Wiretap Channel with Side Information

Vom Fachbereich Ingenieurwissenschaften

der Universität Duisburg-Essen

zur Erlangung des akademischen Grades einer

Doktorin der Ingenieurwissenschaften(Dr.-Ing.)

genehmigte Dissertation

von

Yanling Chen

aus Henan, China

Referent: Prof. A. J. Han Vinck

Korreferent: Prof. Yuan Luo

Tag der mündlichen Prüfung: 17. September 2007

Wiretap Channel with Side Information

October 25, 2007, Essen, Germany

Editor: Yanling Chen

With refs.

ISBN: 3-9807929-8-6

Publisher: Institute for Experimental Mathematics, Ellernstr. 29, 45326 Essen, Germany

To the memory of my father Qingxian Chen and to my mother Xiumei Wang.

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my supervisor, Prof. A. J. Han Vinck, for his guidance and helpful suggestions throughout the entire course of this research. He is brilliant, knowledgeable, insightful, and most importantly, always available. I thank him for guiding me to learn the art of research and the philosophy behind it.

Also I am deeply grateful to Prof. Trung van Tran for his constant support and encouragement. A special thank goes to Prof. Yuan Luo for reviewing the previous version of this dissertation and providing valuable comments.

Thanks are also due to all the colleagues in the Institute for Experimental Mathematics, for the vivid discussions we had on various topics. Special thanks should go to Pavol, Anil, Ashot and Marjan for their brainstorming with me when I failed coming up with ideas. I'm also grateful to Balakirsky and Anahit for many simulating discussions and lectures that helped me improve my knowledge in related area. I would further like to thank the secretary, Birgit, for her willingness to help and kindness.

I additionally would like to express my appreciation to the Graduate College of the University Duisburg-Essen and DFG (Deutsche Forschungsgemeinschaft) for their financial contributions.

I wish to thank Prof. Shiyi Shen and my former advisors, Prof. Fangwei Fu and Prof. Lusheng Chen, who are at Nankai University, China, but never failed to give me great encouragement and suggestions.

I owe many thanks to my friends outside of my research, Ziad, Yanke, Huizhi, Viktorija, Heike, Alenka and Jing. Their support and care helped me overcome setbacks and stay focused on my research. I am also indebted to my cat, Timtim, who is always incredibly sweet and brings me a lot of fun.

Last but not least, I would like to express my heartfelt gratitude to my family, especially my mother Xiumei Wang, my sister Ling Chen and my brother Yajun Chen, for always being there when I need them most and for supporting me through all these years.

Contents

Chapter 1

Introduction

1.1 Historical perspective

The concept of the wiretap channel was first introduced by Wyner [1]. The model which he proposed is shown in Figure 1.1. It is a form of degraded broadcast channel [2], but the goal here is quite different. For the degraded broadcast channel, one seeks to maximize the flow of information to both receivers. However, for the wiretap channel, we assume that the wiretapper knows the encoding scheme used at the transmitter and the decoding scheme used at the legitimate receiver. The objective is to maximize the rate of reliable communication from the source to the legitimate receiver, subject to the constraint that the wiretapper learns as little as possible about the source output.

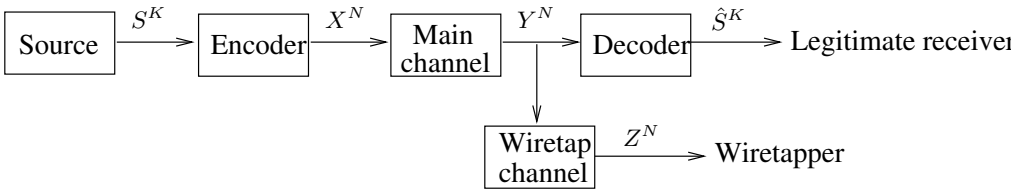


Figure 1.1: Wyner wiretap channel.

In this thesis, we will denote random variables U, V, X, etc. by capital letters and their ranges by corresponding script letters. Let $\mathcal{U}$ be a finite set. Denote its cardinality by $|\mathcal{U}|$. We will denote various joint and conditional probability distributions by $p_{UV}(u,v) = \Pr\{U = u, V = v\}$, $p_{U|V}(u|v) = \Pr\{U = u|V = v\}$, $u \in \mathcal{U}$, $v \in \mathcal{V}$. Consider $\mathcal{U}^N$, the set of N vectors with components in $\mathcal{U}$. The members of $\mathcal{U}^N$ will be written as $u^N = (u_1, u_2, \cdots, u_N)$, where subscripted letters denote the components and superscripted letters denote the vector. A similar convention applies to random vectors and random variables, which are denoted by upper-case letters.

