I_r + HQH^\dagger)) \geq t \\ & \operatorname{tr}(Q) \leq P, \ \ Q \succeq 0, \ Q = Q^\dagger. \end{aligned} \tag{5.3}$$

This is a convex maximization problem over a convex constraint set. There is rich research on solving the convex maximization problem (referred to as concave minimization in most



(a) (b)

Figure 5.1: $I(X;Y) - I(X;Z)$ for 2×2 random generated MIMO systems as a function of the covariance matrix coefficients $Q(1,1)$ and $Q(1,2)$, with the power constraint satisfied with equality.

references) numerically, as described in detail in [28], but their applicability is not straightforward to our problem due to the complex function format used here.

5.2 A simple case: MISO

Although problem (5.2) is non-convex, and thus hard when H and G are of arbitrary size, the problem can be simplified for the MISO case, where both receivers at Bob and Eve have only a single antenna. Denote n to be the number of transmit antennas, then H and G are $1 \times n$ vectors in this case. To avoid confusion, we use vectors $\mathbf{h}$ and $\mathbf{g}$ of size $1 \times n$ to denote the channel realization, and rewrite the channel model as

$$y = \mathbf{hx} + w_1, \tag{5.4a}$$

$$z = \mathbf{gx} + w_2. \tag{5.4b}$$

Both the noise and the outputs are scalar now. We can further simplify the model by a coordinate transformation. Suppose we have a unitary matrix R of size $n \times n$, with property

$$RR^\dagger = R^\dagger R = I_n. \tag{5.5}$$

Then (5.4) is equivalent to

$$y = \mathbf{h}RR^{\dagger}\mathbf{x} + w_1 = \tilde{\mathbf{h}}\tilde{\mathbf{x}} + w_1, \tag{5.6a}$$

$$z = \mathbf{g}RR^{\dagger}\mathbf{x} + w_2 = \tilde{\mathbf{g}}\tilde{\mathbf{x}} + w_2, \tag{5.6b}$$

where $\tilde{\mathbf{x}}$, $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ are the vector representations of $\mathbf{x}$, $\mathbf{h}$ and $\mathbf{g}$ in the transformed space spanned by R. Since R is invertible, it is clear that $I(\mathbf{x}; y) = I(\tilde{\mathbf{x}}; y)$ and $I(\mathbf{x}; z) = I(\tilde{\mathbf{x}}; z)$.

To simplify the model, we can choose R in the following way

1. The first column is $\mathbf{r}_1 = \mathbf{h}^{\dagger}/||\mathbf{h}||$,

2. The second column $\mathbf{r}_2$ is orthogonal to $\mathbf{r}_1$, and lies in the space spanned by $\mathbf{h}$ and $\mathbf{g}$. Mathematically, this means

$$\mathbf{r}_2 = \frac{(\mathbf{g} - (\mathbf{g}\mathbf{r}_1)\mathbf{r}_1^{\dagger})^{\dagger}}{||\mathbf{g} - (\mathbf{g}\mathbf{r}_1)\mathbf{r}_1^{\dagger}||} = \frac{(\mathbf{g} - ||\mathbf{g}||\alpha\mathbf{r}_1^{\dagger})^{\dagger}}{||\mathbf{g}||\sqrt{1-\alpha^{\dagger}\alpha}}, \tag{5.7}$$

   where α is the normalized correlation coefficient, defined as

$$\alpha = \frac{\mathbf{g}\mathbf{h}^{\dagger}}{||\mathbf{g}|| \cdot ||\mathbf{h}||}.$$

   (It is assumed that $\mathbf{h}$ and $\mathbf{g}$ are not in the same direction here, since in that situation, the channel is just reduced to a scalar Gaussian broadcast channel).

3. The rest of the rows are an arbitrarily chosen orthonormal basis set for the remaining $n - 2$ dimensions, and are orthogonal to the first two rows.

With this selection of R, we have

$$\tilde{\mathbf{h}} = \mathbf{h}R = ||\mathbf{h}|| \cdot [1, 0, \cdots, 0], \tag{5.8}$$

$$\tilde{\mathbf{g}} = \mathbf{g}R = ||\mathbf{g}|| \cdot [\alpha, \sqrt{1-\alpha^{\dagger}\alpha}, \cdots, 0]. \tag{5.9}$$

Since $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ both have zero components in the subspace spanned by $\{\mathbf{r}_3, \cdots, \mathbf{r}_n\}$, no power should be put into those dimensions. So we can focus only on the subspace spanned by the first two rows of R. This reduces the MISO channel model to

$$y = ||\mathbf{h}|| \cdot [1, 0] \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} + w_1, \tag{5.10a}$$

$$z = ||\mathbf{g}|| \cdot \left[\alpha, \sqrt{1-\alpha^\dagger\alpha}\right] \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} + w_2. \tag{5.10b}$$

From now on, we will refer

$$\tilde{\mathbf{x}} = \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix}, \ \tilde{\mathbf{h}} = ||\mathbf{h}|| \begin{bmatrix} 1 & 0 \end{bmatrix}, \ \tilde{\mathbf{g}} = ||\mathbf{g}|| \begin{bmatrix} \alpha & \sqrt{1-\alpha^\dagger\alpha} \end{bmatrix}.$$

Our goal is to find the covariance matrix $Q = E[\tilde{\mathbf{x}}\tilde{\mathbf{x}}^\dagger]$ that maximizes the secrecy rate $I(\tilde{\mathbf{x}}; y) - I(\tilde{\mathbf{x}}; z)$ under the power constraint $tr(Q) \leq P$. Once we find Q, we can easily transfer it back to the original space using the transformation matrix R.

5.2.1 Analytical solution

For the transformed model (5.10), we have

$$\mathcal{R}_x(Q) = I(\tilde{\mathbf{x}}; y) - I(\tilde{\mathbf{x}}; z) \tag{5.11}$$

$$= \log(1 + \tilde{\mathbf{h}}Q\tilde{\mathbf{h}}^\dagger) - \log(1 + \tilde{\mathbf{g}}Q\tilde{\mathbf{g}}^\dagger) \tag{5.12}$$

$$= \log \frac{1 + \tilde{\mathbf{h}}Q\tilde{\mathbf{h}}^\dagger}{1 + \tilde{\mathbf{g}}Q\tilde{\mathbf{g}}^\dagger}. \tag{5.13}$$

So, maximizing $\mathcal{R}_x(Q)$ is equivalent to maximizing $(1+\tilde{\mathbf{h}}Q\tilde{\mathbf{h}}^\dagger)/(1+\tilde{\mathbf{g}}Q\tilde{\mathbf{g}}^\dagger)$. Since the matrix Q is Hermitian and positive semidefinite, it can be written as $Q = \sum_{i=1}^2 \lambda_i u_i u_i^\dagger$, where u_i are orthogonal unit vectors and $\lambda_i \geq 0$ for $i = 1, 2$. Also, since the optimal solution always uses up all available power (this point is more clear from the alternative method in Section

5.2.2), we let $tr(Q) = P$, which yields $\sum_i \lambda_i = P$. Then, we can write

$$1 + \tilde{\mathbf{h}}Q\tilde{\mathbf{h}}^\dagger = \sum_{i=1}^{2} \frac{\lambda_i}{P} u_i^\dagger u_i + \sum_{i=1}^{2} \lambda_i \tilde{\mathbf{h}} u_i u_i^\dagger \tilde{\mathbf{h}}^\dagger \tag{5.14}$$

$$= \sum_{i=1}^{2} \frac{\lambda_i}{P} u_i^\dagger I_2 u_i + \sum_{i=1}^{2} \lambda_i u_i^\dagger \tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}} u_i \tag{5.15}$$

$$= \sum_{i=1}^{2} \frac{\lambda_i}{P} u_i^\dagger (I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}}) u_i, \tag{5.16}$$

where we utilized the fact that for MISO $\tilde{\mathbf{h}}u_i$ is a scalar so that $\tilde{\mathbf{h}}u_i u_i^\dagger \tilde{\mathbf{h}}^\dagger = u_i^\dagger \tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}} u_i$. Similarly, we can write

$$1 + \tilde{\mathbf{g}}Q\tilde{\mathbf{g}}^\dagger = \sum_{i=1}^{2} \frac{\lambda_i}{P} u_i^\dagger (I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}}) u_i. \tag{5.17}$$

Thus,

$$\frac{1 + \tilde{\mathbf{h}}Q\tilde{\mathbf{h}}^\dagger}{1 + \tilde{\mathbf{g}}Q\tilde{\mathbf{g}}^\dagger} = \frac{\sum_{i=1}^{2} \lambda_i u_i^\dagger (I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}}) u_i}{\sum_{i=1}^{2} \lambda_i u_i^\dagger (I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}}) u_i}. \tag{5.18}$$

Denote $a_i = u_i^\dagger (I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}}) u_i$ and $b_i = u_i^\dagger (I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}}) u_i$, then maximizing $\mathcal{R}_x(Q)$ is equivalent to

$$\text{maximize } M \text{ such that } \frac{\sum_i \lambda_i a_i}{\sum_i \lambda_i b_i} \geq M. \tag{5.19}$$

Since $\lambda_i \geq 0$, $a_i \geq 0$, and $b_i \geq 0$, the above problem can be rewritten as $\sum_i \lambda_i (a_i - M b_i) \geq 0$. The largest M that satisfies the constraint is

$$M^* = \max_i \frac{a_i}{b_i}, \tag{5.20}$$

and the corresponding λ_i are

$$\lambda_j = \begin{cases} P & j = \arg\max_i \frac{a_i}{b_i}, \\ 0 & \text{otherwise.} \end{cases} \tag{5.21}$$

Moreover,

$$\max_i \frac{a_i}{b_i} = \max_u \frac{u_i^\dagger (I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}}) u_i}{u_i^\dagger (I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}}) u_i}, \tag{5.22}$$

which can be converted to a well known Rayleigh quotient problem. To see this, note that $I_2 + P\tilde{\mathbf{g}}^\dagger\tilde{\mathbf{g}}$ is Hermitian and positive definite, so it can be factorized as $I_2 + P\tilde{\mathbf{g}}^\dagger\tilde{\mathbf{g}} = VD^2V^\dagger$ where V is unitary and contains the eigenvectors of the matrix, and D is diagonal and contains the square roots of the associated eigenvalues. Since the eigenvalues are nonzero, we can define a new vector related to u by an invertible transformation: $v = DV^\dagger u$. Then the optimization problem becomes

$$\max_v \frac{v^\dagger D^{-1}V^\dagger(I_2 + P\tilde{\mathbf{h}}^\dagger\tilde{\mathbf{h}})VD^{-1}v}{v^\dagger v}. \tag{5.23}$$

The optimal solution v^* is just the eigenvector corresponding to the largest eigenvalue of the matrix $D^{-1}V^\dagger(I_2+P\tilde{\mathbf{h}}^\dagger\tilde{\mathbf{h}})VD^{-1}$. This may then be transformed back to obtain the optimal normalized solution u^*. The resulting optimal covariance matrix is simply $Q^* = Pu^*u^{*\dagger}$. We note that the solution u^* is also the generalized eigenvector corresponding to the largest generalized eigenvalue of the two matrices $I_2 + P\tilde{\mathbf{h}}^\dagger\tilde{\mathbf{h}}$ and $I_2 + P\tilde{\mathbf{g}}^\dagger\tilde{\mathbf{g}}$. In other words, it is the eigenvector with the largest eigenvalue of the matrix

$$\begin{aligned}
A &= (I_2 + P\tilde{\mathbf{g}}^\dagger\tilde{\mathbf{g}})^{-1}(I_2 + P\tilde{\mathbf{h}}^\dagger\tilde{\mathbf{h}}) && (5.24)\\
&= \begin{bmatrix} P||\mathbf{g}||^2\alpha^\dagger\alpha + 1 & P||\hat{\mathbf{g}}||^2\alpha^\dagger\sqrt{1-\alpha^\dagger\alpha} \\ P||\mathbf{g}||^2\alpha\sqrt{1-\alpha^\dagger\alpha} & P||\mathbf{g}||^2(1-\alpha^\dagger\alpha)+1 \end{bmatrix}^{-1} \begin{bmatrix} P||\hat{\mathbf{h}}||^2 + 1 & 0 \\ 0 & 1 \end{bmatrix} && (5.25)\\
&= \left(\frac{P||\hat{\mathbf{h}}||^2+1}{P||\hat{\mathbf{g}}||^2+1}\right) \begin{bmatrix} P||\hat{\mathbf{g}}||^2(1-\rho^2)+1 & \frac{-P||\hat{\mathbf{g}}||^2\rho\sqrt{1-\rho^2}}{P||\hat{\mathbf{h}}||^2+1} \\ -P||\hat{\mathbf{g}}||^2\rho\sqrt{1-\rho^2} & \frac{P||\hat{\mathbf{g}}||^2\rho^2+1}{P||\hat{\mathbf{h}}||^2+1} \end{bmatrix} && (5.26)
\end{aligned}$$

5.2.2 Alternative view

The method in previous subsection gives an analytical solution to our problem. An alternative view might provide more insight to this problem, as we will explain in this section.

We can expand (5.10) to the following

$$y = ||\mathbf{h}||\tilde{x}_1 + w_1, \tag{5.27a}$$

$$z = ||\mathbf{g}|| \left(\alpha\tilde{x}_1 + \sqrt{1-\alpha^\dagger\alpha}\,\tilde{x}_2 \right) + w_2. \tag{5.27b}$$

Then we can write the achievable secrecy rate as

$$\mathcal{R}_x(Q) = I(\tilde{\mathbf{x}}; y) - I(\tilde{\mathbf{x}}; z) \tag{5.28}$$

$$= H(y) - H(y|\tilde{\mathbf{x}}) - (H(z) - H(z|\tilde{\mathbf{x}})) \tag{5.29}$$

$$= H(y) - H(z) \tag{5.30}$$

$$= \log(2\pi e P_y) - \log(2\pi e P_z), \tag{5.31}$$

where the last step uses the assumption that $\tilde{\mathbf{x}}$ is a zero mean Gaussian random variable. P_y and P_z are the output powers at Bob and Eve respectively. Denote P_1 and P_2 as the power of $\tilde{x}_1$ and $\tilde{x}_2$, then we have

$$P_y = E[yy^\dagger] = ||\mathbf{h}||^2 P_1 + 1, \tag{5.32}$$

$$P_z = E[zz^\dagger] = ||\mathbf{g}||^2 \left(\alpha\alpha^\dagger P_1 + (1-\alpha^\dagger\alpha)P_2 + \gamma \right) + 1, \tag{5.33}$$

with

$$\gamma = \alpha\sqrt{1-\alpha^\dagger\alpha} E[\tilde{x}_1\tilde{x}_2^\dagger] + \alpha^\dagger\sqrt{1-\alpha^\dagger\alpha} E[\tilde{x}_1^\dagger\tilde{x}_2]. \tag{5.34}$$

Define ρ be the normalized correlation coefficient

$$\rho = \frac{E[\tilde{x}_1\tilde{x}_2^\dagger]}{\sqrt{P_1P_2}},$$

then

$$\gamma = \alpha\sqrt{1-\alpha^\dagger\alpha}\rho\sqrt{P_1P_2} + \alpha^\dagger\sqrt{1-\alpha^\dagger\alpha}\rho^\dagger\sqrt{P_1P_2} \tag{5.35}$$

$$= (\alpha\rho + \alpha^\dagger\rho^\dagger)\sqrt{(1-\alpha^\dagger\alpha)P_1P_2} \tag{5.36}$$

$$= 2\Re(\alpha\rho)\sqrt{(1-\alpha^\dagger\alpha)P_1P_2}. \tag{5.37}$$

Now our problem is converted to finding the optimal $\{P_1, P_2, \rho\}$ (which determines Q), to maximize $I(\tilde{\mathbf{x}}; y) - I(\tilde{\mathbf{x}}; z)$ with the power constraint $P_1 + P_2 \leq P$.

An important observation here is that the optimization over the correlation coefficient ρ can be separated from the optimization over the power allocation. For a given power allocation $\{P_1, P_2\}$, to maximize $\mathcal{R}_x(Q)$, we should minimize $H(z)$, which is equivalent to minimizing P_z, and in turn minimizing γ. From (5.37), we conclude that we should choose ρ to minimize $\Re(\alpha\rho)$, and meanwhile satisfy the constraint $\rho\rho^\dagger \leq 1$. Let α_r and α_i denote the real and imaginary part of α respectively, and similarly for ρ_r and ρ_i, then ρ_r and ρ_i is the solution to the following optimization problem:

$$\begin{aligned} &\text{minimize} && \alpha_r\rho_r - \alpha_i\rho_i, \\ &\text{subject to} && \rho_r^2 + \rho_i^2 \leq 1. \end{aligned} \tag{5.38}$$

This is a convex optimization problem that can be easily solved with the Lagrangian method, and the optimal solution is $\rho^* = -\alpha^\dagger/||\alpha||$.

With $\rho = \rho^*$, we obtain

$$\gamma = -2||\alpha||\sqrt{(1-\alpha^\dagger\alpha)P_1P_2}, \tag{5.39}$$

$$\sigma_z^2 = ||\mathbf{g}||^2\left(\sqrt{\alpha^\dagger\alpha P_1} - \sqrt{(1-\alpha^\dagger\alpha)P_2}\right)^2 + 1. \tag{5.40}$$

Substituting (5.32) and (5.40) back to (5.31), we obtain

$$\begin{aligned} \mathcal{R}_x(P_1, P_2) &= \log(P_y) - \log(P_z) && (5.41) \\ &= \log\left(\frac{||\mathbf{h}||^2 P_1 + 1}{||\mathbf{g}||^2\left(\sqrt{\alpha^\dagger\alpha P_1} - \sqrt{(1-\alpha^\dagger\alpha)P_2}\right)^2 + 1}\right). && (5.42) \end{aligned}$$

Now, we can choose P_1 and P_2 to maximize the above secrecy rate with the power constraint. Note that the denominator is minimized when $\sqrt{\alpha^\dagger\alpha P_1} = \sqrt{(1-\alpha^\dagger\alpha)P_2}$, which implies that

$\tilde{x}_1$ and $\tilde{x}_2$ cancel each other completely at the eavesdropper's receiver so that she essentially gets no information on the input. We call this zero-forcing at Eve, and when it happens, we have

$$P_2 = \frac{\alpha^\dagger \alpha}{1 - \alpha^\dagger \alpha} P_1. \tag{5.43}$$

Thus, for a given P_1, if $P - P_1 \geq \frac{\alpha^\dagger \alpha}{1-\alpha^\dagger \alpha} P_1$, which means $P_1 \leq (1 - \alpha^\dagger \alpha)P$, we should choose $P_2 = \frac{\alpha^\dagger \alpha}{1-\alpha^\dagger \alpha} P_1$ to maximize $\mathcal{R}_x(P_1, P_2)$. When $P_1 > (1 - \alpha^\dagger \alpha)P$, due to the power constraint, zero-forcing is not possible. To maximize $\mathcal{R}_x(P_1, P_2)$, we should do the canceling as much as possible, which means $P_2 = P - P_1$. With this analysis, we can remove P_2 from the parameter list and obtain

$$\mathcal{R}_x(P_1) = \begin{cases} \log(||\mathbf{h}||^2 P_1 + 1), & P_1 \leq (1 - \alpha^\dagger \alpha)P \\ \log\left(\frac{||\mathbf{h}||^2 P_1 + 1}{||\mathbf{g}||^2 \left(\sqrt{\alpha^\dagger \alpha P_1} - \sqrt{(1-\alpha^\dagger \alpha)(P - P_1)}\right)^2 + 1}\right), & (1 - \alpha^\dagger \alpha)P \leq P_1 \leq P. \end{cases} \tag{5.44}$$

Note that the first segment of $\mathcal{R}_x(P_1)$ increases with P_1, which means it has the maximum at $P_1 = (1 - \alpha^\dagger \alpha)P$. This corresponds to the best secrecy rate with zero-forcing, and can be consider as the lower bound to our achievable secrecy rate. However, zero-forcing rate is constant regardless of Eve's actual channel gain, so it might not be the optimal P_1, as we can see from Figure 5.2. For the same $\alpha = 0.7$, when Eve's channel gain is relatively large, the zero-nulling rate (corresponding to the intersection of the two curves) is very good, while when Eve's channel gain is relatively small, it is not the best achievable secrecy rate.