1.1.1 Wyner wiretap channel

Wyner [1] investigated the communication system as shown in Figure 1.1. He considered the situation when both the main channel and the wiretap channel are discrete memoryless channels (DMCs). Let S be the source with finite alphabet $\mathcal{S}$. Denote $S^K = (S_1, \cdots, S_K)$, where $S_i, 1 \leq i \leq K$ are independent, identically distributed (i.i.d.) random variables that take values in the finite set $\mathcal{S}$. The encoder encodes every K source outputs S^K into an

N-vector X^N, which is the input of the main channel. Let Y^N and Z^N be the output of the main channel and overall wiretap channel, respectively. The *rate* of transmission to the legitimate receiver is defined to be

$$R = \frac{KH(S)}{N}. \tag{1.1}$$

The *equivocation* of the source at the output of the wiretap channel is defined to be

$$\Delta = \frac{1}{K} H(S^K|Z^N). \tag{1.2}$$

Upon receipt of Y^N the decoder at the legitimate receiver makes an estimate $\hat{S}^K$ of the source output S^K. The *error-rate* for a given encoder-decoder pair is defined as

$$P_e = \frac{1}{K} \sum_{i=1}^{K} \Pr\{\hat{S}_i \neq S_i\}. \tag{1.3}$$

We say that the pair (R^*, d^*) (where $R^*, d^* > 0$) is *achievable* if, for all $\epsilon > 0$, there exists an encoder-decoder pair such that

$$R \geq R^* - \epsilon, \quad \Delta \geq d^* - \epsilon, \quad P_e \leq \epsilon. \tag{1.4}$$

In particular, if Δ is equal to $H(S)$, then it is considered that the transmission is accomplished in *perfect secrecy*. Wyner showed that in most cases, there exits a *secrecy capacity* C_s such that reliable transmission at rates up to C_s is possible in approximately perfect secrecy. Define the *capacity region* of the wiretap channel as the set of all achievable (R^*, d^*) pairs. Let the capacity of the main channel be C_M. Then the capacity region, when both the main channel and the wiretap channel are DMCs, is characterized as follows:

$$\mathcal{R} \stackrel{\triangle}{=} \{(R, d): \quad 0 \leq R \leq C_M, \quad 0 \leq d \leq H(S), \quad Rd \leq H(S)\Gamma(R)\}, \tag{1.5}$$

where

$$\Gamma(R) = \sup_{p_X(x) \in \mathcal{P}(R)} I(X; Y|Z), \tag{1.6}$$

and $\mathcal{P}(R)$ is the set of $p_X(x)$ such that $I(X;Y) \geq R$.

A particular simple example results when the main channel is noiseless and the wiretap channel is a binary symmetric channel (BSC) with crossover probability p. Wyner showed that

$$R \leq 1, \quad d \leq 1, \quad Rd \leq h(p) \tag{1.7}$$

defines the set of all achievable rate equivocation pairs. As noted by Wyner, this region is not convex.

However, when a source with memory is considered, it is necessary to modify the definitions of rate R and equivocation Δ. In [1, Appendix C], Wyner discussed an example to illustrate such a need. Consider a stationary and ergodic source and suppose that $H(S_1) > H(S)$. Let the main channel be a noiseless binary channel and the wiretap channel be a BSC with zero capacity. A possible encoder-decoder has $K = N = 1$ and takes $X_1 = S_1$. Such a scheme has $P_e = 0$, but $R = H(S)$ and $\Delta = H(S_1) > H(S)$ due to the

definitions given in (1.1) and (1.2). Using (1.4), this would lead us to accept the rate equivocation pair $(H(S), H(S_1))$ as achievable, which would not be reasonable. Accordingly, Wyner [1] modified the definition of the equivocation per source letter to be

$$\Delta = \lim_{v\to\infty} \frac{1}{Kv} H(S^{Kv}|Z^{Nv}).$$

Recall that for a stationary source S,

$$H(S) = \lim_{v\to\infty} \frac{1}{v} H(S^v).$$

Therefore, we have an achievable pair $(\lim_{v\to\infty} \frac{1}{v} H(S^v), \lim_{v\to\infty} \frac{1}{Kv} H(S^{Kv}|Z^{Nv}))$ according to the modified definitions. However, such a rate equivocation pair could not tell explicitly about rate and security of the transmission, though it is clear that the rate to the legitimate receiver is $H(S_1)$ and the transmission is accomplished in perfect secrecy.