It is easy to see that the power constraint should always be satisfied with equality, since the optimal P_1 satisfies $P_1 \geq (1 - \alpha^\dagger \alpha)P$. Also, we only need to maximize the second segment of $\mathcal{R}_x(P_1)$ over its corresponding range of P_1. However, the function format is complicated, and an analytical optimal solution of P_1 is hard to obtain in this way.

This view gives some insight on how coding should be performed for secrecy reason. Note that $\rho^* \rho^{*\dagger} = 1$ suggests that $\tilde{x}_2 = c\tilde{x}_1$, where c is some optimally chosen constant.

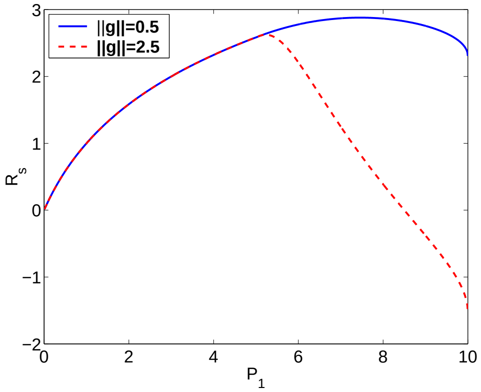


Figure 5.2: Change of $\mathcal{R}_x(P_1)$ with P_1 at different Eve's channel gains. $\alpha = 0.7$. $P = 10$, $||\mathbf{h}|| = 1$.

In other words, $\tilde{x}_2$ is linearly correlated with $\tilde{x}_1$ in such a way that they cancel each other to some optimal extent at Eve. When (5.43) holds, the two inputs completely cancel each other, and the mutual information between z and the input $\tilde{\mathbf{x}}$ is zero. If we consider $\tilde{x}_1$ as the information bearing signal, and $\tilde{x}_2$ as a jamming signal, then our problem is a little similar to the correlated jamming case described in [57,68], except that we have a different objective function, and the jammer and the user are cooperative.

5.3 Numerical evaluation

We now evaluate the achievable secrecy rate $\mathcal{R}_x^* = \max_Q \log(1 + \mathbf{h}Q\mathbf{h}^\dagger) - \log(1 + \mathbf{g}Q\mathbf{g}^\dagger)$, and see how it varies with the MISO channel realizations $\mathbf{h}$ and $\mathbf{g}$ pictorially. For a fixed power budget P, $\mathcal{R}_x^*$ is determined by $||\mathbf{h}||$, $||\mathbf{g}||$ and α. In evaluation, we fix $||\mathbf{h}|| = 1$, and vary $||\mathbf{g}||$ and α. For simplicity, we consider only the real channel here so that α is real. It does not matter if α is positive or negative, since ρ^* will always compensate that factor, so we only evaluate the secrecy rate with positive α. The results are shown in Figure 5.3.

We note that Eve's channel gain $||\mathbf{g}||$ has a significant effect on the secrecy rate only

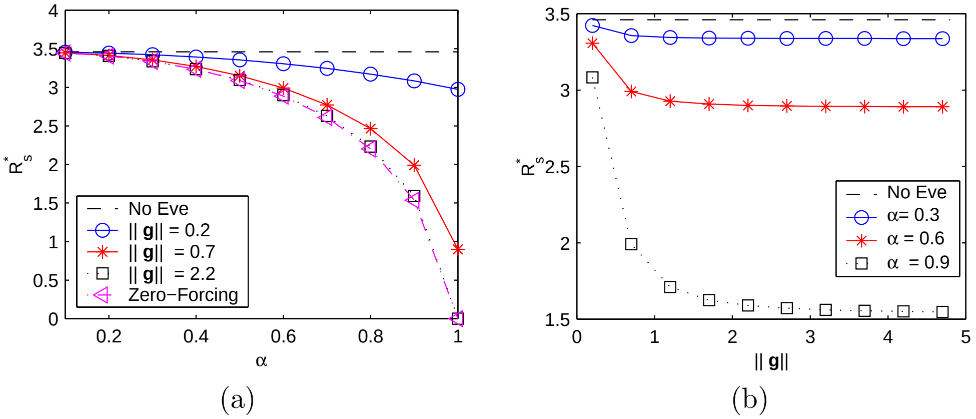


Figure 5.3: Change of R_s^* with the normalized channel correlation coefficient α and Eve's channel gain α. $P = 10$, $||\mathbf{h}|| = 1$.

when it is worse than Bob's channel. When $||\mathbf{g}|| > ||\mathbf{h}||$, zero-forcing strategy is close to optimal, and $||\mathbf{g}||$ becomes almost irrelevant. As expected, the larger α, the more correlated the two channels are, the lower the secrecy rate. α plays the critical role on the achievable secrecy rate when $||\mathbf{g}|| > ||\mathbf{h}||$. Increasing α results in a sharp drop of the secrecy rate, and $\alpha = 1$ shuts down the secure communication completely when $||\mathbf{g}|| > ||\mathbf{h}||$. On the other hand, we note that when α is small, the rate loss relative to the normal capacity is small. Moreover, as long as the normalized channel correlation $\alpha \neq 1$, we can get a positive secrecy rate no matter how strong Eve's channel is. Since $\alpha = 1$ means Eve's channel is a scaled version of Bob's channel, the chance of this to happen is small in a fading environment with multiple antennas. Also, the more number of transmit antennas, the more likely that the correlation of the two channels is small. Therefore, multiple transmit antennas provide more freedom, and in turn allow secret communication even when Eve's channel is much better.

5.4 Discussion

In this work, we studied the achievable secrecy rate for a multiple antenna system, and the optimal input structure to achieve this rate. For the general multiple input multiple output case, the problem is not convex and is hard to solve. However, for the MISO case, the problem can be reformulated, and can be solved. An analytical solution is derived for this simple case and the implication of the results are discussed in this paper. Multiple antenna provides extra degree of freedom to the transmitter such that some beamforming like approach can be used to provide advantage to the intended receiver against the eavesdropper.

We note that a similar result was derived independently in [67]. Result for MIMO channel with two transmit antenna, two receive antenna and one eavesdropping antenna was presented in [66]. It was proved later by [31, 53, 63] that the achievable rate we derived for a MISO system is indeed the capacity. For the more general MIMO case, a Gaussian input is optimal, and no auxiliary random variable is needed. However, analytical solution for the optimal covariance matrix is still hard to obtain. Nevertheless, the authors show that the optimal covariance matrix will render the eavesdropper's channel to be a degraded one of the intended receiver's channel.

Chapter 6

Secrecy Rate Region of a Class of One-sided Interference Channels

Due to the shared nature of the wireless medium, secret communication becomes more complicated when there exist multiple transmitter-receiver pairs simultaneously transmitting in a network setting. Not only does the communication over the links interfere each other, but also each transmitter i must encode its messages so that only the corresponding receiver i can decode the messages. The receiver of any link $j \neq i$ is not permitted to resolve more than arbitrarily little information regarding the information communicated on link i.

Unlike the single transmitter scenario, in interference channels, the secrecy afforded to link i from an eavesdropping receiver j may depend on the signaling employed on link j as well as on other links. For example, in a 2-user Gaussian interference channel, if transmitter 2 is silent, then receiver 2 can act as a traditional eavesdropper of link 1. Similarly, over a discrete memoryless channel, user 2 may choose to transmit a particular symbol that best "opens" the channel for eavesdropping. On the other hand, if transmitter 2 sends at a nonzero rate, because receiver 2 must also decode its own messages, this signal can interfere with the eavesdropping ability of receiver 2. That is, the rate at which user 1 can communicate secretly will depend on the signaling strategy of user 2. Alternatively, transmitter 2 can also act as a helper to facilitate transmitter 1's secret communication, and then the two transmitters reverse roles in the next round.

There have been several works on multi-user secret communication in recent years. Multi-access channels were considered by [50, 75]. The relay channel is considered in [35] where the second transmitter acts as a helper and does not transmit it's own message. Several relay strategies, such as decode and forward, amplify and forward, noise forwarding strategies, were considered and their corresponding achievable rates were evaluated. Both broadcast channels and interference channels were considered in [51], where both the inner bound and the outer bound of the two-user interference channel were proposed. The memoryless channel is characterized by the transition probability $P(\mathbf{y}_1, \mathbf{y}_2|\mathbf{x}_1, \mathbf{x}_2) = \prod_{i=1}^{n} P(y_{1,i}, y_{2,i}|x_{1,i}, x_{2,i})$ where $\mathbf{x_1}, \mathbf{x_2}$ are the length n transmitted codewords, and i is the time index. The authors showed that the inner bound and the outer bound coincide for a switch channel example. However, for a switch channel, due to the time sharing nature, there is no real interference among the users. For more general interference channels, because of the large number of possibilities for the auxiliary random variables and their correlations, it is hard to evaluate the bound and find the points on the border of the regions.

In this work, we investigate the secrecy rate region of a class of one-sided interference channel, as illustrated in Figure 6.1. Although the inner and outer bounds of the general two user interference channel have been previously derived in [51], these bounds are hard to compute due to auxiliary random variables in the formulation. In our work, we provide a more tractable outer bound specifically for the class of one-sided interference channel. We show that this bound is tight for a deterministic channel example, and is achievable within one bit for a Gaussian one-sided interference channel example.

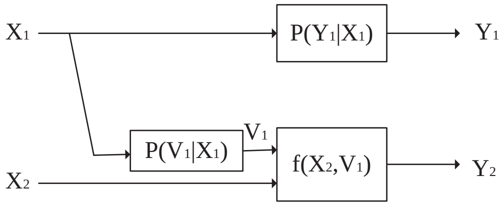


Figure 6.1: One-sided interference channel model.

6.1 Problem formulation

The class of one-sided interference channel model we consider is shown in Figure 6.1. The channels are memoryless, and the output $Y_2 = f(X_2, V_1)$ is a deterministic function of the input X_1 and the interference V_1, where $f(\cdot,\cdot)$ satisfies the condition

$$H(Y_2|X_2) = H(V_1), \tag{6.1}$$

for all product probability distributions on X_1 and X_2. This condition is equivalent to requiring the existence of a function $h(\cdot,\cdot)$ such that $V_1 = h(X_2, Y_2)$. This channel model is a generalization of the one-sided interference channel model examined in [21], which considers the case when $P(V_1|X_1)$ is a deterministic mapping. In this work, the stochastic mapping $P(V_1|X_1)$ enables randomness in the channel from X_2 to Y_2 despite $f(X_2, V_1)$ being deterministic. For example, this model covers the Gaussian one-sided interference channel shown in Figure 6.4 with $Y_1 = X_1 + N_1$,$V_1 = aX_1 + N_2$ and $Y_2 = V_1 + X_2$, where N_1, N_2 are unit variance Gaussian noise, and a is the cross channel gain.

There are two communication links in this system. Each transmitter i produces input x_i for each channel use and each receiver i observes the output y_i. We assume that each transmitter i communicates an independent message index $W_i \in \{1, \cdots, M_i\}$ to receiver i by transmitting a codeword denoted by the vector $X_i^n = [x_i(1), \cdots, x_i(n)]$ of n transmitted symbols. Given the observation sequence $Y_i^n = [y_i(1), \cdots, y_i(n)]$, receiver i guesses a message index $\hat{W}_i$. Each user's rate is given by $R_i = \log_2(M_i)/n$. The secrecy rate $\mathbf{R} = (R_1, R_2)$

is said to be achievable if given any $\epsilon > 0$, there exists a coding strategy for the two users such that the following conditions are satisfied:

- The communication for each user is reliable, i.e., the maximal decoding error probability $\max_i P(W_i \neq \hat{W}_i) \leq \epsilon$.
- The communication for each user is confidential in spite of the other receiver's eavesdropping. That is, the normalized information leakage satisfies $I(W_i; Y_j^n)/n \leq \epsilon$ for $i = 1, j = 2$ and $i = 2, j = 1$. This is equivalent to the definition $H(W_i|Y_j^n)/n \geq R - \epsilon$, which has been used in the literature. Note that in our one-sided interference channel model, the message sent by user 2 is always confidential as there is no link from transmitter 2 to receiver 1.

We note that, for this definition of secrecy, the transmitters are assumed to be trustworthy and will not deviate from the strategy agreed upon before communication. However, trustworthy does not mean that they know the signal transmitted by the others or that they share some common randomness. We aim at finding the capacity region of this class of one-sided interference channel. However, exact characterization of the secrecy capacity region is not so straightforward. Instead, we will present an outer bound region in the next section, which is shown to be tight for the deterministic channel described in Section 6.3, and is achievable within a constant gap for some Gaussian one-sided interference channels.

6.2 An outer bound

As mentioned earlier, an outer bound for the general interference channel with the transition probability $P(Y_1Y_2|X_1X_2)$ has been investigated in [51]. However, this bound is hard to compute, even for the class of one-sided interference channel that we have considered here.

In this work, we focus on our specific one-sided interference channel and derive a bound that is easier to compute for some cases. The main result of this paper is the following theorem.

Theorem 6.1 *The secrecy capacity region of the channel of Figure 6.1 is contained in the union over all channel inputs of the form $P(u)P(u_1|u)P(x_1|u_1)P(x_2)$ of all pairs (R_1, R_2) for which*

$$0 \leq R_1 \leq I(X_1; Y_1|Y_2), \tag{6.2a}$$

$$0 \leq R_2 \leq I(X_2; Y_2|X_1), \tag{6.2b}$$

$$0 \leq R_1 + R_2 \leq I(U_1; Y_1|U) - I(U_1; Y_2|X_2U) + I(X_2; Y_2|X_1). \tag{6.2c}$$

When the more capable condition

$$I(X_1; Y_1) \geq I(X_1; V_1) \tag{6.3}$$

is satisfied for all possible input distributions $P(x_1)$, $U_1 = X_1$ and the bound (6.2c) is replaced by

$$0 \leq R_1 + R_2 \leq I(X_1; Y_1|U) - I(X_1; Y_2|X_2U) + I(X_2; Y_2|X_1). \tag{6.4}$$

The proof of Theorem 6.1 is based on the techniques developed in [15], and is provided below. The first bound (6.2a) is obtained by enhancing receiver 1 such that it has knowledge of what receiver 2 gets. The second bound (6.2b) is the maximum rate that user 2 can obtain, and is very straightforward. The third bound (6.2c) characterizes the sum rate bound, and shows the trade-off between the rates of the two users. Note that $I(U_1; Y_1|U) - I(U_1; Y_2|X_2U)$ in (6.2c) is essentially the secrecy capacity for the channel of X_1 to Y_1, with V_1 being the eavesdropper's observation. So, if X_2 is silent, that is the maximum secrecy rate user 1 can get. However, if X_2 is not silent and is willing to sacrifice its own rate, then user 1 might get a higher rate than he would otherwise.

Proof: The bounds (6.2b) are obvious. Now we will prove the R_1 bound (6.2a) and the sum rate bound (6.2c).

$$\begin{aligned} nR_1 &\leq I(W_1;Y_1^n) + n\epsilon_1 && (6.5) \\ &\leq I(W_1;Y_1^n) - I(W_1;Y_2^n) + n(\epsilon_1+\epsilon_2). && (6.6) \end{aligned}$$

The inequality in (6.5) utilizes the Fano inequality, and the inequality in (6.6) utilizes the secrecy constraint $I(W_1;Y_2^n) \leq n\epsilon_2$.

Let $\epsilon = \epsilon_1 + \epsilon_2$, we can further write

$$\begin{aligned} nR_1 &\leq I(W_1;Y_1^nY_2^n) - I(W_1;Y_2^n) + n\epsilon && (6.7) \\ &= I(W_1;Y_1^n|Y_2^n) + n(\epsilon) && (6.8) \\ &\leq H(Y_1^n|Y_2^n) - H(Y_1^n|W_1X_1^nY_2^n) + n\epsilon && (6.9) \\ &\leq \sum_{i=1}^{n}[H(Y_{1,i}|Y_{2,i}) - H(Y_{1,i}|X_{1,i}Y_{2,i})] + n\epsilon, && (6.10) \end{aligned}$$

where the last step is due to the chain rule, the Markov chain $W_1 \rightarrow X_1 \rightarrow Y_1Y_2$ and the memoryless property of the channel.

For the sum rate, we have

$$\begin{aligned} nR_1 + nR_2 &\leq I(W_1;Y_1^n) - I(W_1;Y_2^n) + I(X_2^n;Y_2^n) + n\epsilon && (6.11) \\ &= I(W_1;Y_1^n) - I(W_1;Y_2^nV_1^n) + I(W_1;V_1^n|Y_2^n) + I(X_2^n;Y_2^n) + n\epsilon && (6.12) \\ &= I(W_1;Y_1^n) - I(W_1;V_1^n) - I(W_1;Y_2^n|V_1^n) + I(W_1;V_1^n|Y_2^n) \\ &\quad + I(X_2^n;Y_2^n) + n\epsilon. && (6.13) \end{aligned}$$

Define $Y_1^{i-1} = Y_{1,1} \cdots Y_{1,i-1}$, $\tilde{V}_1^{i+1} = V_{1,i+1} \cdots V_{1,n}$, $U_i = Y_1^{i-1}\tilde{V}_1^{i+1}$ and $U_{1,i} = (W_1, U_i)$. We also have

$$I(W_1; Y_1^n) - I(W_1; V_1^n) = \sum_{i=1}^{n} I(U_{1,i}; Y_{1,i}|U_i) - I(U_{1,i}; V_{1,i}|U_i). \tag{6.14}$$

The details of the intermediate steps are essentially the same as in (3.24) - (3.41), with some notation changes, in particular, the W_1 here for V in (3.24), Y_1^n here for Y^M in (3.24), V_1^n here for Z^M in (3.24), $U_{1,i}$ here for $\hat{V}_m$ in (3.41) and U_i here for U_m in (3.41). This proof is derived from [15, section V], and a similar result with a slightly different proof can be found in [51, section IV].

Due to the Markov chain $W_1 \to X_1 \to V_1 \to Y_2$,

$$I(W_1; Y_2^n|V_1^n) = 0. \tag{6.15}$$

Moreover, we can write

$$\begin{aligned}
I(W_1; V_1^n|Y_2^n) &= H(V_1^n|Y_2^n) - H(V_1^n|Y_2^n W_1) && (6.16)\\
&\leq H(V_1^n|Y_2^n) - H(V_1^n|Y_2^n X_1^n W_1) && (6.17)\\
&= H(V_1^n|Y_2^n) - H(V_1^n|Y_2^n X_1^n) && (6.18)\\
&= H(V_1^n Y_2^n) - H(Y_2^n) - H(V_1^n|Y_2^n X_1^n) && (6.19)\\
&= H(V_1^n) + H(Y_2^n|V_1^n) - H(Y_2^n) - H(V_1^n|Y_2^n X_1^n).
\end{aligned}$$

The property of the deterministic mapping (3.11) implies that

$$\begin{aligned}
I(W_1; V_1^n|Y_2^n) &\leq H(Y_2^n|X_2^n) + H(Y_2^n|V_1^n) - H(Y_2^n) - H(V_1^n|Y_2^n X_1^n)\\
&= -I(X_2^n; Y_2^n) + H(Y_2^n|V_1^n) - H(V_1^n|Y_2^n X_1^n). && (6.20)
\end{aligned}$$

So,

$$\begin{aligned} I(W_1; V_1^n | Y_2^n) + I(X_2^n; Y_2^n) &\leq H(Y_2^n|V_1^n) - H(V_1^n|Y_2^n X_1^n) && (6.21) \\ &= H(Y_2^n|V_1^n) - H(V_1^n Y_2^n|X_1^n) + H(Y_2^n|X_1^n) && (6.22) \\ &= H(Y_2^n|V_1^n) - H(V_1^n|X_1^n) - H(Y_2^n|V_1^n X_1^n) \\ &\quad + H(Y_2^n|X_1^n) && (6.23) \\ &= -H(V_1^n|X_1^n) + H(Y_2^n|X_1^n). && (6.24) \end{aligned}$$

Since all channels are memoryless, we can write

$$\begin{aligned} I(W_1; V_1^n | Y_2^n) + I(X_2^n; Y_2^n) &= \sum_{i=1}^{n} H(Y_{2,i}|Y_2^{i-1} X_1^n) - H(V_{1,i}|V_1^{i-1} X_1^n) && (6.25) \\ &\leq \sum_{i=1}^{n} H(Y_{2,i}|X_{1,i}) - H(V_{1,i}|X_{1,i}). && (6.26) \end{aligned}$$

Substituting (6.14), (6.15) and (6.26) into (6.13) and dropping the ϵ_1, ϵ_2, we get

$$\begin{aligned} n(R_1 + R_2) \leq \sum_{i=1}^{n} [&I(U_{1,i}; Y_{1,i}|U_i) - I(U_{1,i}; V_{1,i}|U_i) + H(Y_{2,i}|X_{1,i}) \\ &- H(V_{1,i}|X_{1,i})]. && (6.27) \end{aligned}$$

Introducing a random variable Q uniformly distributed over $\{1, \cdots n\}$, we can bound $R_1 + R_2$ as follows

$$\begin{aligned} n(R_1 + R_2) &\leq n \sum_{i=1}^{n} \frac{1}{n} [I(U_{1,i}; Y_{1,i}|U_i, Q = i) - I(U_{1,i}; V_{1,i}|U_i, Q = i) \\ &\quad + H(Y_{2,i}|X_{1,i}, Q = i) - H(V_{1,i}|X_{1,i}, Q = i)] \\ &= n[I(U_{1,Q}; Y_{1,Q}|U_Q, Q) - I(U_{1,Q}; V_{1,Q}|U_Q, Q) \\ &\quad + H(Y_{2,Q}|X_{1,Q}, Q) - H(V_{1,Q}|X_{1,Q}, Q)] && (6.28) \end{aligned}$$

Defining $U = (U_Q, Q)$, $U_1 = U_{1,Q}$, $V_1 = V_{1,Q}$, $X_1 = (X_{1,Q}, Q)$, $X_2 = (X_{2,Q}, Q)$, $Y_1 = (Y_{1,Q}, Q)$, $Y_2 = (Y_{2,Q}, Q)$, we can see that the conditional probabilities remain the same as the original variables, and the same Markov chain $U \to U_1 \to X_1 \to Y_1V_1$ holds. Then, we get

$$R_1 + R_2 \leq I(U_1; Y_1|U) - I(U_1; V_1|U) + H(Y_2|X_1) - H(V_1|X_1). \tag{6.29}$$

Applying the same trick to (6.10), we get the bound (6.2a) on R_1.

Since the function $Y_2 = f(X_2, V_1)$ is deterministic with property (3.11), and V_1 and X_2 are independent, we have

$$\begin{aligned} H(V_1|X_2Y_2) &= H(V_1X_2Y_2) - H(X_2Y_2) && (6.30)\\ &= H(V_1) + H(X_2|V_1) + H(Y_2|V_1X_2) - H(X_2) - H(Y_2|X_2) && (6.31)\\ &= 0. && (6.32)\end{aligned}$$

Then,

$$\begin{aligned} H(V_1|X_1) &= H(V_1) + H(X_1|V_1) - H(X_1) && (6.33)\\ &= H(Y_2|X_2) + H(X_1|V_1X_2Y_2) - H(X_1|X_2), && (6.34)\end{aligned}$$

with the last step utilizing the independence of X_1 and X_2, and of X_1 and X_2Y_2 conditioned on V_1. It follows that

$$\begin{aligned} H(V_1|X_1) &= H(Y_2|X_2) + H(X_1|X_2Y_2) + H(V_1|X_1X_2Y_2) - H(V_1|X_2Y_2)\\ &\quad - H(X_1|X_2) && (6.35)\\ &= H(X_1Y_2|X_2) - H(X_1|X_2) && (6.36)\\ &= H(Y_2|X_1X_2). && (6.37)\end{aligned}$$

With the Markov chain $U \to U_1 \to X_1 \to V_1$, a similar manipulation yields

$$H(V_1|U) = H(Y_2|X_2U) \tag{6.38}$$

and

$$H(V_1|U_1U) = H(Y_2|X_2U_1U). \tag{6.39}$$

Thus,

$$I(U_1;V_1|U) = H(V_1|U) - H(V_1|U_1U) = I(U_1;Y_2|X_2U). \tag{6.40}$$

Substituting (6.37) and (6.40) into (6.29), we get

$$\begin{aligned} R_1 + R_2 &\leq I(U_1;Y_1|U) - I(U_1;Y_2|X_2U) + H(Y_2|X_1) - H(Y_2|X_1X_2) && (6.41) \\ &= I(U_1;Y_1|U) - I(U_1;Y_2|X_2U) + I(X_2;Y_2|X_1). && (6.42) \end{aligned}$$

When the channel from X_1 to Y_1 is more capable than the channel from X_1 to V_1,

$$\begin{aligned} I(X_1;Y_1|U_1U) - I(X_1;V_1|U_1,U) &= \sum_{u_1,u}[I(X_1;Y_1|u_1,u) - I(X_1;V_1|u_1,u)]P(u_1,u) \\ &\geq 0 && (6.43) \end{aligned}$$

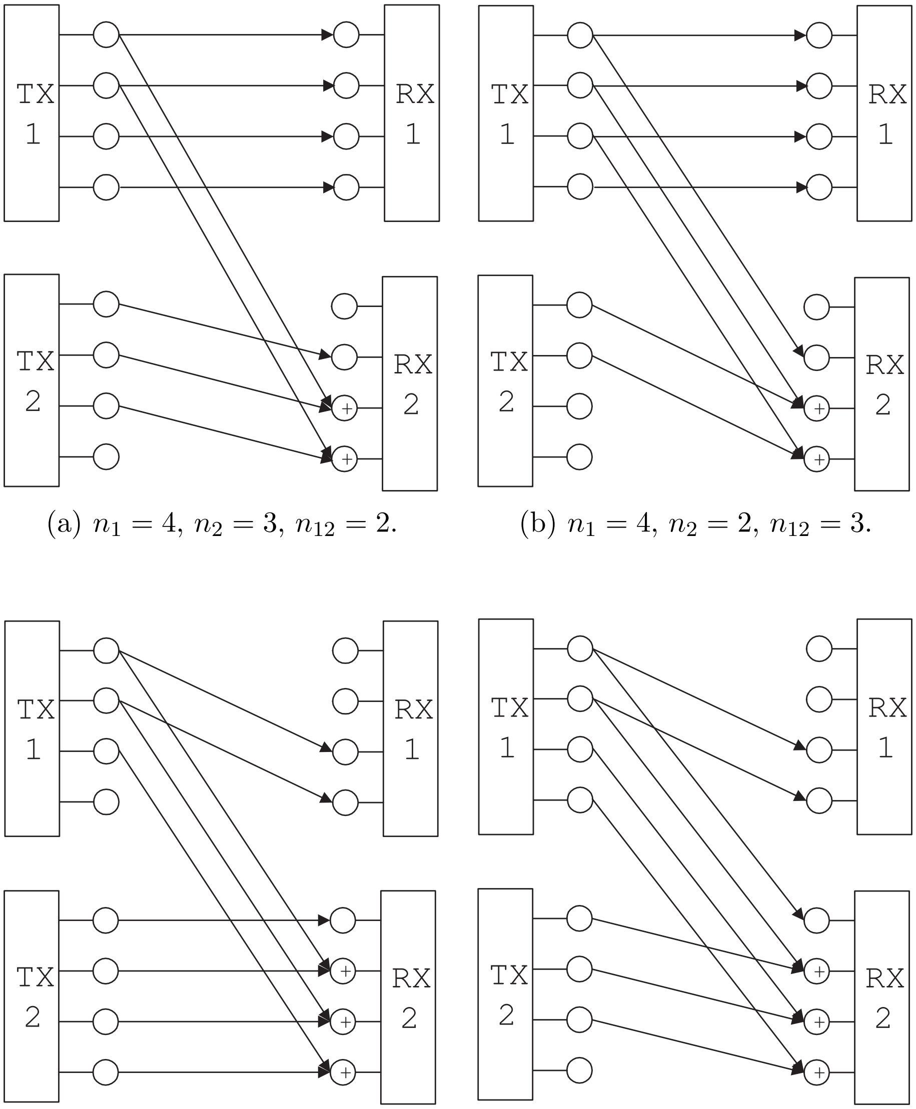
for any probability distribution $P(U_1,U)$. Therefore,

$$\begin{aligned} I(U_1;Y_1|U) - I(U_1;V_1|U) &= I(X_1;Y_1|U) - I(X_1;V_1|U) - [I(X_1;Y_1|U_1U) \\ &\quad - I(X_1;V_1|U_1U)] && (6.44) \\ &\leq I(X_1;Y_1|U) - I(X_1;V_1|U). && (6.45) \end{aligned}$$

So,

$$\begin{aligned} R_1 + R_2 &\leq I(X_1;Y_1|U) - I(X_1;V_1|U) + I(X_2;Y_2|X_1) \\ &= I(X_1;Y_1|U) - I(X_1;Y_2|X_2U) + I(X_2;Y_2|X_1). \end{aligned}$$

This completes the proof of Theorem 6.1. □



(a) $n_1 = 4$, $n_2 = 3$, $n_{12} = 2$.

(b) $n_1 = 4$, $n_2 = 2$, $n_{12} = 3$.

(c) $n_1 = 2$, $n_2 = 4$, $n_{12} = 3$.

(d) $n_1 = 2$, $n_2 = 3$, $n_{12} = 4$.

Figure 6.2: Examples of binary expansion one-sided deterministic interference channel.

6.3 Binary expansion deterministic one-sided interference channel

In this section, we consider the secrecy rate region of a binary expansion deterministic one-sided interference channel. This type of deterministic channel model was introduced in [7] as a model for the Gaussian interference channel in high SNR. Following the notation used there, we use q to denote the maximum number of binary inputs that both transmitters can have, and S to denote the $q \times q$ shift matrix

$$S = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}. \tag{6.46}$$

Among the q binary inputs of $\mathbf{x}_1$, the first n_1 bits (called the most significant bits) are delivered to receiver 1 noiselessly. In other words, the received signal $\mathbf{y}_1$ is a $(q - n_1)$ down-shifted version of the transmitted signal $\mathbf{x}_1$. Mathematically, this is

$$\mathbf{y}_1 = S^{q-n_1}\mathbf{x}_1. \tag{6.47}$$

Due to the interference link between transmitter 1 and receiver 2, receiver 2 will get n_{12} most significant bits from transmitter 1, as well as n_2 most significant bits from transmitter 2. The interaction of the interference bits and the signal bits from transmitter 2 is modeled as modulo 2. Mathematically, the received signal at receiver 2 can be written as

$$\mathbf{y}_2 = S^{q-n_{12}}\mathbf{x}_1 \oplus S^{q-n_2}\mathbf{x}_2. \tag{6.48}$$

There are four possible combinations of the ordering between n_1 and n_{12}, and n_2 and n_{12}, as listed below:

1. $n_1 \geq n_{12}$, $n_2 \geq n_{12}$;

2. $n_1 \geq n_{12}$, $n_2 < n_{12}$;

3. $n_1 < n_{12}$, $n_2 \geq n_{12}$;

4. $n_1 < n_{12}$, $n_2 < n_{12}$;

An example of each case is shown in Figure 6.2 with q = 4.

Define $x^+ = \min(x, 0)$. With the help of Theorem 6.1, we obtain the following result.

Theorem 6.2 *The secrecy capacity region of the deterministic one-sided interference channel (6.47)-(6.48) is*

$$0 \leq R_1 \leq (n_1 - (n_{12} - n_2)^+)^+, \tag{6.49a}$$

$$0 \leq R_2 \leq n_2, \tag{6.49b}$$

$$0 \leq R_1 + R_2 \leq (n_1 - n_{12})^+ + n_2. \tag{6.49c}$$

Proof: First, we label the inputs for transmitter i at level j to be $x_{i,j}$, with the highest level (most significant bit) be $j = 1$. Then, we can write down the received signal at receiver 1 explicitly as

$$\mathbf{y}_1 = (x_{1,1}, \cdots, x_{1,n_1}). \tag{6.50}$$

For receiver 2, when $n_2 \geq n_{12}$, the received signal is

$$\mathbf{y}_2 = (x_{2,1}, \cdots, x_{2,n_2-n_{12}}, x_{2,n_2-n_{12}+1} \oplus x_{1,1}, \cdots, x_{2,n_2} \oplus x_{1,n_{12}}). \tag{6.51}$$

When $n_2 < n_{12}$, the received signal is

$$\mathbf{y}_2 = (x_{1,1}, \cdots, x_{1,n_{12}-n_2}, x_{2,1} \oplus x_{1,n_{12}-n_2+1}, \cdots, x_{2,n_2} \oplus x_{1,n_{12}}). \tag{6.52}$$

Note that we omit those output levels that do not receive input signal in this representation.

To evaluate the rate bound (6.2a) for rate R_1, we note that the bound can be simplified as

$$R_1 \leq I(X_1; Y_1|Y_2) = H(Y_1|Y_2) \tag{6.53}$$

$$\leq H(Y_1) \leq n_1. \tag{6.54}$$

Moreover, when $n_2 < n_{12}$, we can tighten the bound by noticing that

$$H(Y_1|Y_2) \leq H((X_{1,1}, \cdots, X_{1,n_1})|(X_{1,1}, \cdots, X_{1,n_{12}-n_2})) \tag{6.55}$$

$$\leq (n_1 - (n_{12} - n_2))^+. \tag{6.56}$$

Combining both bounds, we get (6.49a).

The second bound (6.49b) is straightforward because it is just the capacity of the second transmitter-receiver pair's channel. Since there is no leakage of information from transmitter 2 to receiver 1, the rate bound is not affected by the secrecy requirement.

The sum rate bound (6.49c) is obtained by evaluating (6.2c). From (6.40), we can get

$$I(U_1; Y_1|U) - I(U_1; Y_2|X_2U) = I(U_1; Y_1|U) - I(U_1; V_1|U), \tag{6.57}$$

which is the secrecy capacity of the channel $X_1 \to Y_1V_1$, with V_1 being the eavesdropper's output. Since the channel $X_1 \to Y_1V_1$ is degraded one way or the other depending on the order of n_1 and n_{12},

$$I(U_1; Y_1|U) - I(U_1; V_1|U) \leq (n_1 - n_{12})^+, \tag{6.58}$$

where the equality holds when $U_1 = X_1$ if $n_1 > n_{12}$ or $U_1 = 0$ if $n_1 \leq n_{12}$ and U be a constant. Together with $I(X_2; Y_2|X_1) = H(Y_2|X_1) \leq n_2$, we get the sum rate bound (6.49c).

To prove the achievability, let us consider the cases with different ordering of n_1, n_2 and n_{12} respectively.

1. $n_1 \geq n_{12}$, $n_2 \geq n_{12}$.

For this case, the bound (6.49) is simplified to

$$0 \le R_1 \le n_1, \tag{6.59a}$$

$$0 \le R_2 \le n_2, \tag{6.59b}$$

$$0 \le R_1 + R_2 \le n_1 - n_{12} + n_2. \tag{6.59c}$$

This outer bound region is illustrated in Figure 6.3(a). We note that for this example, the outer bound is the same as the capacity region without secrecy constraint (obtained by evaluating Theorem 2 in [21]). However, the two regions are not always the same in general. To prove the achievability, we note that the outer bound is characterized by the four corner rate pairs (R_1, R_2) equaling $(n_1, 0)$, $(n_1, n_2 - n_{12})$, $(n_1 - n_{12}, n_2)$, and $(0, n_2)$. If the four corner rate pairs can be achieved, then the whole region can be achieved by time sharing. Now we will show that these four rate pairs are actually achievable.