In [3], Leung-Yan-Cheong considered the wiretap channel of Wyner's model with an ergodic source with a finite alphabet. Differently from Wyner [1], he defined the *rate* of transmission to the legitimate receiver to be

$$R = \frac{H(S^K)}{N}, \tag{1.8}$$

the fractional *equivocation* of the wiretapper to be

$$\Delta = \frac{H(S^K|Z^N)}{H(S^K)}, \tag{1.9}$$

and the *error rate* at the legitimate receiver to be

$$P_e = \Pr\{S^K \neq \hat{S}^K\}. \tag{1.10}$$

The new definitions have the advantage that they are adaptive also to a source with memory, for instance, a stationary and ergodic source. Furthermore, the equivocation is normalized by the entropy of the source and thus Δ is always bounded by a constant 1, which is not dependent on the source. In particular, $\Delta = 1$ implies that the wiretapper's posterior uncertainty about the source output is equal to his priori uncertainty. Thus the wiretapper is no better informed after he receives his data than he was before. So the transmission is accomplished in *perfect secrecy*. Recall the example [1, Appendix C] discussed above. According to the new definitions, we have an achievable pair $(H(S_1), 1)$, which tells explicitly that the rate to the legitimate receiver is $H(S_1)$ and the transmission is accomplished in perfect secrecy.

The pair (R^*, d^*) is said to be *achievable* if, for all $\epsilon > 0$, there exists an encoder-decoder pair such that

$$R \geq R^* - \epsilon, \quad \Delta \geq d^* - \epsilon, \quad P_e \leq \epsilon. \tag{1.11}$$

Consequently, the *secrecy capacity* C_s is defined to be the maximum R such that $(R, 1)$ is achievable. Based on the new definitions, Leung-Yan-Cheong [3] rewrote Wyner's result on the achievable (R, d) region as the following.

$$\mathcal{R}=\{(R,d): \quad 0 \leq R \leq C_M, \quad 0 \leq d \leq 1, \quad Rd \leq \Gamma(R)\}, \tag{1.12}$$

where $\Gamma(R)$ is the same as defined in (1.6). Furthermore, Leung-Yan-Cheong [3] showed that, if $I(X;Y)$ and $I(X;Z)$ are simultaneously maximized by the same probability distribution $p_X(x)$, then $\Gamma(R)$ is a constant and equals the difference of the capacities of the main channel and overall wiretap channel. It is clear that in this case $\Gamma(R)$ is also the secrecy capacity. As proved by Leung-Yan-Cheong [3], such situation happens when both main channel and overall wiretap channel are symmetric discrete memoryless channels.

1.1.2 Broadcast channel

The broadcast channel was first introduced by Cover [23]. A model is given in Figure. 1.2 for the two-receiver broadcast channel. Here the problem is how to send different pieces of information simultaneously from a single source to different receivers. This problem is still open in the sense that for the general case, there is no single-letter characterization of the set of achievable rates to different receivers known yet.

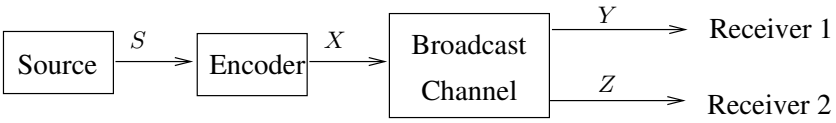


Figure 1.2: Broadcast channel.

In [31], Körner and Marton introduced two ways of partially ordering DMCs with the same input alphabet. They defined a DMC $X \to Y$ to be *more capable* than a DMC $X \to Z$, if $I(X;Y) \geq I(X;Z)$ for every probability distribution on X. They defined a DMC $X \to Y$ to be *less noisy* than a DMC $X \to Z$, if $I(U;Y) \geq I(U;Z)$ for every DMC $U \to X$ with finite input alphabet and for every probability distribution on U. In [2], Bergmans defined the DMC $X \to Z$ to be a *degraded version* of the DMC $X \to Y$, if there exists a DMC $Y \to Z$ such that $X \to Z$ can be represented as the cascade of the channels $X \to Y$ and $Y \to Z$. It is shown in [31] that being more capable is a strictly weaker condition than being less noisy in the sense that the latter implies the former and that being more noisy is a strictly weaker condition than being a degraded version.