To achieve the rate $(R_1, R_2) = (n_1, n_2 - n_{12})$, user 1 can transmit independent binary information bits through each of his 1-bit uncoded channels, while user 2 puts equiprobable random noise bits into his $n_2 - n_{12} + 1$ to n_2 1-bit channels and transmits independent uncoded information bits through the remaining $n_2 - n_{12}$ 1-bit channels. Hence, the transmission rates of user 1 and user 2 are n_1 and $n_2 - n_{12}$ respectively. The reliability of the information bits is obvious given the deterministic nature of the channel. Since the information bit is uncoded and is represented by X_1, the information leakage of user 1 is given by $I(X_1; Y_2)$. Denote

$$Y_{2,c} = (X_{2,1}, \cdots, X_{2,n_2-n_{12}}) \tag{6.60}$$

$$Y_{2,i} = (X_{2,n_2-n_{12}+1} \oplus X_{1,1}, \cdots, X_{2,n_2} \oplus X_{1,n_{12}}), \tag{6.61}$$

we can write

$$
\begin{aligned}
I(X_1; Y_2) &= I((X_{1,1}, \cdots, X_{1,n_1}); Y_{2,c}, Y_{2,i}) && (6.62)\\
&= I((X_{1,1}, \cdots, X_{1,n_1}); Y_{2,c}) + I((X_{1,1}, \cdots, X_{1,n_1}); Y_{2,i}|Y_{2,c}) && (6.63)\\
&= H(Y_{2,i}) - H(X_{2,n_2-n_{12}+1}, \cdots, X_{2,n_2}) && (6.64)\\
&= 0. && (6.65)
\end{aligned}
$$

Thus, the receiver 2 cannot get any information on X_1 from Y_2, and perfect secrecy is achieved.

To achieve the rate $(R_1, R_2) = (n_1 - n_{12}, n_2)$, user 1 can transmit binary information bits through his $n_{12} + 1$ to n_1 1-bit channels and be silent in the rest, while user 2 transmits information bits through all of his 1-bit channels. Clearly, this strategy satisfies both the reliability and the secrecy requirement.

The achievability of the other two corner rate pairs are just trivial. Thus, the outer bound is actually the capacity region. Note that by choosing the auxiliary random variables matching to the scheme here, the inner bound proposed in [51] provides the same secrecy rate.

2. $n_1 \geq n_{12}$, $n_2 < n_{12}$;

   For this case, the bound (6.49) is simplified to

$$
\begin{aligned}
&0 \leq R_2 \leq n_2, && (6.66a)\\
&0 \leq R_1 + R_2 \leq n_1 - n_{12} + n_2. && (6.66b)
\end{aligned}
$$

   This outer bound region is illustrated in Figure 6.3(b). The corner rate pairs are $(0, n_2)$, $(n_1 - n_{12}, n_2)$ and $(n_1 - n_{12} + n_2, 0)$. Rate pair $(0, n_2)$ is trivially achieved by transmitter 2 transmitting binary signal bits in all its levels while transmitter 1 keeping silent. Rate pair $(n_1 - n_{12}, n_2)$ can be achieved by transmitter 2 transmitting binary signal bits in all its levels, while transmitter 1 transmits binary signal bits only in the levels that do not generate interference at receiver 2, for example, the lowest level of user 1 in Figure 6.2(b). The number of such levels is $n_1 - n_{12}$, so user 1 gets rate $n_1 - n_{12}$. Then rate pair $(n_1 - n_{12} + n_2, 0)$ is achieved by transmitter 2 transmitting binary noise in all its levels, while transmitter 1 transmits in the lowest $n_1 - n_{12} + n_2$ levels. Among the bits transmitter 1 transmits, those in the lowest $n_1 - n_{12}$ levels are not heard by receiver 2 at all, and thus are secret. The bits in the n_2 levels above the lowest $n_1 - n_{12}$ levels will reach receiver 2. However, due to the random noise generated by transmitter 2, receiver 2 cannot derive any information on the transmitted signal. This can be proved in the similar way as that in (6.62)-(6.65).

3. $n_1 < n_{12}$, $n_2 \geq n_{12}$;

For this case, the bound (6.49) is simplified to

$$0 \leq R_1 \leq n_1 \tag{6.67a}$$

$$0 \leq R_1 + R_2 \leq n_2. \tag{6.67b}$$

This outer bound region is illustrated in Figure 6.3(c). The corner rate pairs are $(0, n_2)$ and $(n_1, n_2 - n_1)$. Rate pair $(0, n_2)$ is trivially achieved by transmitter 2 transmitting binary signal bits in all its levels while transmitter 1 keeping silent. To achieve rate pair $(n_1, n_2 - n_1)$, transmitter 1 transmits binary signal bits in its first n_1 levels. These inputs would reach level $q - n_{12} + 1$ to $q - n_{12} + n_1$ at receiver 2. So to prevent the information leakage and deafen receiver 2, transmitter 2 should transmit binary noise in the levels $2q - n_{12} - n_2 + 1$ to $2q - n_{12} - n_2 + n_1$, such that the noise would add to the information signal from transmitter 1 at receiver 2 and protect the

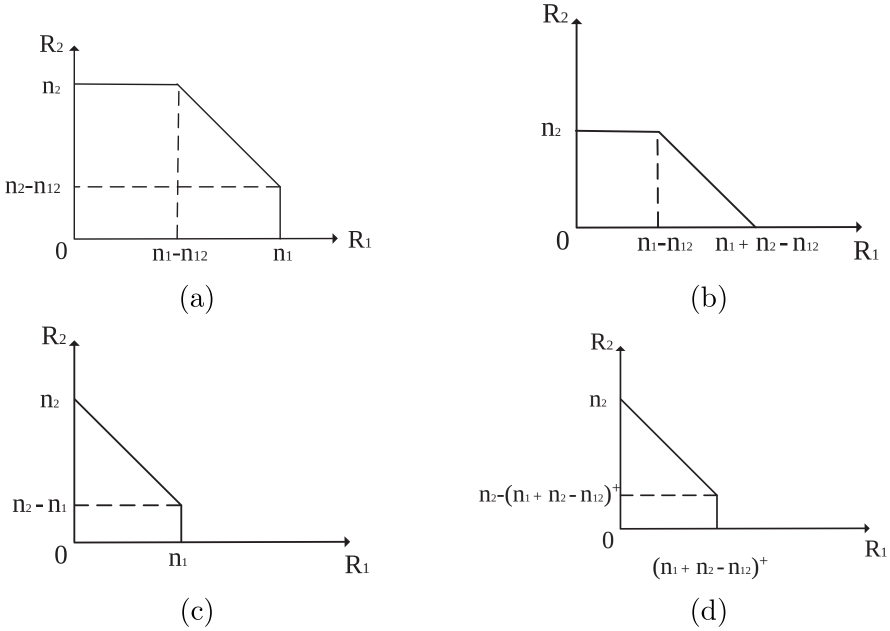


Figure 6.3: The secrecy capacity region of the one-sided deterministic interference channel. (a) $n_1 \geq n_{12}$, $n_2 \geq n_{12}$; (b) $n_1 \geq n_{12}$, $n_2 < n_{12}$; (c) $n_1 < n_{12}$, $n_2 \geq n_{12}$; (d) $n_1 < n_{12}$, $n_2 < n_{12}$;

information signal. Meanwhile, transmitter 2 can transmit binary information signal in its remaining $n_2 - n_1$ levels to get a rate $n_2 - n_1$. For example, for the channel in Figure 6.2(c), transmitter 1 will transmit information bits in its first two levels, while transmitter 2 transmits noise in its second and third level, and information bits in its first and fourth level to achieve a rate pair $(2, 2)$.

4. $n_1 < n_{12}$, $n_2 < n_{12}$;

For this case, the bound (6.49) is simplified to

$$0 \leq R_1 \leq (n_1 - n_{12} + n_2)^+, \tag{6.68a}$$

$$0 \leq R_1 + R_2 \leq n_2. \tag{6.68b}$$

This outer bound region is illustrated in Figure 6.3(c). If $n_1 - n_{12} + n_2 \leq 0$, a positive secrecy rate from transmitter 1 to receiver 1 is not possible. Otherwise, a maximum of $n_1 - n_{12} + n_2$ bits can be transmitted secretly to receiver 1. The key behind achievability is similar as in the earlier cases. That is, to achieve the rate pair $(n_1 - n_{12} + n_2, n_{12} - n_1)$, user 1 transmits binary information bit in its $n_{12} - n_2 + 1$ to n_1 levels, while user 2 transmits binary noise in its first $n_1 - n_{12} + n_2$ levels and binary information bit in its $n_1 - n_{12} + n_2 + 1$ to n_2 levels. For example, for the channel in Figure 6.2(d), transmitter 1 will transmit information bits in its second level, while transmitter 2 transmits noise in its first level, and information bits in its second and third level to achieve a rate pair $(1, 2)$.

In summary, we proved that the region defined by (6.49) is the capacity region of the deterministic one-sided interference channel (6.47) and (6.48). □

6.4 Gaussian one-sided interference channel

In this section, we consider the Gaussian one-sided interference channel

$$Y_1 = h_{11}X_1 + N_1, \tag{6.69a}$$

$$Y_2 = h_{22}X_2 + h_{12}X_1 + N_2, \tag{6.69b}$$

where N_1 and N_2 are unit variance Gaussian noise. The channel model is illustrated in Figure 6.4. Define $\overline{\mathsf{SNR}}_1 = h_{11}^2 \bar{P}_{X_1}$, $\overline{\mathsf{INR}}_1 = h_{12}^2 \bar{P}_{X_1}$, $\overline{\mathsf{SNR}}_2 = h_{22}^2 \bar{P}_{X_2}$, where $\bar{P}_{X_i}$ is the maximum average power of user i, so that $\overline{\mathsf{SNR}}_i$ and $\overline{\mathsf{INR}}_1$ are the maximum signal-to-noise ratio and interference-to-noise ratio, respectively. Since the actual transmit power might be lower than the maximum available power, we will use SNR_i and INR_1 to denote the actual signal-to-noise ratio and interference-to-noise ratio. Note that $\mathsf{SNR}_1/\mathsf{INR}_1 = \overline{\mathsf{SNR}}_1/\overline{\mathsf{INR}}_1 = h_{11}^2/h_{12}^2$. Because the capacity function of an AWGN channel $\log_2(1+x)$ (with the factor $\frac{1}{2}$ omitted for simplicity) will appear many times, we will use

$$\mathcal{C}(x) = \log_2(1+x)$$

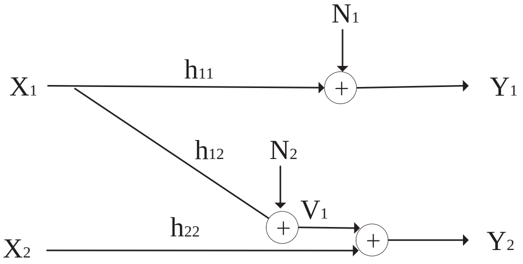


Figure 6.4: A Gaussian one-sided interference channel example.

to simplify the notation from now on.

Using Theorem 6.1, we can obtain the following outer bound.

Theorem 6.3 *An outer bound to the secrecy capacity region of the one-sided interference channel is given by*

$$0 \leq R_1 \leq \mathcal{C}\left(\overline{\mathsf{SNR}}_1 \frac{\overline{\mathsf{SNR}}_2 + 1}{\overline{\mathsf{INR}}_1 + \overline{\mathsf{SNR}}_2 + 1}\right), \tag{6.70a}$$

$$0 \leq R_2 \leq \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) \tag{6.70b}$$

$$0 \leq R_1 + R_2 \leq \left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right)\right)^+ + \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right). \tag{6.70c}$$

Proof: The outer bound is a direct application of Theorem 6.1 evaluated with Gaussian input. With $V_1 = h_{12}X_1 + N_2$, the channel $X_1 \to Y_1, V_1$ is equivalent to a broadcast AWGN channel. Due to (6.40), we can write

$$I(U_1; Y_1|U) - I(U_1; Y_2|X_2U) = I(U_1; Y_1|U) - I(U_1; V_1|U).$$

The right side is maximized by Gaussian input $U_1 = X_1$ with maximum power and a constant U [17, 38] when $\overline{\mathsf{SNR}}_1 \geq \overline{\mathsf{INR}}_1$, and is zero otherwise. Meanwhile, Gaussian X_2 maximizes $I(X_2; Y_2|X_1)$. So, Gaussian input maximizes (6.2c). Evaluating (6.2c) with Gaussian input, we can obtain the outer bound (6.70c). The bound (6.70b) is self-evident.

We will prove the first bound (6.70a) below.

$$R_1 \leq I(X_1;Y_1|Y_2) \tag{6.71}$$

$$= I(X_1;Y_1Y_2) - I(X_1;Y_2) \tag{6.72}$$

$$= I(X_1X_2;Y_1Y_2) - I(X_2;Y_1Y_2|X_1) - I(X_1X_2;Y_2) + I(X_2;Y_2|X_1) \tag{6.73}$$

$$= I(X_1X_2;Y_1Y_2) - I(X_1X_2;Y_2), \tag{6.74}$$

where the last equality follows the independence between X_2 and Y_1 conditioned on X_1. The right hand side of (6.74) is equivalent to the secrecy capacity of a wiretap channel with two independent inputs X_1 and X_2, and the intended receiver receives both Y_1 and Y_2, while the eavesdropper receives only Y_2. So, the intended receiver has a less noisy channel. Since full power Gaussian inputs maximize both $I(X_1X_2;Y_1Y_2)$ and $I(X_1X_2;Y_2)$, it will maximize the right side of (6.74) as well [17]. Therefore, we can continue to write

$$R_1 \leq I(X_1X_2;Y_1Y_2) - I(X_1X_2;Y_2) \tag{6.75}$$

$$= H(Y_1Y_2) - H(N_1N_2) - H(Y_2) + H(N_2) \tag{6.76}$$

$$\leq \frac{1}{2}\log\left((2\pi e)^2|\Lambda|\right) - \frac{1}{2}\log\left((2\pi e)(h_{12}^2\bar{P}_{X_1} + h_{22}^2\bar{P}_{X_2} + 1)\right) - H(N_1) \tag{6.77}$$

$$= \frac{1}{2}\log\left(|\Lambda|\right) - \frac{1}{2}\log\left(h_{12}^2\bar{P}_{X_1} + h_{22}^2\bar{P}_{X_2} + 1\right), \tag{6.78}$$

where Λ is the covariance of the joint Gaussian distribution Y_1Y_2, given by

$$\Lambda = \begin{pmatrix} h_{11}^2\bar{P}_{X_1} + 1 & h_{11}h_{12}\bar{P}_{X_1} \\ h_{11}h_{12}\bar{P}_{X_1} & h_{12}^2\bar{P}_{X_1} + h_{22}^2\bar{P}_{X_2} + 1 \end{pmatrix}. \tag{6.79}$$

To be consistent with the earlier simplification, we omit the factor 1/2 and get

$$R_1 \le \log\left((h_{11}^2\bar{P}_{X_1}+1)(h_{12}^2\bar{P}_{X_1}+h_{22}^2\bar{P}_{X_2}+1)-h_{11}^2h_{12}^2\bar{P}_{X_1}^2\right)$$

$$-\log\left(h_{12}^2\bar{P}_{X_1}+h_{22}^2\bar{P}_{X_2}+1\right) \tag{6.80}$$

$$=\log\left((h_{11}^2\bar{P}_{X_1}+1)-\frac{h_{11}^2h_{12}^2\bar{P}_{X_1}^2}{h_{12}^2\bar{P}_{X_1}+h_{22}^2\bar{P}_{X_2}+1}\right) \tag{6.81}$$

$$=\mathcal{C}\left(\overline{\mathsf{SNR}}_1-\frac{\overline{\mathsf{SNR}}_1\overline{\mathsf{INR}}_1}{\overline{\mathsf{INR}}_1+\overline{\mathsf{SNR}}_2+1}\right) \tag{6.82}$$

$$=\mathcal{C}\left(\overline{\mathsf{SNR}}_1\frac{\overline{\mathsf{SNR}}_2+1}{\overline{\mathsf{INR}}_1+\overline{\mathsf{SNR}}_2+1}\right), \tag{6.83}$$

which is the rate bound (6.70a). □

When $\overline{\mathsf{SNR}}_1 \ge \overline{\mathsf{INR}}_1$, (6.70c) is just

$$R_1+R_2 \le \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right)-\mathcal{C}\left(\overline{\mathsf{INR}}_1\right)+\mathcal{C}\left(\overline{\mathsf{SNR}}_2\right).$$

Combine this with the bound (6.70a), we can get that

$$R_1 \le \min\left\{\mathcal{C}\left(\overline{\mathsf{SNR}}_1\frac{\overline{\mathsf{SNR}}_2+1}{\overline{\mathsf{INR}}_1+\overline{\mathsf{SNR}}_2+1}\right), \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right)-\mathcal{C}\left(\overline{\mathsf{INR}}_1\right)+\mathcal{C}\left(\overline{\mathsf{SNR}}_2\right)\right\} \tag{6.84}$$

$$\le \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right)-\left(\mathcal{C}\left(\overline{\mathsf{INR}}_1\right)-\mathcal{C}\left(\overline{\mathsf{SNR}}_2\right)\right)^+. \tag{6.85}$$

Note that the last step above actually loosens the upper bound for R_1. However, it works fine when $\overline{\mathsf{SNR}}_1 \ge \overline{\mathsf{INR}}_1$ in the sense that it can be shown that this loose upper bound can still be achieved within a 1 bit gap. It also provides a good analogy to the binary deterministic channel. Therefore, we will use it as the bound for R_1 when $\overline{\mathsf{SNR}}_1 \ge \overline{\mathsf{INR}}_1$ and rewrite the outer bound region as

$$R_1 \le \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right)-\left(\mathcal{C}\left(\overline{\mathsf{INR}}_1\right)-\mathcal{C}\left(\overline{\mathsf{SNR}}_2\right)\right)^+, \tag{6.86a}$$

$$R_2 \le \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right), \tag{6.86b}$$

$$R_1+R_2 \le \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right)-\mathcal{C}\left(\overline{\mathsf{INR}}_1\right)+\mathcal{C}\left(\overline{\mathsf{SNR}}_2\right). \tag{6.86c}$$

For this case, we can obtain the achievability result stated in the following theorem.

Theorem 6.4 *When $\overline{\mathsf{SNR}}_1 \geq \overline{\mathsf{INR}}_1$, the region*

$$R_1 \leq \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \left(\mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right)\right)^+ - 1 \tag{6.87a}$$

$$R_2 \leq \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - 1 \tag{6.87b}$$

$$R_1 + R_2 \leq \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) + \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 2 \tag{6.87c}$$

is achievable, which is within one bit of the outer bound (6.86).

Proof: To prove the result on achievable rates, we note that both the outer bound and the achievable rate region in Theorem 6.4 have the same shape as that in Figure 6.3(a) when $\overline{\mathsf{SNR}}_2 > \overline{\mathsf{INR}}_1$, and Figure 6.3(b) when $\overline{\mathsf{SNR}}_2 \leq \overline{\mathsf{INR}}_1$, with n_1, n_2 and n_{12} being replaced by $\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right)$, $\mathcal{C}\left(\overline{\mathsf{SNR}}_2\right)$ and $\mathcal{C}\left(\overline{\mathsf{INR}}_1\right)$ respectively for outer bound or being replaced by $\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - 1$, $\mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - 1$ and $\mathcal{C}\left(\overline{\mathsf{INR}}_1\right)$ respectively for the achievable rate region. The achievable rate region is within one bit (the sum rate is within two bits for the two users) of the outer bound. This is similar to the result in [18], which proposed a scheme to come within one bit of the outer bound of the Gaussian interference channel.

When $\overline{\mathsf{SNR}}_2 > \overline{\mathsf{INR}}_1$, the rate region defined by (6.87) is characterized by the four corner rate pairs

$$\begin{aligned}
(R_1, R_2) &= \left(0, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - 1\right), \\
(R_1, R_2) &= \left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - 1\right), \\
(R_1, R_2) &= \left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - 1, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1\right), \\
(R_1, R_2) &= \left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - 1, 0\right).
\end{aligned}$$

When $\overline{\mathsf{SNR}}_2 < \overline{\mathsf{INR}}_1$, the last two corner rate pairs are replaced by one at

$$(R_1, R_2) = \left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) + \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1, 0\right).$$

If we can achieve these corner rate pairs, by time sharing we can achieve the whole region. Now we will show we can actually achieve higher rates than these corner rate pairs with Gaussian signaling.

1. As $\left(0, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right)\right)$ is trivially achievable with $X_1 = 0$ and X_2 maximum power with Gaussian signaling, so is the corner rate pair $\left(0, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - 1\right)$.

2. To achieve the rate pair $\left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - 1\right)$, we set the power of X_1 to be $P_{X_1} = \min\{1/h_{12}^2, \bar{P}_{X_1}\}$ so that the actual interference to noise ratio at receiver 2 caused by user 1 is $\mathsf{INR}_1 = \min\{1, \overline{\mathsf{INR}}_1\}$. User 2 uses the usual deterministic Gaussian signaling with full power and treats the interference from user 1 as noise. Since user 2 uses a deterministic encoding, receiver 2 can strip X_2 off after decoding the message from the transmitter 2. Receiver 2 then gets a clean look at V_1. For user 1, this is simply a Gaussian broadcast channel, whose secrecy capacity is given by the difference between the capacity of the $X_1 \rightarrow Y_1$ channel and the capacity of the $X_1 \rightarrow V_1$ channel, using the result in [17, 38]. Thus, the rate achievable by this scheme is

$$R_1 = \mathcal{C}\left(\mathsf{SNR}_1\right) - \mathcal{C}\left(\mathsf{INR}_1\right) \tag{6.88}$$

$$= \mathcal{C}\left(\frac{\overline{\mathsf{SNR}}_1 \mathsf{INR}_1}{\overline{\mathsf{INR}}_1}\right) - \mathcal{C}\left(\mathsf{INR}_1\right) \tag{6.89}$$

$$= \mathcal{C}\left(\min\left\{\frac{\overline{\mathsf{SNR}}_1}{\overline{\mathsf{INR}}_1}, \overline{\mathsf{SNR}}_1\right\}\right) - \mathcal{C}\left(\min\{1, \overline{\mathsf{INR}}_1\}\right), \tag{6.90}$$

$$R_2 = \mathcal{C}\left(\frac{\overline{\mathsf{SNR}}_2}{\mathsf{INR}_1 + 1}\right) = \mathcal{C}\left(\frac{\overline{\mathsf{SNR}}_2}{\min\{1, \overline{\mathsf{INR}}_1\} + 1}\right). \tag{6.91}$$

If $\overline{\mathsf{INR}}_1 \leq 1$, $R_1 = \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right)$. Otherwise, $\overline{\mathsf{INR}}_1 > 1$ and

$$R_1 = \mathcal{C}\left(\frac{\overline{\mathsf{SNR}}_1}{\overline{\mathsf{INR}}_1}\right) - 1 > \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1. \tag{6.92}$$

We also have

$$R_2 \geq \mathcal{C}\left(\frac{\overline{\mathsf{SNR}}_2}{2}\right) > \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - 1. \tag{6.93}$$

Thus, the achievable rate pair with this scheme is higher than the corner rate pair $\left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - 1\right)$.

3. When $\overline{\mathsf{SNR}}_2 > \overline{\mathsf{INR}}_1$, the rate outer bound region has the shape in Figure 6.3(a). In order to achieve the rate pair $\left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - 1, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1\right)$, we let $X_2 = U_2 + A_2$, where U_2 is an information bearing signal with power P_U, and A_2 is an independent artificial noise with power $P_A = P_{X_2} - P_U$. Define $\mathsf{SNR}_U = h_{22}^2 P_U$, and $\mathsf{SNR}_A = h_{22}^2 P_A$. Moreover, we choose the power of P_U and P_A such that $\mathsf{SNR}_A = \max\{\overline{\mathsf{INR}}_1 - 1, 0\}$ and $\mathsf{SNR}_U + \mathsf{SNR}_A = \overline{\mathsf{SNR}}_2$. Deterministic coding is used for the information bearing signal U_2, with A_2 being considered as random Gaussian noise. So, after decoding the message, receiver 2 can strip U_2 off, but not A_2. Thus, transmitter 1 effectively faces a broadcast channel with the intended receiver facing the additive white Gaussian noise N_1, and the eavesdropper (receiver 2) facing the additive white noise $N_2 + h_{22}A_2$. With similar reasoning as earlier, we can get the achievable secrecy rate be

$$R_1 = \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \mathcal{C}\left(\frac{\overline{\mathsf{INR}}_1}{\mathsf{SNR}_A + 1}\right), \tag{6.94}$$

$$R_2 = \mathcal{C}\left(\frac{\mathsf{SNR}_U}{\mathsf{SNR}_A + \overline{\mathsf{INR}}_1 + 1}\right). \tag{6.95}$$

Moreover,

$$R_1 \geq \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - 1, \tag{6.96}$$

$$\begin{aligned} R_2 &= \mathcal{C}\left(\overline{\mathsf{SNR}}_2 + \overline{\mathsf{INR}}_1\right) - \mathcal{C}\left(\mathsf{SNR}_A + \overline{\mathsf{INR}}_1\right) && (6.97)\\ &\geq \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\max\{2\overline{\mathsf{INR}}_1 - 1, \overline{\mathsf{INR}}_1\}\right) && (6.98)\\ &> \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1 && (6.99) \end{aligned}$$

Thus, the achievable rate pair with this scheme is higher than the corner rate pair $\left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - 1, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1\right)$.

4. When $\overline{\mathsf{SNR}}_2 \leq \overline{\mathsf{INR}}_1$, the rate outer bound region has the shape in Figure 6.3(b). In order to achieve the rate pair $\left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) + \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1, 0\right)$, we set $P_{X_1} = \min\{(h_{22}^2 \bar{P}_{X_2} + 1)/h_{12}^2, \bar{P}_{X_1}\}$ so that the actual interference to noise ratio at receiver 2 caused by user 1 is $\mathsf{INR}_1 = \min\{\overline{\mathsf{SNR}}_2 + 1, \overline{\mathsf{INR}}_1\}$. Also, since the rate for the second transmitter-receiver pair is zero, transmitter 2 can transmit white Gaussian noise with all its power $\bar{P}_{X_2}$. The achievable rate of this scheme is

$$\begin{aligned} R_1 &= \mathcal{C}\left(\mathsf{SNR}_1\right) - \mathcal{C}\left(\frac{\mathsf{INR}_1}{\overline{\mathsf{SNR}}_2 + 1}\right) && (6.100)\\ &= \mathcal{C}\left(\min\left\{\frac{\overline{\mathsf{SNR}}_1(\overline{\mathsf{SNR}}_2 + 1)}{\overline{\mathsf{INR}}_1}, \overline{\mathsf{SNR}}_1\right\}\right) - \mathcal{C}\left(\frac{\min\{\overline{\mathsf{SNR}}_2 + 1, \overline{\mathsf{INR}}_1\}}{\overline{\mathsf{SNR}}_2 + 1}\right), && (6.101)\\ R_2 &= 0. && (6.102) \end{aligned}$$

When $\overline{\mathsf{INR}}_1 \geq \overline{\mathsf{SNR}}_2 + 1$, $\mathsf{INR}_1 = \overline{\mathsf{SNR}}_2 + 1$, and the rate R_1 can be bounded as

$$\begin{aligned} R_1 &= \mathcal{C}\left(\frac{\overline{\mathsf{SNR}}_1(\overline{\mathsf{SNR}}_2 + 1)}{\overline{\mathsf{INR}}_1}\right) - \mathcal{C}\left(1\right) && (6.103)\\ &= \log_2\left(\frac{\overline{\mathsf{INR}}_1}{\overline{\mathsf{SNR}}_2 + 1} + \overline{\mathsf{SNR}}_1\right) + \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \log_2(\overline{\mathsf{INR}}_1) - 1 && (6.104)\\ &\geq \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) + \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1. && (6.105) \end{aligned}$$

When $\overline{\mathsf{SNR}}_2 < \overline{\mathsf{INR}}_1 < \overline{\mathsf{SNR}}_2 + 1$, $\mathsf{INR}_1 = \overline{\mathsf{INR}}_1$, and the rate R_1 can be bounded as

$$\begin{aligned} R_1 &= \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \mathcal{C}\left(\frac{\overline{\mathsf{INR}}_1}{\overline{\mathsf{SNR}}_2 + 1}\right) && (6.106)\\ &= \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) + \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\overline{\mathsf{SNR}}_2 + \overline{\mathsf{INR}}_1\right) && (6.107)\\ &\geq \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) + \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(2\overline{\mathsf{INR}}_1\right) && (6.108)\\ &\geq \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) + \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\overline{\mathsf{INR}}_1\right) - 1. && (6.109) \end{aligned}$$

So for both cases, the outer bound of R_1 is achieved within one bit.

5. Finally, when $\overline{\mathsf{SNR}}_2 > \overline{\mathsf{INR}}_1$, by making $X_2 = A_2$ and $\mathsf{SNR}_A = \overline{\mathsf{SNR}}_2$, i.e., user 2 does not transmit an information bearing signal but pure Gaussian white noise, we achieve the rate

$$\begin{aligned} R_1 &= \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \mathcal{C}\left(\frac{\overline{\mathsf{INR}}_1}{\overline{\mathsf{SNR}}_2 + 1}\right) && (6.110)\\ R_2 &= 0. && (6.111) \end{aligned}$$

Clearly, $R_1 > \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - 1$. So, we achieve a better rate rate than the corner rate pair $\left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - 1, 0\right)$.

Since all corner rate pairs of the region defined by (6.87) can be achieved, the whole region can be achieved with time sharing. □

When $\overline{\mathsf{SNR}}_1 < \overline{\mathsf{INR}}_1$, (6.70c) becomes

$$R_1 + R_2 \leq \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right),$$

which makes bound (6.70b) redundant. If

$$\overline{\mathsf{SNR}}_1 \frac{\overline{\mathsf{SNR}}_2 + 1}{\overline{\mathsf{INR}}_1 + \overline{\mathsf{SNR}}_2 + 1} < \overline{\mathsf{SNR}}_2, \tag{6.112}$$

which is equivalent to

$$\overline{\mathsf{INR}}_1 > (\overline{\mathsf{SNR}}_2 + 1)\left(\frac{\overline{\mathsf{SNR}}_1}{\overline{\mathsf{SNR}}_2} - 1\right), \tag{6.113}$$

the outer bound will have four sides (including the axis) and are characterized by the rate pairs

$$(R_1, R_2) = \left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1 \frac{\overline{\mathsf{SNR}}_2 + 1}{\overline{\mathsf{INR}}_1 + \overline{\mathsf{SNR}}_2 + 1}\right), 0\right) \tag{6.114a}$$

$$(R_1, R_2) = \left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1 \frac{\overline{\mathsf{SNR}}_2 + 1}{\overline{\mathsf{INR}}_1 + \overline{\mathsf{SNR}}_2 + 1}\right), \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right) - \mathcal{C}\left(\overline{\mathsf{SNR}}_1 \frac{\overline{\mathsf{SNR}}_2 + 1}{\overline{\mathsf{INR}}_1 + \overline{\mathsf{SNR}}_2 + 1}\right)\right), \tag{6.114b}$$

$$(R_1, R_2) = \left(0, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right)\right). \tag{6.114c}$$

Otherwise, bound (6.70a) will also be redundant, and the outer bound will have a triangle shape that is characterized by the rate pairs $(\mathcal{C}\left(\overline{\mathsf{SNR}}_2\right), 0)$ and $(0, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right))$.

With the similar strategy as before, we can achieve the rate region stated as following.

Theorem 6.5 *When $\overline{\mathsf{SNR}}_1 \leq \overline{\mathsf{INR}}_1 \leq \overline{\mathsf{SNR}}_2 + 1$, the four-sided region defined by the origin and the following three corner points*

$$(R_1, R_2) = \left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \mathcal{C}\left(\frac{\overline{\mathsf{INR}}_1}{\overline{\mathsf{SNR}}_2 + 1}\right), 0\right), \tag{6.115a}$$

$$(R_1, R_2) = \left(\mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - 1, \mathcal{C}\left(\overline{\mathsf{SNR}}_2 + \overline{\mathsf{INR}}_1\right) - \mathcal{C}\left(\max\{2\overline{\mathsf{INR}}_1 - 1, \overline{\mathsf{INR}}_1\}\right)\right), \tag{6.115b}$$

$$(R_1, R_2) = \left(0, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right)\right), \tag{6.115c}$$

is achievable.

Proof: The achievability scheme is similar as before. The first corner rate pair is achieved by transmitter 2 transmits noise while transmitter 1 transmits Gaussian codewords with stochastic coding. The second rate pair is achieved by letting user 1 transmit at full power with Gaussian codes, while user 2 transmits $X_2 = U_2 + A_2$, where U_2 is an information bearing signal with power P_U, and A_2 is an independent artificial noise with power $P_A = P_{X_2} - P_U$. Moreover, the power of P_U and P_A are chosen such that $\mathsf{SNR}_A = \max\{\overline{\mathsf{INR}}_1 - 1, 0\}$ and $\mathsf{SNR}_U = \overline{\mathsf{SNR}}_2 - \mathsf{SNR}_A$. With the same reasoning as earlier, we can get the achievable secrecy rate be

$$R_1 = \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - \mathcal{C}\left(\frac{\overline{\mathsf{INR}}_1}{\mathsf{SNR}_A + 1}\right), \tag{6.116}$$

$$\geq \mathcal{C}\left(\overline{\mathsf{SNR}}_1\right) - 1, \tag{6.117}$$

$$R_2 = \mathcal{C}\left(\frac{\mathsf{SNR}_U}{\mathsf{SNR}_A + \overline{\mathsf{INR}}_1 + 1}\right) \tag{6.118}$$

$$= \mathcal{C}\left(\overline{\mathsf{SNR}}_2 + \overline{\mathsf{INR}}_1\right) - \mathcal{C}\left(\mathsf{SNR}_A + \overline{\mathsf{INR}}_1\right) \tag{6.119}$$

$$= \mathcal{C}\left(\overline{\mathsf{SNR}}_2 + \overline{\mathsf{INR}}_1\right) - \mathcal{C}\left(\max\{2\overline{\mathsf{INR}}_1 - 1, \overline{\mathsf{INR}}_1\}\right) \tag{6.120}$$

The third rate pair is achieved trivially by transmitter 1 being silent, and transmitter 2 transmits at his own capacity. Since all corner rate pairs are achievable, the whole region can be achieved with time sharing. □

We note that although (6.115a) and (6.115c) are within 1 bit of the outer bound corner rate pair (6.114a) and (6.114c), (6.115b) might be not. In particular, consider the case where $\overline{\mathsf{INR}}_1 = \overline{\mathsf{SNR}}_2 + 1$, then (6.115b) gives zero rate for user 2, while the outer bound (6.114b) can be non-zero. So, either a better bound or a more complicated signaling strategy is necessary to reduce the gap.

When $\overline{\mathsf{INR}}_1 > \overline{\mathsf{SNR}}_2 + 1$, the power of transmitter 2 is not enough to hide the message sent by the transmitter 1. For this case, transmitter 1 has to lower its signal power for secrecy. Specifically, user 1 can transmit at the power $P_{X_1} = (h_{22}^2 \bar{P}_{X_2} + 1)/h_{12}^2$ such that the interference it generates at receiver 2 is $\mathsf{INR}_1 = \overline{\mathsf{SNR}}_2 + 1$. Then, transmitter 2 can transmit white Gaussian noise with all its power $\bar{P}_{X_2}$. The achievable rate of this scheme is

$$R_1 = \mathcal{C}\left(\mathsf{SNR}_1\right) - \mathcal{C}\left(\frac{\mathsf{INR}_1}{\overline{\mathsf{SNR}}_2 + 1}\right) \tag{6.121}$$

$$= \mathcal{C}\left(\frac{\overline{\mathsf{SNR}}_1(\overline{\mathsf{SNR}}_2 + 1)}{\overline{\mathsf{INR}}_1}\right) - 1 \tag{6.122}$$

$$R_2 = 0. \tag{6.123}$$

To summarize, we have the following theorem.

Theorem 6.6 *When* $\overline{\mathsf{SNR}}_1 \leq \overline{\mathsf{INR}}_1$, *and* $\overline{\mathsf{SNR}}_2 + 1 \leq \overline{\mathsf{INR}}_1$, *the triangle defined by the origin and the following two corner points*

$$(R_1, R_2) = \left(\mathcal{C}\left(\frac{\overline{\mathsf{SNR}}_1(\overline{\mathsf{SNR}}_2 + 1)}{\overline{\mathsf{INR}}_1}\right) - 1, 0\right) \tag{6.124a}$$

$$(R_1, R_2) = \left(0, \mathcal{C}\left(\overline{\mathsf{SNR}}_2\right)\right). \tag{6.124b}$$

is achievable.