Classical approaches which can be applied to the broadcast channel are time sharing and maxmin. Cover [23] introduced a superposition random coding scheme and showed that one can generally transmit at higher rates. He designed the coding schemes for the binary symmetric broadcast channel and the Gaussian broadcast channel. The optimality of his scheme for the binary symmetric broadcast channel was shown by Wyner [26], and for the Gaussian broadcast channel by Bergmans [27]. The binary symmetric broadcast channel and the Gaussian broadcast channel are special cases of the degraded broadcast channel. Bergmans [2] reformulated Cover's superposition scheme for the case of the degraded broadcast channel and proved a rigorous random coding scheme for it. Later his rate region was shown to be optimal by Ahlswede and Körner [12]. Thus the theory on the degraded broadcast channel is fairly complete. For the general non-degraded broadcast channel, an achievable region was put forth independently by Cover [25] and van der Meulen [28]. For more results on broadcast channels, please refer to [29] and [30] and the references therein.

1.1.3 Broadcast channel with confidential messages

Csiszár and Körner [5] investigated the broadcast channel with confidential messages. The model is shown in Figure 1.3. It is a broadcast channel but with the additional feature that the message sent to the legitimate receiver is confidential and the wiretapper should be kept as ignorant of it as possible. Following Wyner [8], they measured confidentiality by equivocation per source letter. They showed that when both the main channel and the wiretap channel are DMCs, the secrecy capacity of this communication system can be expressed as

$$C_s = \max_{U \to X \to (Y,Z)} [I(U;Y) - I(U;Z)], \tag{1.13}$$

where the maximum is over all possible random variables U in joint distribution with X, Y and Z such that $U \to X \to (Y, Z)$ is a Markov chain [1]. An example is shown in Figure 1.4 (a).

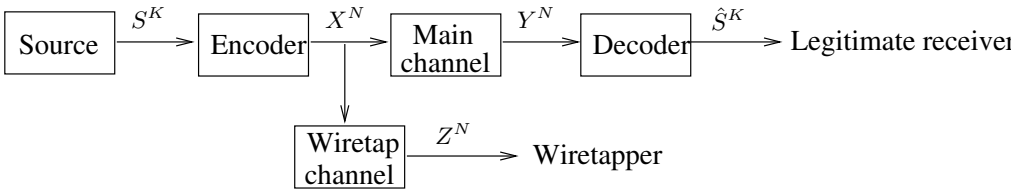


Figure 1.3: Csiszár-Körner wiretap channel.

It is clear that, the wiretap channel model of Wyner is a special case of the wiretap channel model of Csiszár and Körner, in a manner that the overall wiretap channel is a degraded version of the main channel. Such an example is given in Figure 1.4 (d). So up to now, the problem of single-letter characterization the secrecy capacity for the discrete memoryless wiretap channels of these two models has been solved.

In [6], van Dijk considered a special class of broadcast channels with confidential messages where the main channel is less noisy than the wiretap channel. Following the definitions of the rate, equivocation and error rate by Leung-Yan-Cheong [3] as given in (1.8), (1.9) and (1.10), he rewrote the capacity region of the broadcast channel with confidential messages, where the main channel is less noisy than the wiretap channel, given by Csiszár and Körner as followings.

$$\mathcal{R}=\{(R,d) : R \geq 0, 0 \leq d \leq 1, \exists\, P_X \text{ s.t. } R \leq I(X;Y) \text{ and } Rd \leq I(X;Y) - I(X;Z)\}. \tag{1.14}$$

In particular, if the main channel is more capable (including less noisy situation) than the wiretap channel, then the secrecy capacity satisfies

$$C_s = \max_{p_X(x)} [I(X;Y) - I(X;Z)], \tag{1.15}$$

where the maximum is over all possible distributions of X. Such an example is given in Figure 1.4 (b).