We note that the achievable rate (6.124a) is within 1 bit gap to the outer bound rate pair (6.114a) because

$$\mathcal{C}\left(\frac{\overline{\mathsf{SNR}}_1(\overline{\mathsf{SNR}}_2 + 1)}{\overline{\mathsf{INR}}_1}\right) > \mathcal{C}\left(\overline{\mathsf{SNR}}_1 \frac{\overline{\mathsf{SNR}}_2 + 1}{\overline{\mathsf{INR}}_1 + \overline{\mathsf{SNR}}_2 + 1}\right). \tag{6.125}$$

However, due to the outer bound rate pair (6.115b) when (6.113) is satisfied, a significant gap can exist between the achievable rate and the outer bound. Again, either a better bound or a more complicated signaling strategy is necessary to reduce the gap.

6.5 Discussion

In this chapter, we derived an outer bound for the secrecy capacity region of the one-sided interference channel. The outer bound is shown to be tight for the binary expansion deterministic channel. For the Gaussian one-sided interference channel, the outer bound is evaluated and is shown to be achievable within one bit when the interference channel is noisier than the corresponding main channel, i.e. $\overline{\mathsf{SNR}}_1 \geq \overline{\mathsf{INR}}_1$. The achievability scheme used for Gaussian channel is analogous to that used for the binary expansion deterministic channel counter part. This is not surprising as it was illustrated in [7] that the deterministic channel can serve as a good approximation of the Gaussian channel.

For the one-sided Gaussian channel with $\overline{\mathsf{SNR}}_1 < \overline{\mathsf{INR}}_1$, the achievable rates are not always within a constant gap to the outer bound. Comparing to the binary expansion deterministic channel counterpart, we can see that, the major difference between the binary channel and the Gaussian channel is that the former can easily deploy independent coding for each input level so that information-bearing signal in low SNR can be transmitted despite of the noise at high SNR, and thus can assign the levels in an optimal way without wasting any power. Therefore, a more complicated coding scheme for Gaussian channels might be needed to reduce the gap between the achievable rates and the outer bounds.

Chapter 7

Secrecy Rate with Practical Signaling

So far in this thesis, we have been mainly focused on the performance of Gaussian random codes for secret communication. However, in a practical digital communication system, Gaussian random codes cannot be implemented. Instead, the input often has a finite alphabet, and thus discrete signaling is actually used, such as Quadrature Amplitude Modulation (QAM) or Phase Shift Keying (PSK). For communication without a secrecy requirement, coding across time is often used to achieve a reliable communicate rate close to the mutual information between the channel input and channel output. However, this rate is always limited by the size of the underlying constellations, and is always smaller than the capacity that is achievable with the optimal Gaussian codes. Increasing the size of the constellation will reduce the gap to the capacity. For the same input constellation, increasing the signal power results in a larger SNR, and thus better error performance. Does discrete signaling have a similar influence on secret communication? This is the main question we want to address in this chapter.

In this work, we examine the information-theoretic limits behind secret communication using practical, discrete modulation schemes. Since much of the analysis leads to unwieldy equations, we will often resort to numerical evaluations. We focus on both the AWGN channel and the fading channel studied in earlier chapters, and we observe that the effect of discrete signaling is different for the two channels. Unlike prior Gaussian coding secrecy results, where a larger transmission power is always better, for discrete constellations, there exists an optimal power level beyond which additional power helps an eavesdropper and hurts secret communication. For the AWGN channel, a larger constellation is always better, while for the fading channel, the optimal constellation size varies with the power constraint and can even perform better than random Gaussian coding! The result also reflects the difficulty of finding the optimal input for fast fading channels.

7.1 Problem setup

7.1.1 Channel models

There will be two primary wireless channel models that we will consider in this chapter: the AWGN broadcast channel, and the fading broadcast channel.

AWGN Broadcast Channel: The first communication model that we shall consider is the real AWGN broadcast channel

$$Y = \sqrt{b}X + W_1, \tag{7.1a}$$

$$Z = X + W_2, \tag{7.1b}$$

where X is the signal transmitted by Alice, Y is the signal received by Bob, and Z is the signal received by EVE respectively, W_1 and W_2 are white Gaussian noise with unit power, b is Bob's channel gain normalized by Eve's channel gain, and Eve's channel gain is normalized to 1.

Fading Broadcast Channel:

The second model we consider is a fading broadcast channel where the main channel (Alice→Bob) is a constant AWGN channel and the eavesdropper channel is fast Rayleigh fading. The realizations of the fading channel are known to the eavesdropper only, and the transmitter just knows the fading statistics. This model was described in Chapter 4, where the performance of Gaussian signaling was discussed. Mathematically, the channel model is

$$Y = \sqrt{b}X + W_1, \tag{7.2a}$$

$$Z = \sqrt{G}X + W_2 \tag{7.2b}$$

where W_1 and W_2 are white Gaussian noise of unit variance, b is Bob's channel gain normalized by Eve's *average* channel gain, and Eve's channel gain G is an exponential random variable because of Rayleigh fading. The mean of G is normalized to one. Note that the fast fading assumption instead of slow fading is very important. For a slow fading Gaussian channel, it has been shown in [23] that a Gaussian two-tier signaling scheme is secrecy-capacity-achieving. But for a fast fading Gaussian channel, the secrecy capacity is still unknown so far, and as we will shown later, Gaussian signaling is not always optimal.

7.1.2 Discrete modulation scheme

Gaussian coding has served as the basis for studying the conventional capacity of communications systems. In practice, however, discrete input constellations, such as BPSK and QPSK, are used instead. One notable reason for this is that discrete coding has an easier implementation at both the transmitter and the receiver, although it suffers the price of reduced communication rate.

In this work, we shall consider quadrature amplitude modulation (QAM) because of its simplicity and popularity. The observations we make here for QAM will apply to other discrete constellation as well. Note that for QAM modulation, the transmitted signal is complex since it has both the in-phase and the quadrature components. The channel attenuation is often complex as well. However, since both the intended receiver and the eavesdropper are assumed to know their channel states, they can compensate for the channel phase rotation and reduce the channel to two real sub-channels with identical channel gain (but independent noise), one for each input dimension. Hence, we use the real AWGN channel model (7.1) and the real fading channel model (7.2) for mathematical simplicity, while keeping in mind that they only represent one component of the actual channel.

Quadrature Amplitude Modulation: The signal space representation of QAM signaling is

$$\mathbf{x}_i = \begin{bmatrix} a_i \\ b_i \end{bmatrix}, \qquad i = 1, \cdots, M, \tag{7.3}$$

where a_i and b_i are the amplitudes of the quadratic carriers of the information bearing signal. The constellation points are equally spaced and are equally probable. In this work, we consider the case for $M = 4, 16, 64$, so a_i and b_i each takes the value from $\{(-\sqrt{M}+2i-1)d\}$ for $i = 1, \cdots, \sqrt{M}$ with equal probability. d is chosen such that the average symbol power is P. With some algebra, we can calculate d to be

$$d = \sqrt{\frac{\sqrt{M}P}{2\sum_{i=1}^{\sqrt{M}}(-\sqrt{M}+2i-1)^2}}. \tag{7.4}$$

For example, the constellation for 16-QAM is shown in Figure 7.1, where $d = \sqrt{P/10}$.

When the input X is distributed over the discrete set $\{\mathbf{x}_i\}$, the probability distribution function of X can be written as

$$f_X(\mathbf{x}) = \sum_{i=1}^{M} p_i \delta(\mathbf{x} - \mathbf{x}_i), \tag{7.5}$$

where p_i is the probability of $\mathbf{x} = \mathbf{x}_i$, and M is the total number of possible x values. For QAM, all constellation points are equally likely, so $p_i = 1/M$.

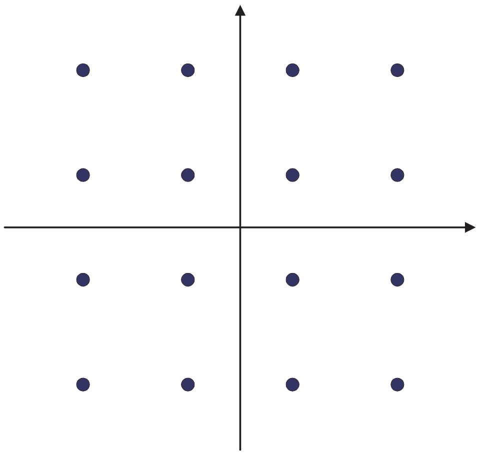


Figure 7.1: Signal constellation for 16-QAM modulation

7.2 Secrecy rate in AWGN scenarios

We begin with the real AWGN broadcast channel described in Section 7.1. It has been shown in [38] that the secrecy capacity of this channel in bits per channel use with a power constraint P is

$$\mathcal{C}_s = \frac{1}{2}[\log_2(1+bP) - \log_2(1+P)]^+, \tag{7.6}$$

and that a Gaussian input of power P achieves the secrecy capacity. The secrecy capacity is exactly the difference between the main channel's mutual information and the eavesdropper's channel mutual information. To achieve a positive secrecy capacity, the main channel normalized channel gain b must be greater than 1.

Gaussian coding, however, is not practical, and thus it is important to consider the implications of discrete input constellations on the secrecy rate. In this case, the input distribution is of the form of (7.5). The secrecy rate with this discrete signaling is given by the mutual information difference between the main channel and the eavesdropper's channel, i.e.

$$\begin{aligned}
\mathcal{R}^{AWGN} &= I(X;Y) - I(X;Z) && (7.7)\\
&= H(Y) - H(Y|X) - H(Z) + H(Z|X) && (7.8)\\
&= -\int_{-\infty}^{\infty} f_Y(\mathbf{y}) \log_2(f_Y(\mathbf{y}))\, d\mathbf{y} + \int_{-\infty}^{\infty} f_Z(\mathbf{z}) \log_2(f_Z(\mathbf{z}))\, d\mathbf{z} && (7.9)
\end{aligned}$$

where $f_Y(\mathbf{y})$ and $f_Z(\mathbf{z})$ are the probability distribution function of the output Y and Z respectively.

Let $\mathcal{N}(\mathbf{t}, \mu)$ be the unit Gaussian distribution

$$\mathcal{N}(\mathbf{t}, \mu) = \frac{1}{(2\pi)^{N/2}} \exp\left(-\frac{||\mathbf{t} - \mu||^2}{2}\right), \tag{7.10}$$

where N is the dimensionality of the input, which is 1 for BPSK, and 2 for M-QAM and M-PSK with $M > 2$. For the AWGN model (7.1), $f_Y(\mathbf{y})$ and $f_Z(\mathbf{z})$ are given by

$$f_Y(\mathbf{y}) = \sum_{i=1}^{M} p_i \mathcal{N}(\mathbf{y}, \sqrt{b}\mathbf{x}_i), \quad f_Z(\mathbf{z}) = \sum_{i=1}^{M} p_i \mathcal{N}(\mathbf{z}, \mathbf{x}_i). \tag{7.11}$$

As an example, for BPSK signaling with input power P, the input is one dimensional with probability distribution function

$$f_X(x) = \frac{1}{2}\delta(x - \sqrt{P}) + \frac{1}{2}\delta(x + \sqrt{P}). \tag{7.12}$$

Hence, the output probability distributions are

$$\begin{aligned}
f_Y(y) &= \frac{1}{2}\mathcal{N}(y, \sqrt{bP}) + \frac{1}{2}\mathcal{N}(y, -\sqrt{bP}), && (7.13)\\
f_Z(z) &= \frac{1}{2}\mathcal{N}(z, \sqrt{P}) + \frac{1}{2}\mathcal{N}(z, -\sqrt{P}). && (7.14)
\end{aligned}$$

Define $\gamma_b = bP$ and $\gamma_e = P$, which correspond to the SNR for Bob and Eve, respectively. Also define

$$\psi^+(y, \gamma) = \mathcal{N}(y, \sqrt{\gamma}),$$

$$\psi^-(y,\gamma) = \mathcal{N}(y, -\sqrt{\gamma}).$$

Then we can rewrite the output probability distributions as

$$f_Y(y) = \frac{1}{2}\psi^+(y,\gamma_b) + \frac{1}{2}\psi^-(y,\gamma_b), \tag{7.15}$$

$$f_Z(z) = \frac{1}{2}\psi^+(z,\gamma_e) + \frac{1}{2}\psi^+(z,\gamma_e). \tag{7.16}$$

Note that

$$\psi^-(y,\gamma) = \psi^+(y,\gamma)\exp\left(-2y\sqrt{\gamma}\right) = \psi^+(-y,\gamma). \tag{7.17}$$

Using the expression in (7.15), we can write

$$\begin{aligned}
&-\int f_Y(y)\log_2(f_Y(y))\ dy \\
&\quad= -\int_{-\infty}^{\infty} \frac{\psi^+(y,\gamma_b)+\psi^-(y,\gamma_b)}{2}\log_2\frac{\psi^+(y,\gamma_b)+\psi^-(y,\gamma_b)}{2}\ dy && (7.18)\\
&\quad= -\frac{1}{2}\int_{-\infty}^{\infty}\psi^+(y,\gamma_b)\log_2\left(\psi^+(y,\gamma_b)+\psi^-(y,\gamma_b)\right)\ dy \\
&\qquad -\frac{1}{2}\int_{-\infty}^{\infty}\psi^-(y,\gamma_b)\log_2\left(\psi^+(y,\gamma_b)+\psi^-(y,\gamma_b)\right)\ dy + 1, && (7.19)
\end{aligned}$$

Note that

$$\begin{aligned}
&\int_{-\infty}^{\infty}\psi^+(y,\gamma_b)\log_2\left(\psi^+(y,\gamma_b)+\psi^-(y,\gamma_b)\right)\ dy && (7.20)\\
&\quad= \int_{-\infty}^{\infty}\psi^+(y,\gamma_b)\log_2\psi^+(y,\gamma_b)\left(1+\exp\left(-2y\sqrt{\gamma_b}\right)\right)\ dy && (7.21)\\
&\quad= -\frac{1}{2}\log_2(2\pi e) + \int_{-\infty}^{\infty}\psi^+(y,\gamma_b)\log_2\left(1+\exp\left(-2y\sqrt{\gamma_b}\right)\right)\ dy, && (7.22)
\end{aligned}$$

and

$$\begin{aligned}
&\int_{-\infty}^{\infty}\psi^-(y,\gamma_b)\log_2\left(\psi^+(y,\gamma_b)+\psi^-(y,\gamma_b)\right)\ dy && (7.23)\\
&\quad= \int_{-\infty}^{\infty}\psi^+(-y,\gamma_b)\log_2\left(\psi^-(-y,\gamma_b)+\psi^+(-y,\gamma_b)\right)\ dy && (7.24)\\
&\quad= \int_{-\infty}^{\infty}\psi^+(y,\gamma_b)\log_2\left(\psi^-(y,\gamma_b)+\psi^+(y,\gamma_b)\right)\ dy. && (7.25)
\end{aligned}$$

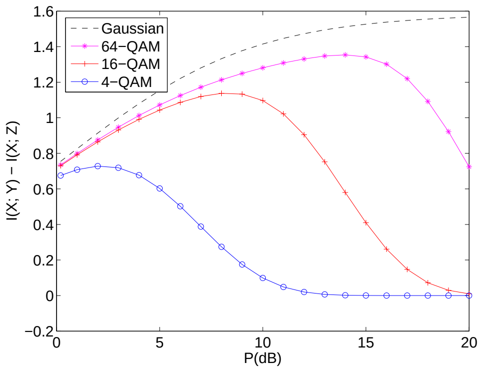


Figure 7.2: Secrecy rate of AWGN channel with Gaussian signaling and M-QAM discrete signaling. $b = 3$.

Thus,

$$-\int f_Y(y)\log_2(f_Y(y))\,dy = 1 + \frac{1}{2}\log_2(2\pi e) - \int_{-\infty}^{\infty}\psi^+(y,\gamma_b)\log_2\left(1+\exp\left(-2y\sqrt{\gamma_b}\right)\right)\,dy. \tag{7.26}$$

Similarly,

$$-\int f_Z(z)\log_2(f_Z(z))\,dz = 1 + \frac{1}{2}\log_2(2\pi e) - \int_{-\infty}^{\infty}\psi^+(z,\gamma_e)\log_2\left(1+\exp\left(-2z\sqrt{\gamma_e}\right)\right)\,dz. \tag{7.27}$$

Substituting (7.26) and (7.27) into (7.9), we can get that the secrecy rate for BPSK signaling with power P is given by

$$\mathcal{R}^A_{BPSK}(P) = \phi(\gamma_b) - \phi(\gamma_e), \tag{7.28}$$

where the superscript A indicates AWGN channel, and the function $\phi(\gamma)$ is defined as

$$\phi(\gamma) = -\int_{-\infty}^{\infty}\mathcal{N}(t,\sqrt{\gamma})\log_2(1+\exp(-2t\sqrt{\gamma}))dt. \tag{7.29}$$

The secrecy rate for 4-QAM is equivalent to two BPSK channels with the same channel gain, but each channel has a power budget $P/2$ in order to satisfy the total power constraint. Mathematically, that is

$$\mathcal{R}^A_{4QAM}(P) = 2\mathcal{R}^A_{BPSK}(\frac{P}{2}). \tag{7.30}$$

The simplification of (7.9) becomes more complicated as the size of the constellation increases, and we always end up with some complex integrals that cannot be evaluated analytically, even for the above BPSK example. Hence, we resort to numerical methods to evaluate the secrecy rate, hoping to gain some insights on the behavior of the secrecy rate with discrete input constellations. Figure 7.2 shows how the secrecy rates evaluated numerically vary with the power used and the size of QAM constellation. Here are the key observations:

1. Secrecy rates with discrete inputs are smaller than the rates with Gaussian signaling. The achievable secrecy rates increase with the size of the input constellation size. This is expected as Gaussian signaling has been shown to be optimal, i.e., it is secrecy-capacity-achieving. A larger input constellation reduces the difference between the achievable secret rate and the optimal Gaussian distribution's secret communication rate.

2. With discrete inputs, there always exists an optimal power P^* corresponding to the maximal secrecy rate. Using more power than P^* will only decrease the secrecy rate. This is very different from the Gaussian input case, where larger power is always better. Intuitively, this means you need to use just enough power so that Bob can decode correctly. Any additional power beyond necessary will only benefit Eve, and in turn reduce the secrecy.

In general, we can denote the mutual information of the AWGN channel for a given size-M uniform discrete constellation as $\mathcal{I}(\gamma)$, which is a function of SNR γ. With transmission power P, the main channel has SNR $\gamma_b = bP$, and the eavesdropper's channel has SNR

$\gamma_e = P$. Thus, the achievable secrecy rate can be written as

$$\mathcal{R}^A(P) = \mathcal{I}(bP) - \mathcal{I}(P). \tag{7.31}$$

It is clear that

$$\lim_{P \to 0} \mathcal{R}^A(P) = 0, \tag{7.32}$$

$$\lim_{P \to \infty} \mathcal{R}^A(P) = \log_2 M - \log_2 M = 0. \tag{7.33}$$

Since $b > 1$ and $\mathcal{I}(\gamma)$ is a monotonically increasing function of γ for the AWGN channel, $\mathcal{R}^A(P)$ is always non-negative. Therefore, there must exist a positive power $P^* < \infty$ that maximizes the secrecy rate $\mathcal{R}^A(P)$. Also, P^* satisfies

$$\frac{d}{dP}\mathcal{R}^A(P^*) = 0. \tag{7.34}$$

In other words,

$$b\mathcal{I}'(bP^*) = \mathcal{I}'(P^*). \tag{7.35}$$

As proved in [24], the derivative of the mutual information for AWGN channel corresponds to the minimum mean square error (MMSE) of the MMSE estimate of the input given the output, and is monotonically decreasing with the SNR. Mathematically, this means for a $X \to Y$ AWGN channel with SNR γ,

$$\frac{dI(\gamma)}{d\gamma} = \frac{1}{2}E\left[(X - E[X|Y,\gamma])^2\right].$$

Hence, at the optimal P^*, the MMSE of the eavesdropper's channel is b times of the MMSE of the main channel.

The optimal P^* is a function of both the constellation size and the main channel's normalized channel gain b. Variation of P^* with b for several QAM constellation sizes M is plotted in dashed lines in Figure 7.3(a). Note that P^* is also the SNR for Eve at the optimal

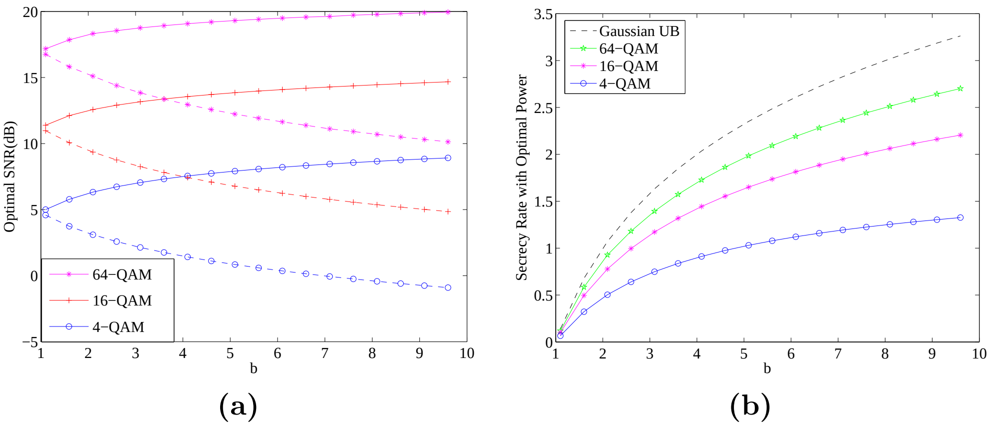


Figure 7.3: (a) The channel SNR with the optimal power for AWGN with M-QAM signaling. The solid curves are the main channel optimal SNR and the dashed curves are the eavesdropper's channel SNR. (b) The secrecy rate corresponding to the optimal power for the AWGN channel with M-QAM signaling.

power. For the same M, P^* decreases with b. Intuitively, the optimal P^* should be just enough to ensure the main channel's reliability. We also plot the main channel SNR bP^* using solid lines in Figure 7.3(a). Although the main channel SNR is not flat across different b, its variation is small. The optimal power also increases with the constellation size, as larger power is necessary to decode a higher input constellation reliably. Figure 7.3(b) shows the rate achieved with the optimal P^*. As expected, the maximal achievable secrecy rate increases with the constellation size. However, the benefit of a larger constellation diminishes gradually since the secrecy capacity is always upper bounded by $\log_2(b)$, plotted using a dashed line in Figure 7.3(b), regardless of the power used.

7.3 Secrecy rate in fading scenarios

For the fading model (7.2), if we consider the random channel observation G_i at Eve as an output, Eve's channel is equivalent to a channel with output (G, Z) and the channel transition probability is $\Pr(GZ|X) = \Pr(G)\Pr(Z|XG)$. Following Csiszár and Körner's arguments [15], the secrecy capacity of the channel model (7.2) is

$$
\begin{aligned}
\mathcal{C}_s &= \max_{V \to X \to YGZ} I(V;Y) - I(V;GZ) && (7.36)\\
&= \max_{V \to X \to YGZ} I(V;Y) - I(V;G) - I(V;Z|G) && (7.37)\\
&= \max_{V \to X \to YGZ} I(V;Y) - I(V;Z|G), && (7.38)
\end{aligned}
$$

where (7.38) follows from the independence of V and G since Alice does not know G and cannot choose V according to G. V is an auxiliary random variable that satisfies the Markov condition $V \to X \to YGZ$. It has been shown in [15, 17] that when the more capable condition $I(X;Y) \geq I(X;ZG)$ for any input X is satisfied, V is not necessary, or in other words, the optimal V equals X. However, our channel does not satisfy the more capable condition, and it appears to be hard to obtain the optimal V and the mapping $P(X|V)$. In Chapter 4, we discussed an achievable secrecy rate that is possible with Gaussian inputs, including artificial noise and bursting strategy. In this work, we will evaluate the achievable secrecy rates when the input are discrete and when $V = X$.

The achievable secrecy rate with $V = X$ is given by

$$
\begin{aligned}
\mathcal{R}_x^F &= I(X;Y) - I(X;Z|G) && (7.39)\\
&= H(Y) - H(Z|G) && (7.40)\\
&= -\int_{-\infty}^{\infty} f_Y(\mathbf{y}) \log_2(f_Y(\mathbf{y}))\, d\mathbf{y}\\
&\quad + \int_0^{\infty} \int_{-\infty}^{\infty} f_{Z|G}(\mathbf{z}) \log_2(f_{Z|G}(\mathbf{z}))\, d\mathbf{z}\, e^{-g} dg. && (7.41)
\end{aligned}
$$

For a discrete input with probability distribution given by (7.5), the distribution of Y is the same as that in (7.11), but the distribution of Z depends on the random realization of Eve's channel gain. The conditional distribution of Z conditioned on the eavesdropper's

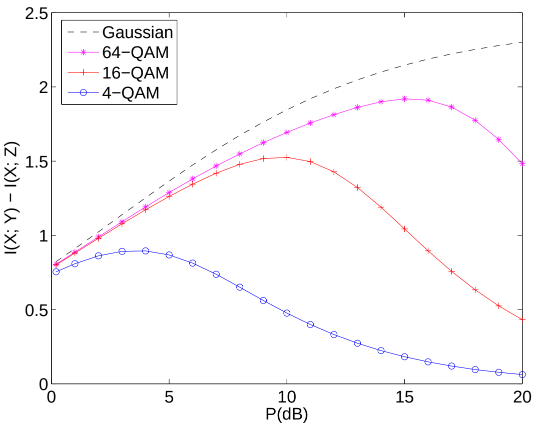


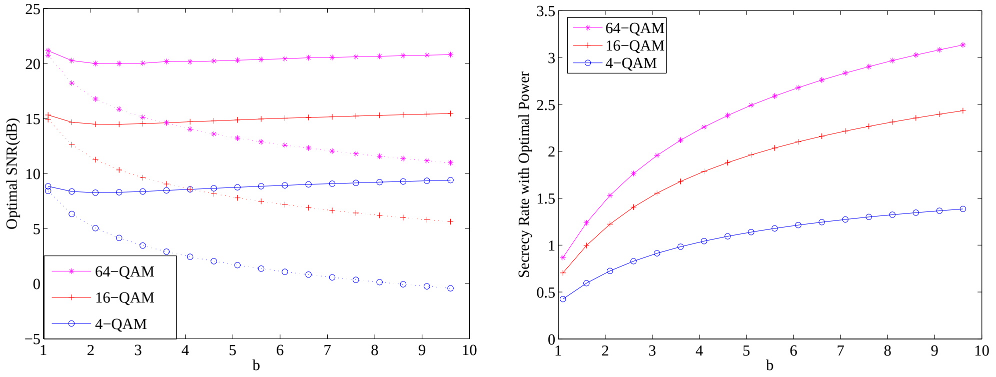
Figure 7.4: The secrecy rate of the fading channel (7.2) with Gaussian signaling and discrete signaling. $b = 3$.

channel realization G is given by

$$f_{Z|G}(\mathbf{z}) = \sum_{i=1}^{M} p_i \mathcal{N}(\mathbf{z}, \sqrt{g}\mathbf{x}_i). \tag{7.42}$$

Again, the analytical expression of the achievable rate is hard to obtain, and we resort to numerical evaluation to gain insight on how the system behaves with discrete input. Numerically evaluating (7.41) with Gaussian input distribution and also M-QAM for $b = 3$, we get Figure 7.4. Note that the secrecy rate of the fading channel is higher than that of the AWGN channel, under the same configuration and average SNR, because fading effectively degrades the eavesdropper's channel. The shapes of the curves look similar to that of the AWGN case as shown in Figure 7.2. Again, for discrete inputs, there exists an optimal power P^* that maximizes the secrecy rate. Using a power greater than the P^* will hurt the secrecy. The underlying reasoning is exactly the same as that for the AWGN channel model. For this example, Gaussian input performs better than M-QAM.

We plot the optimal channel SNR as a function of the main channel's normalized channel gain b at several constellation sizes in Figure 7.5(a). The solid lines are the main channel SNR and the dashed line are the eavesdropper's channel SNR. The optimal power decreases

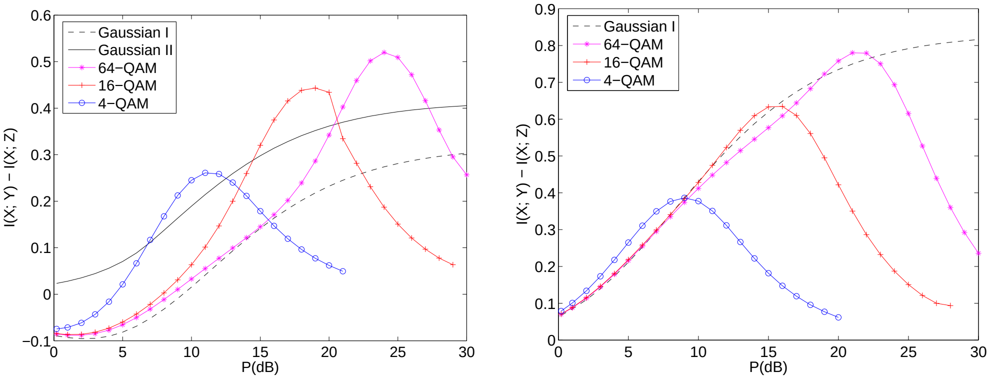


(a) **(b)**

Figure 7.5: (a) The channel SNR with the optimal power for fading channel model (7.2) with M-QAM signaling. The solid curve are the main channel optimal SNR and the dashed curves are the eavesdropper's channel average SNR. (b) The secrecy rate corresponding to the optimal power.

with b to lower the eavesdropper's SNR, while maintaining the main channel SNR to an almost stable level. As the size of the constellation increases, the optimal power also increases. The secrecy rates corresponding to the optimal power are shown in Figure 7.5(b).

Gaussian input, however, is not always optimal for the fading scenario. When we evaluate the secrecy rate for $b = 0.7$ and $b = 1$ with both Gaussian inputs and discrete inputs, we get a different result, as shown in Figure 7.6. Gaussian I corresponds to the strategy of using a simple Gaussian input with power P, while Gaussian II corresponds to the strategy of using a Gaussian input combined with artificial noise and bursting, as proposed in Chapter 4. When $b < 1$, the latter strategy can improve the achievable secrecy rate. For this setting, discrete signaling does better than Gaussian signaling. Moreover, a larger constellation is not always better than a smaller constellation. With a small power, smaller constellations work better. As the power used increases, larger constellations start to perform better. So the optimal constellation depends on the power constraint. The figure also implies that by time sharing among the constellations, the upper envelop of the curves for discrete inputs



(a) **(b)**

Figure 7.6: Secrecy rate of fading channel (7.2) with Gaussian signaling and M-QAM signaling. (a) $b = 0.7$ (b) $b = 1$.

can be achieved.

The reason that discrete signaling can work better than Gaussian signaling when the main channel is on average worse than the eavesdropper's channel is because discrete inputs effectively limit the information that can be obtained by the eavesdropper when his channel realizations are better than the main channel. During those instances when the eavesdropper's channel is better than the main channel, the eavesdropper can gain more information than the legitimate receiver. Gaussian inputs would maximize this information leakage. Because the main channel is worse than the eavesdropper's channel on average, the excess information leakage due to Gaussian input cannot be compensated for by the information gain at the time instances when the main channel is better. On the other hand, with discrete input, the information leakage when the eavesdropper's channel is better is limited by the input entropy, which is $\log_2 M$, no matter how good the eavesdropper's channel is. Therefore, discrete input provides some advantage in terms of secret communication when the eavesdropper's channel is better on average, and this advantage is more significant as the main channel channel gain gets worse. The gain diminishes as the main channel becomes comparable or even better than the eavesdropper's average channel gain.

7.4 Discussion

In this work, we evaluated the secrecy rate for communication involving discrete signaling for both the AWGN channel and Rayleigh fast fading channel. Because practical signaling always adopts discrete inputs with regular constellations in signal space, investigating a communication system's performance under discrete inputs is important. The results show that for discrete signaling there always exists an optimal power for maximal secrecy rate. Extra power will only benefit the eavesdropper and hurt secrecy. For AWGN channels, larger constellations are always better, while for fading channels, the optimal constellation size varies with the power constraint and can perform better than random Gaussian coding. The result also reflects the difficulty of finding the optimal inputs for the fast fading channel. In this work, we only evaluated the performance with QAM because of its popularity in practical system, but theoretically arbitrary discrete input $\{p_i, \mathbf{x}_i\}$ can be used, and it is very hard to obtain the optimal input distributions which might vary with the channel parameters and the power constraint.

The observation that discrete input can perform better than Gaussian input for the fading scenario is very interesting, as it reminds us that, for communication capacity without a secrecy requirement, discrete input distributions have been shown to be capacity achieving when the channel state information is available to neither the transmitter nor the receiver [29]. The proof relies on the concavity of the mutual information function. Computing the optimal input distribution achieving this capacity, often referred as non-coherent capacity, is a difficult task. Nevertheless, numerical computation of the capacity and the optimal input distribution has been made possible using the Kuhn-Tucker condition which is a necessary and sufficient condition for optimality, for a SISO channel [29] and for a MIMO channel [65]. However, the secrecy capacity is often not concave. As a result, the approach applicable to the conventional capacity might not be directly applied to secrecy capacity.

Chapter 8

Future work

8.1 Thesis summary

This thesis examines the challenges of information-theoretic secret communication that utilizes the temporal variations and spatial diversity advantages of the wireless medium to improve secret communication rates. We examined the secrecy capacity of a system consisting of independent parallel channels with one transmitter, one intended receiver and one eavesdropper. We showed that the secrecy capacity of the system is simply the summation of the secrecy capacities of the individual channels. We further derived the optimal power allocation strategy for a system with parallel AWGN channels subject to a total power constraint, which shows that the power should be allocated according to the difference of the channel gain between the main channel and the eavesdropper's channel. The results were also extended to random fading channels with additive Gaussian noise. Secrecy capacity was evaluated numerically for OFDM channels and Rayleigh fading channels. It was shown that the diversity, either in frequency or in time, improves the rate of secret communication and allows secret communication even when the eavesdropper's channel is on average better than the legitimate party's channels.

We then studied the achievable secrecy rate with Gaussian random codes for the situation where the channel of the intended receiver is a constant AWGN channel, while the eavesdropper's channel is fast Rayleigh fading with unknown realizations but known statistics to the transmitter. When Bob's channel is on average worse than Eve's channel, A simple Gaussian input distribution with average power P cannot always guarantee positive secrecy capacity. We proposed a scheme with artificial noise and bursting, which will allow positive secrecy rate even when Bob's channel is on average worse than Eve's channel. This secrecy rate is achieved without knowing when Eve's channel is bad or the changing rate of the eavesdropper's channel.

We also examined the achievable secrecy rate for a multiple antenna system, and the optimal input structure needed to achieve this rate. For the general multiple input multiple output (MIMO) case, the problem is not convex and is hard to solve. However, for the multiple input single output (MISO) case, the problem can be reformulated and solved. An analytical solution was derived for this simple case and the implication of the results were discussed. Multiple antenna systems provide extra degrees of freedom to the transmitter so that a beamforming-like approach can be used to provide advantage to the intended receiver against the eavesdropper.

Next we derived an outer bound of secrecy capacity region for a class of one-sided interference channels. The outer bound is shown to be tight for a class of binary deterministic one-sided interference channels, and can be achieved within one bit for some Gaussian one-sided interference channels. Finally, since the Gaussian random codes are not practical for a real system, we evaluated the effect of discrete signaling on achievable secrecy rate. We observed that with discrete signaling, there always exists an optimal power that maximizes the achievable secrecy rate. Extra power will only benefit the eavesdropper and hurt the secrecy. For the AWGN channel, larger constellation is always better. While for fading channel, the optimal constellation size varies with the power constraint, and discrete signaling can perform better than random Gaussian coding.

8.2 Future work

Although information theoretic secret communication for wireless channels was first studied by Wyner in 1975, the research on this topic had been sparse for decades since then. Recently, this old topic has attracted more attentions from the information theory society, due to the opportunities provided by the diversity of wireless channels. This thesis presented some opportunistic ways to utilize the temporal and spatial variations of wireless channels for secret communication. As always the case, there are many more interesting problems in this field that deserve further exploration. We will conclude this thesis by discussing some possible directions for future research.

In this thesis, we have always assumed that the transmitter knows the channel state information associated with the intended receiver. The channel state information can be obtained by either a feed-back channel from the receiver, or by utilizing the reciprocity and the duplex properties of the link, i.e. by the intended receiver transmitting a training sequence so that the transmitter can estimate the channel. However, sometimes getting the channel state information at the transmitter is so difficult or inconvenient that it is desirable to work without the channel state information at the transmitter. The secrecy capacity for this scenario, as well as any viable secret communication scheme under this scenario would be very interesting to study.

Multiple antennas have been shown to be beneficial to both the conventional capacity and the secrecy capacity. Optimal space-time codings on multiple antenna systems for conventional capacity have been extensively studied since the pioneering work in [86]. When it comes to secrecy capacity, the same set of questions arise: what are the tradeoffs among the secrecy, rate and the diversity? The problem becomes even more interesting when we extend the Alice-Bob-Eve model to multiple access channels and broadcast channels, due to the extra degree of the freedom provided by the multiple antennas and the interference nature of wireless channels. For example, consider a scenario where there are one receiver with two antennas, two transmitters with two antennas, and one eavesdropper with two antennas. Due to the extra degree of freedom, the transmitter might choose to transmit some artificial noise to reduce the information leakage to the eavesdropper. Then how should the users position their signal and noise to maximize the confusion at Eve and the sum rate at the receiver? How does the rate scale with the number of each party's antenna?