Note that at present the calculation of secrecy capacity is still an unsolved problem when the main channel and wiretap channel are general DMCs. However, it can be simplified

[1] Random variables U, X, Y are said to form *a Markov chain* in such a order $U \to X \to Y$ if the conditional distribution of Y depends only on X and is conditionally independent of U.

for some special cases. For instance, if the main channel is less noisy than the wire tap channel, the expression of the secrecy capacity is given in (1.15). Moreover, as shown by van Dijk [6], the main channel being less noisy than the wire tap channel is equivalent to the condition that $I(X;Y)-I(X;Z)$ is a concave function of the input probability distribution $p_X(x)$. Hence, the secrecy capacity can be calculated using convex optimization methods. In [32], Yasui et al. proposed an Arimoto-Blahut type algorithm for computing the secrecy capacity for this situation. In addition, van Dijk [6] showed that, if $I(X;Y)$ and $I(X;Z)$ are individually maximized by the same probability distribution $p_X(x)$, and the main channel is less noisy than the wiretap channel, the secrecy capacity is

$$C_s = C_M - C_{MW}, \tag{1.16}$$

where C_M and C_{MW} are capacities of the main channel and the wiretap channel, respectively. Such an example is shown in Figure 1.4 (c).

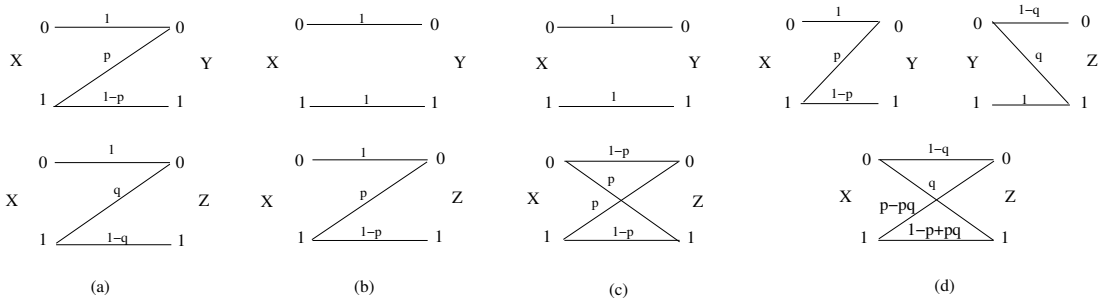


Figure 1.4: (a), (b), (c) are channels of Csiszár-Körner's model, (d) is of Wyner's model. (a) $C_s = \max_{U\to X\to(Y,Z)}[I(U;Y)-I(U;Z)]$; (b) $C_s = \max_{p_X(x)}[I(X;Y)-I(X;Z)]$; (c) $C_s = C_M - C_{MW}$; (d) $C_s = \max_{p_X(x)}[I(X;Y)-I(X;Z)]$.

1.1.4 Gaussian wiretap channel

In [4], Leung-Yan-Cheong and Hellman investigated the Gaussian wiretap channel. It is a variant of Wyner's wiretap channel. The model is shown in Figure 1.5. The source is assumed to be stationary, ergodic and with a finite alphabet. The noise vectors in the main channel and the wiretap channel, η_1^N and η_2^N are independent and have components that are i.i.d. according to $\mathcal{N}(0,N_1)$ and $\mathcal{N}(0,N_2)$, respectively. The message $S^K \in \mathcal{S}^K$ has finite alphabet. The input X^N to the main channel has continuous alphabet with an average power constraint: $\frac{1}{N}\sum_{i=1}^{N}\mathrm{E}[X_i^2] \le P$, where $\mathrm{E}(\cdot)$ is the expectation operator. The outputs of the main channel and the wiretap channel are $Y^N = X^N + \eta_1^N$ and $Z^N = Y^N + \eta_2^N$, respectively.

Following the definitions as given in (1.8), (1.9) and (1.10), Leung-Yan-Cheong and Hellman [4] showed that the secrecy capacity of the Gaussian wiretap channel is

$$C_s = C_M - C_{MW} = \frac{1}{2}\log\frac{(P+N_1)(N_1+N_2)}{N_1(P+N_1+N_2)}, \tag{1.17}$$

where C_M and C_{MW} are the capacities of the main channel and overall wiretap channel, respectively. Furthermore, the capacity region of the Gaussian wiretap channel is defined