Another direction that is worth exploring is the secrecy capacity in a network scenario with multiple transmitter-receiver pairs. Recently, tight outer bounds for the capacity without the secrecy requirement of the two-user Gaussian interference channel were derived in [6, 18]. A similar approach might be useful to study the secrecy capacity of the two-user Gaussian interference channel. Extending the results to multiple users could be even more exciting, because the mixture of the interference from the multiple users might provide a natural means to protect each individual message against a non-intended receiver or the out-of-network eavesdropper. The interference alignment approach proposed in [12] could be an excellent option because the interference from multiple transmitter are aligned perfectly. Due to the careful alignment, the intended receiver can extract the signal sent to her cleanly, while the non-intended receiver would only get a mixture consisting of signals from all transmitters, and would not have enough SNR to extract any particular message from the mixture. Examining more forms of cooperation and their performance in secret communication is a challenging and promising direction to explore.

The research on information theoretic secret communication has been mainly focused on the information theoretic limit of the secrecy rate over various wireless channels. However, to implement the idea in a real system, we need to study the practical coding schemes and analyze their performance. LDPC codes and turbo codes are the most promising candidates since they achieve communication rates close to the conventional capacity without secrecy requirement. Studying how these codes can be modified for secret communication, and evaluating their performance and sensitivity to coding parameters is another valuable direction for future research.

References

[1] http://mathworld.wolfram.com/en-function.html.

[2] http://mathworld.wolfram.com/euler-mascheroniconstant.html.

[3] ITU-T rec X.509 the directory-authentication framework. International Telecommunication Union, 1993.

[4] Lecture notes on cryptography. MIT Summer Course, available at http://www.cs.ucsd.edu/users/mihir/papers/gb.html, 2001.

[5] R. Ahlswede and I. Csiszar. Common randomness in information theory and cryptography, part 1: secret sharing. *IEEE Trans. Inform. Theory*, 39:1121–1132, 1993.

[6] V.S. Annapureddy and V.V. Veeravalli. Gaussian interference networks: Sum capacity in the low interference regime and new outer bounds on the capacity region. *submitted to IEEE Trans. on Info. Theory*, 2008.

[7] A.S. Avestimehr, S. Diggavi, and D. Tse. A deterministic approach to wireless relay networks. *Proceedings of Allerton Conference*, 2007.

[8] J. Barros and M.R.D. Rodrigues. Secrecy capacity of wireless channels. In *IEEE Int. Symp. Inf. Theory*, pages 356–360, July 2006.

[9] C. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Trans. on Info. Theory*, 41:1915–1923, 1995.

[10] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. Quantum cryptography, or unforgeable subway tokens. *Advances in Cryptology: Crypto '82*, page 267 275, 1982.

[11] S. Boyd and L. Vandenberghe. *Convex Optimization.* Cambridge University Press, 2004.

[12] V.R. Cadambe and S.A. Jafar. Interference alignment and degrees of freedom of the k-user interference channel. *IEEE Trans. on Info. Theory*, 54, 2008.

[13] G. Caire and S. Shamai. On the capacity of some channels with channel state information. *IEEE Transactions on Information Theory*, 45(6):2007–2019, Sep. 1999.

[14] Y. Chen and A.J.H. Vinck. Wiretap channel with side info. In *IEEE Int. Symp. Inf. Theory*, pages 2607 – 2611, July 2006.

[15] I. Csiszár and J. Körner. Broadcast channels with confidental messages. *IEEE Trans. on Info. Theory*, 24(3):339–348, May 1978.

[16] I. Csiszar and P. Narayan. Common randomness and secret key generation with a helper. *IEEE Trans. Inform. Theory*, 46:344–366, 2000.

[17] M. Van Dijk. On a special class of broadcast channels with confidential messages. *IEEE Trans. on Info. Theory*, 43(2):712 – 714, March 1997.

[18] R. Etkin, D. Tse, and H. Wang. Gaussian interference channel capacity to within one bit. *submitted to IEEE Trans. on Info. Theory*, 2007.

[19] G.J. Foschini and M.J. Gans. On limits of wireless communications in a fading environment when using multiple antennas. *Wireless Personal Communications*, 6:311–335, 1998.

[20] R. Gallager. *Information Theory and Reliable Communication.* New York, Wiley, 1968.

[21] A. El Gamal and M. Costa. The capacity region of a class of deterministic interference channels. *IEEE Trans. on Info. Theory*, 28(2):343–346, Mar 1982.

[22] A. J. Goldsmith and P. P. Varaiya. Capacity of fading channels with channel side information. *IEEE Transactions on Information Theory*, 43(6):pp. 1986–1992, Nov. 1997.

[23] P.K. Gopala, L. Lai, and H. El-Gamal. On the secrecy capacity of fading channels. *IEEE Trans. on Info. Theory.* submitted 2006.

[24] D. Guo, S. Shamai, and S. Verdu. Mutual information and minimum mean-square error in gaussian channels. *IEEE Trans. on Infor. Theory*, 51(4), April 2005.

[25] A. Hassan, W. Stark, J. Hershey, and S. Chennakeshu. Cryptographic key agreement for mobile radio. *Digital Signal Processing*, 6:207–212, 1996.

[26] A. O. Hero. Secure space-time communication. *IEEE Trans. on Info. Theory*, 49(12):3235 – 3249, Dec 2003.

[27] J. Hershey, A. Hassan, and R. Yarlagadda. Unconventional cryptographic keying variable management. *IEEE Trans. on Communications*, 43:3–6, 1995.

[28] R. Horst and H. Tuy. *Global Optimization: Deterministic Approaches.* Berlin: Springer-Verlag, 3rd edition, 1996.

[29] M. Trott I. Abou-Faycal and S. Shamai. The capacity of discrete-time memoryles rayleigh-fading channels. *IEEE Trans. on Infor. Theory*, 47(4), May 2001.

[30] A. Khisti, A. Tchamkerten, and G. Wornell. Secure broadcasting. *IEEE Trans. on Info. Theory*, submitted 2007.

[31] A. Khisti and G. Wornell. The mimome channel. In *Forty-Fifth Annual Allerton Conference on Communications, Control and Computing*, 2007.

[32] A. Khisti, G. Wornell, and A. Tchamkerten. Secure broadcasting with multiuser diversity. In *Forty-Fourth Annual Allerton Conference on Communications, Control and Computing*, Sept 2006.

[33] H. Koorapaty, A. Hassan, and S. Chennakeshu. Secure information transmission for mobile radio. *IEEE Commun. Letters*, 4:52–55, 2000.

[34] J. Körner and K. Marton. Comparison of two noisy channels. In I. Csiszár and P. Elias, editors, *Topics In Info. Theory*, pages 411–423. Colloquia Mathematica Societatis Janos Bolyai, Amsterdam, The Netherlands: North Holland, 1977.

[35] L. Lai and H. El-Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. on Info. Theory*, submitted 2006.

[36] L. Lai, H. El-Gamal, and V. Poor. Secrecy capacity of the wiretap channel with noisy feedback. In *Forty-Fifth Annual Allerton Conference on Communications, Control and Computing*, Sept 2007.

[37] L. Lai, H. El-Gamal, and V. Poor. The wiretap channel with feedback: Encryption over the channel. *IEEE Trans. on Info. Theory*, 2008.

[38] S. K. Leung-Yan-Cheong and M. Hellman. The Gaussian wire-tap channel. *IEEE Trans. on Info. Theory*, 24(4):451 – 456, Jul 1978.

[39] X. Li, M. Chen, and E. P. Ratazzi. Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy. In *The 6th IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC'05)*, 2005. The Italian Academy at Columbia University, New York.

[40] X. Li and E. P. Ratazzi. MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks. In *Proc. IEEE Military Communications Conference (MILCOM'2005)*, 2005. Atlantic City, NJ.

[41] Z. Li, W. Trappe, and R.D. Yates. Secret communication via multi-antenna transmission. In *Forty-First Annual Conference on Information Sciences and Systems*, 2007.

[42] Z. Li, R.D. Yates, and W. Trappe. Secrecy capacity of independent parallel channels. In *Forty-Fourth Annual Allerton Conference on Communications, Control and Computing*, Sept 2006.

[43] Z. Li, R.D. Yates, and W. Trappe. Secure communication with a fading eavesdropper channel. In *IEEE Int. Symp. Inf. Theory*, 2007.

[44] Z. Li, R.D. Yates, and W. Trappe. Secrecy capacity region for a class of one-sided interference channels. In *IEEE Int. Symp. Inf. Theory*, 2008.

[45] Y. Liang and V.H. Poor. Generalized multiple access channels with confidential messages. In *IEEE Int. Symp. Inf. Theory*, pages 952 – 956, July 2006.

[46] Y. Liang and V.H. Poor. Secrecy capacity region of binary and gaussian multiple access channels. In *Forty-Fourth Annual Allerton Conference on Communications, Control and Computing*, Sept 2006.

[47] Y. Liang and V.H. Poor. Secure communication over fading channels. In *Forty-Fourth Annual Allerton Conference on Communications, Control and Computing*, Sept 2006.

[48] Y. Liang, V.H. Poor, and S. Shamai(shitz). Secure communication over fading channels. *IEEE Trans. on Info. Theory*, jun 2008.

[49] R. Liu, I. Maric, R.D. Yates, and P. Spasojevic. Discrete memoryless interference and broadcast channels with confidential messages. In *Forty-Fourth Annual Allerton Conference on Communications, Control and Computing*, Sept 2006.

[50] R. Liu, I. Maric, R.D. Yates, and P. Spasojevic. The discrete memoryless multiple access channel with confidential messages. In *IEEE Int. Symp. Inf. Theory*, pages 957 – 961, July 2006.

[51] R. Liu, I. Maric, R.D. Yates, and P. Spasojevic. Memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. on Info. Theory*, November 2007.

[52] R. Liu and H.V. Poor. Multi-antenna gaussian broadcast channels with confidential messages. In *IEEE Int. Symp. Inf. Theory*, July 2008.

[53] T. Liu and S. Shamai. A note on the secrecy capacity of the multi-antenna wiretap channel. 2007.

[54] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: Extracting a cryptographic key from an un-authentiated wireless channel. In *The 14th Annual International Conference on Mobile Computing and Networking, (ACM MobiCom)*, 2008.

[55] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. on Info. Theory*, 39:733–742, 1993.

[56] U. M. Maurer and S. Wolf. Info.-theoretic key agreement: From weak to strong secrecy for free. In *EUROCRYPT*, pages 351–368, 2000.

[57] M. Medard. Capacity of correlated jamming channels. In *Thirty-fifth Annual Allerton Conference on Communications, Control and Computing*, Sept 1997.

[58] M. Medard and R.G. Gallager. Bandwidth scaling for fading multipath channels. *IEEE Trans. Inform. Theory*, 48(6):840–852, April 2002.

[59] A. Menezes, P. vanOorschot, and S. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1997.

[60] C. Mitrpant, A.J.H. Vinck, and Y. Luo. An achievable region for the gaussian wiretap channel with side info. *IEEE Trans. on Info. Theory*, pages 2181 – 2190, May 2006.

[61] R. Negi and S. Goel. Secret communication in presence of colluding eavesdroppers. In *Proc. IEEE Military Communication (MILCOM)*, 2005.

[62] R. Negi and S. Goel. Secret communication using artificial noise. In *Proc. IEEE Vehicular Tech. Conf*, Fall 2005.

[63] F. Oggier and B. Hassibi. The secrecy capacity of the mimo wiretap channel. *IEEE Trans. on Info. Theory*, 2007.

[64] P. Parada and R. Blahut. Secrecy capacity of SIMO and slow fading channels. In *IEEE Int. Symp. Inf. Theory*, pages 2152 – 2155, Sept 2005.

[65] R. R. Perera, K. Nguyen, T.S. Pollock, and T.D. Abhayapala. Capacity of non-coherent rayleigh fading mimo channels. In *Communications, IEE Proceedings-*, Dec 2006.

[66] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the gaussian mimo wire-tap channel: The 2-2-1 channel. *submitted to IEEE Trans. on Info. Theory*, 2007.

[67] S. Shafiee and S. Ulukus. Achievable rates in gaussian miso channels with secrecy constraints. In *IEEE Int. Symp. Inf. Theory*, 2007.

[68] S. Shafiee and S. Ulukus. Mutual information games in multi-user channels with correlated jamming. *IEEE Trans. on Information Theory*, submitted 2005.

[69] C. Shannon. Communication theory of secrecy systems. *Bell Sys. Tech. J.*, 28:657–715, 1949.

[70] J. Spanier and K. Oldham. *The Exponential Integral Ei() and Related Functions. Ch. 37 in An Atlas of Functions.* Washington, DC: Hemisphere, 1987.

[71] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Multiple access channels with generalized feedback and confidential messages. In *Proc. of IEEE Information Theory Workshop on Frontiers in Coding Theory*, Sept 2007.

[72] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Interference-assisted secret communication. In *Proc. of IEEE Information Theory Workshop (ITW)*, May 2008.

[73] E. Tekin and A. Yener. Achievable rates for the general gaussian multiple access wire-tap channel with collective secrecy. In *Forty-Fourth Annual Allerton Conference on Communications, Control and Computing*, Sept 2006.

[74] E. Tekin and A. Yener. The gaussian multiple access wire-tap channel with collective secrecy constraints. In *IEEE Int. Symp. Inf. Theory*, pages 1164 – 1168, July 2006.

[75] E. Tekin and A. Yener. The general gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. *IEEE Trans. on Info. Theory*, November 2007.

[76] E. Telatar. Capacity of multi-antenna Gaussian channels. *European Transactions on Telecommunications*, 10(6):585–595, Nov.-Dec. 1999.

[77] E. Telatar and D. N. C. Tse. Capacity and mutual information of wideband multipath fading channels. *IEEE Trans. on Information Theory*, 46(4):1384–1400, July 2000.

[78] I.E. Telatar. Capacity of multi-antenna gaussian channels. *European Trans. on Telecommunications*, 10(6), Nov/Dec 1999.

[79] W. Trappe and L.C. Washington. *Introduction to Cryptography with Coding Theory.* Prentice Hall, 2002.

[80] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication.* Cambridge University Press, 2005.

[81] S. Verdu. Recent results on the capacity of wideband channels in the low-power regime. *IEEE Wireless Communications*, pages 40–45, August 2002.

[82] S. Verdú. Spectral efficiency in the wideband regime. *IEEE Trans. on Information Theory*, 48(6):1319–1343, June 2002.

[83] D. Wiedemann. Quantum cryptography. *Sigact News*, 18:48–51, 1987.

[84] A. Wyner. The wire-tap channel. *Bell. Syst. Tech. J.*, 54(8):1355–1387, Jan 1975.

[85] R.D. Yates, D. Tse, and Z. Li. Secret communication on interference channels. In *IEEE Int. Symp. Inf. Theory*, 2008.

[86] L. Zheng and D. Tse. Diversity and multiplexing: A fundamental tradeoff in multiple antenna channels. *IEEE Trans. on Inf. Theory*, 2002.

Curriculum Vita

Zang Li

Education

2005 - 2009 Ph.D., Electrical and Computer Engineering, Rutgers University, NJ

2003 - 2005 M.S., Electrical and Computer Engineering, Rutgers University, NJ

1997 - 2000 M.S., Biophysics, Fudan University, Shanghai, China

1993 - 1997 B.S., Physics, Jilin University, Changchun, China

Employment

2008.10 - 2009.4 Software Engineer Intern, Juniper Networks/PrO Unlimited Inc., Sunnyvale, CA

2008.6 - 2008.8 Wireless Communication Intern, Philips Research, Briarcliff Manor, NY

2004.9 - 2005.6 Teaching Assistant, Electrical and Computer Engineering, Rutgers University, New Brunswick, NJ

Publications

Zang Li, Roy Yates, Wade Trappe, "Secrecy Capacity Region of a Class of One-sided Interference Channel", in *IEEE International Symposium on Information Theory*, 2008.

Roy Yates, David Tse, Zang Li, "Secret Communication on Interference Channels", in *IEEE International Symposium on Information Theory*, 2008.

Yu Zhang, Zang Li, Wade Trappe, "Evaluation of Localization Attacks on Power-Modulated Challenge-Response Systems", *IEEE Transactions on Information Forensics and Security*, June 2008.

Yu Zhang, Zang Li, Wade Trappe, "Power-Modulated Challenge-Response Schemes for Verifying Location Claims", in *Proceedings of IEEE Global Communications Conference*, 2007.

Zang Li, Roy Yates, Wade Trappe, “Secure Communication with a Fading Eavesdropper Channel”, in *IEEE International Symposium on Information Theory, 2007.*

Zang Li, Wade Trappe, Roy Yates,“Secret Communication via Multi-antenna Transmission”, in *Forty-First Annual Conference on Information Sciences and Systems*, 2007.

Zang Li, Roy Yates, Wade Trappe, “Secrecy Capacity of Independent Parallel Channels”, in *Forty-Fourth Annual Allerton Conference on Information Sciences and Systems*, 2006.

Zang Li, Wade Trappe, “WBE-Based Anti-collusion Fingerprints: Design and Detection”, IEEE Transactions on Information Forensics and Security (under submission).

Zang Li, Wenyuan Xu, Rob Miller, Wade Trappe,“Securing Wireless Systems via Lower Layer Enforcements”, in *ACM Workshop on Wireless Security*, 2006.

Zang Li, Yanyong Zhang, Wade Trappe, Badri Nath, “Robust Statistical Methods for Securing Wireless Localization in Sensor Networks”, in *International Symposium on Information Processing in Sensor Networks*, 2005.

Zang Li and Wade Trappe, “Collusion-resistant Fingerprints from WBE Sequence Sets”, in *IEEE International Conference on Communications*, 2005.

Zang Li, Yangyong Zhang, Wade Trappe, Badri Nath,“Securing Wireless Localization: Living with Bad Guys”, in *DIMACS Workshop on Wireless Security*, 2004.

Xiangqian Liu, Zang Li, Xiaoli Ma,“An EM algorithm for hop timing estimation in FH networks with frequency collisions”, in *IEEE Proc. Military Communications Conference*, 2004.

Xiangqian Liu, Zang Li, Nicholas D. Sidiropoulos, Ananthram Swami, “Joint signal parameter estimation of wideband frequency hopped transmissions using 2-D antenna arrays”, in *Proc. IEEE Workshop on Signal Processing Advances in Wireless Communications*, 2003.