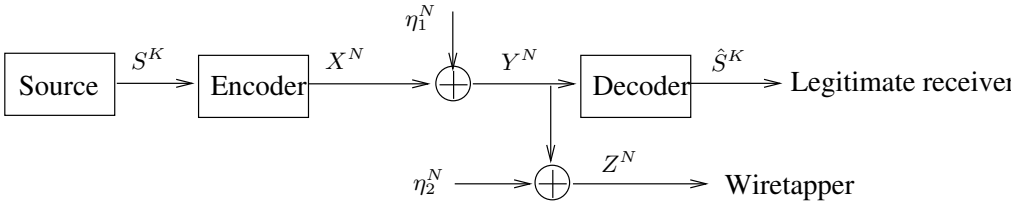


Figure 1.5: Gaussian wiretap channel.

by

$$R \le C_M, \quad d \le 1, \quad Rd \le C_s. \tag{1.18}$$

Surprisingly, $Rd = C_s$ corresponds to a time-sharing curve as established by [4, Lemma 1].

Note that in order to establish the achievability of the entire region, Leung-Yan-Cheong and Hellman [4] only proved that two extreme points $(C_s, 1)$ and $(C_M, C_s/C_M)$ are achievable. Then time sharing [4, Lemma 1] implies the achievability of the capacity region.

1.1.5 Dirty paper channel

Costa [7] considered a communication problem for the following variation of the standard additive white Gaussian noise (AWGN) channel. The model is depicted in Figure 1.6. Here the transmitter wishes to send a message S^K over the channel. The channel output is given by $Y^N = X^N + V^N + \eta^N$, where the channel input X^N has the average power constraint $\frac{1}{N}\Sigma_{i=1}^N \mathrm{E}[X_i^2] \le P$, the noise η^N is distributed according to $\mathcal{N}(0, N\mathrm{I})$, and the side information V^N is independent of η^N and is distributed according to $\mathcal{N}(0, Q\mathrm{I})$. Assume that the side information V^N is known to the transmitter but not to the receiver. Further assume that the side information V^N is *noncausally* available at the transmitter in the sense that at time i the channel input signal X_i can be chosen, based on the message S^K and the whole sequence V^N.

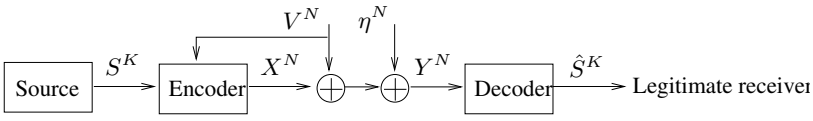


Figure 1.6: Dirty paper channel.

Costa [7] described this channel using an analogy of writing on dirty paper. So the channel is also named dirty paper channel. The communication problem over the dirty paper channel can be stated as follows. Imagine a sheet of paper covered with independent dirt spots having normally distributed intensity. The transmitter writes a message on it using a limited amount of ink and sends it to a receiver. Along the way the paper acquires more normally distributed dirt. Assume that the recipient cannot distinguish between ink and dirt. The question is: how much information can be reliably sent. Surprisingly, Costa [7] showed that the capacity of the dirty paper channel is

$$C = \frac{1}{2}\log(1 + \frac{P}{N}), \tag{1.19}$$

which is equal to the capacity of the corresponding standard AWGN channel. Therefore, the original dirt on the paper (i.e., side information) has no effect on the channel capacity.

To prove this result, Costa [7] used a capacity theorem by Gel'fand and Pinsker [10] and Heegard and El Gamal [11], which states that the capacity of a discrete memoryless channel with side information V noncausally known at the transmitter is given by

$$C = \max_{p_{U,X|V}(u,x|v)} [I(U;Y) - I(U;V)], \tag{1.20}$$

where the maximum is taken over all input distributions $p_{U,X|V}(u,x|v)$ with a finite-alphabet auxiliary random variable U. Costa [7] also pointed out that this result can be extended to continuous alphabets and average input constraints by using the standard argument as in [18, Chapter 7]. Hence, the given problem can be reduced to that of finding an appropriate choice of U and distribution $p(u,x|v)$. With the choice of the input distribution given by

$$\begin{aligned} &X \sim \mathcal{N}(0,P) \qquad \textit{independent of } V, \\ &U = X + \alpha V \qquad \textit{with } \alpha = \frac{P}{P+N}, \end{aligned}$$

it can be readily checked that (1.19) is attained.

Channel models similar to the dirty paper channel have been widely studied. An interesting and fruitful application of the dirty paper coding arises in the Gaussian broadcast channels, where one can treat the encoded signal for one message as the known interference and use the dirty paper coding for the other message [36]. This strategy turns out to be optimal for scalar Gaussian broadcast channels. For multiple antenna Gaussian broadcast channels the optimal sum rate can be obtained [36–39], although the capacity region in general is unknown.

The result on the property that the side information does not affect the capacity of the AWGN channel has been extended in many directions. It has been shown that the same property holds for general ergodic (possibly non-Gaussian) side information and stationary (but not necessarily white) Gaussian noise [34], for any colored (not necessarily stationary or ergodic) Gaussian side information and noise [40], and for the case where the side information is an arbitrary sequence if common randomness is available at both the transmitter and receiver [41]. In addition, it has been shown that the same property holds not only for dirty paper channel but also for some Gaussian multiple user channels [42], for example, the Gaussian broadcast channel with side information, the Gaussian multiple access channel with side information and the physically degraded Gaussian relay channel with side information. Moreover, in [42], it has been pointed out that this result can be extended to any (possible non-Gaussian) stationary ergodic side information and any stationary Gaussian noise.

In practice, the side information could be memory defect locations, known interference, image or audio etc. Costa's result has been applied to many scenarios especially in the fields of watermarking [34] and information hiding [33]. For instance, the watermarking problem can be viewed as a communication problem over the dirty paper channel. Recall that watermarking is to hide a message signal or "watermark" in a host signal or "host image". The embedding must be done such that the embedded signal causes no serious distortion to its host. At the same time, the embedding must be robust to common degradations of the watermarked signal so that the embedded information can be reliably recovered if needed. Note that the host image in watermarking plays the role of side information in the dirty paper channel. Furthermore, the condition that the host image should not be overly perturbed by the watermarking can be translated to an equivalent power constraint on the

distortion, which is corresponding to the power constraint at the transmitter in the dirty paper channel. Therefore, the optimal watermarking scheme uses dirty paper coding and achieves the capacity.

1.1.6 Gaussian wiretap channel with side information

Mitrpant [8, 9] investigated an extension of Wyner's model: the Gaussian wiretap channel with side information. The model is shown in Figure 1.7. It is an extension from the Gaussian wiretap channel by adding an interference (i.e., side information) in the main channel. The interference is modelled as a sequence V^N of i.i.d. random variables such that $V^N \sim \mathcal{N}(0, Q\mathrm{I})$, independent of the noises η_1^N, η_2^N and the message S^K. Assume that the whole sequence of the interference is known to the encoder before the secret message transmission.

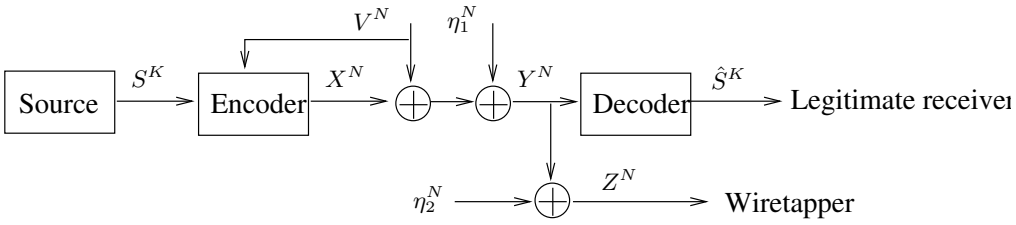


Figure 1.7: Gaussian wiretap channel with side information.

For the Gaussian wiretap channel with side information, Mitrpant gave an achievable rate equivocation region as shown in [8, Theorem 4.4] or [9, Theorem 3]. In order to establish the region, he used the technique similar to Leung-Yan-Cheong and Hellman [4] for the Gaussian wiretap channel without side information. First he showed that under different conditions, three specific rate equivocation pairs are achievable. Time sharing then implies the achievability of the rate equivocation region.

Note that the Gaussian wiretap channel with side information is also an extension of the dirty paper channel by introducing a wiretapper. Using a similar approach of writing on dirty paper, we consider the following communication problem: the transmitter wants to send a secret to a receiver and he knows there is a wiretapper. He writes the secret on a paper using a limited amount of ink and sends it. Along the way to the legitimate receiver, the paper acquires normally distributed dirt. Assume that the wiretapper has access to the paper with additional normally distributed dirt. Now the question of our interest is: how much secret information can be reliably and securely sent to the legitimate receiver without leaking information about the secret to the wiretapper. If the transmitter uses a blank paper (i.e., without side information), he can send secret information at rates up to the secrecy capacity of the Gaussian wiretap channel, which is equal to the difference of the capacities of the main and overall wiretap channels as shown by Leung-Yan-Cheong and Hellman [4]. However, to achieve reliable, efficient and especially secure communication, we wonder whether a dirty paper might be a better choice than the blank paper as one would choose intuitively. To this question, Mitrpant [8, 9] has not provided a complete answer yet.

1.1.7 Other related work

In [43], it was shown that for Wyner's wiretap channel, it is possible to send several low-rate messages, each completely protected from the wiretapper individually, and use the

main channel at rate close to the capacity. However, if any of the messages are available to the wiretapper, the secrecy of the rest may also be compromised.

In [44], it was suggested that the secrecy constraint developed by Wyner [1] and subsequently followed by Csiszár and Körner [5] needed to be strengthened, since it constraints the rate of information leaked to the wiretapper, rather than the total information, and the information of interest might be in this small amount. It was also shown that Wyner's scenario can be extended to "strong" secrecy constraints, where the limit is on the total leaked information rather than just the rate, with no loss in achievable rates using extractor functions.

In [45], Ozarow and Wyner studied another model, referred to as the wiretap channel II, where the main communication channel is noiseless, but the wiretapper has access to a subset of the coded bits. In order to transmit a K-bit message, an N-bit codeword is sent to the channel, where the wiretapper can observe a subset of his choice of $u < N$. The encoder is to be designed to maximize the wiretapper's uncertainty about the message given his intercepted channel bits, subject to the condition that the legitimate receiver can recover the message perfectly. The optimal trade-offs among the parameters K, N, u and the wiretapper's uncertainty have been characterized in [45].

In [46], Maurer considered the wiretap channel with noiseless feedback. The problem is how to distill a secret key to be used for encryption between two parties, when the wiretapper has partial information about a common random variable shared by the two parties. It was shown that the existence of a public feedback channel (where the wiretapper can obtain a perfect copy of the messages transmitted over this public channel), can enable the two parties to generate a secret key even when the wiretapper's channel is superior to the other two channels. Upper and lower bounds were derived for the secrecy capacity of the wiretap channel with noiseless feedback. However, in general, the secrecy capacity of this channel remains unknown. Maurer et al. [47–49] also examined the case of active adversaries, where the wiretapper has read/write access to the channel. In [50, 51], Csiszár and Narayan considered the case of multiple terminals where a number of terminals are trying to distill a secret key and a subset of these terminals act as helper terminals to the rest.

In [52], Yamamoto extended the wiretap channel model to have two parallel discrete memoryless broadcast channels, connecting one encoder and one legitimate decoder, where both channels are wiretapped by non-collaborating wiretappers. Assume that the legitimate channel is less noisy than the wiretapped channel. The admissible region were given in terms of single-letter characterization. In [53], Yamamoto investigated the Gaussian case of the model and described its admissible region by the capacities and secrecy capacities of two Gaussian wiretap channels.

In [54], Yamamoto extended the wiretap channel model in two ways. First, a secret key is allowed to be shared between the encoder and the legitimate receiver. Secondly, a certain distortion in the reconstruction of the source is allowed at the legitimate receiver. In [55], Merhav adopted the structure of a degraded broadcast channel as in [1]. Similarly as in [54], he allowed a secret key shared between the encoder and the legitimate receiver, as well as lossy reconstruction of the source within a prescribed distortion level. But, moreover, he introduced side information, correlated to the source, to be available both to the legitimate receiver and the wiretapper. Assume that the wiretapper receives its side information via a channel that is degraded relative to the side information channel of the legitimate receiver. A single letter characterization of the optimal trade-off was provided among the equivocation at the wiretapper, the rate of the secret key, the distortion in reconstructing the source

at the legitimate receiver, the bandwidth expansion factor of the coded channels, and the average transmission cost (generalized power).

In [56], Tekin and Yener considered the Gaussian multiple access wiretap channel. In this scenario, multiple users communicate with a legitimate receiver in the presence of an wiretapper who receives a degraded version of the signal at the receiver. Achievable rate regions were found for different secrecy constraints. Furthermore, it was shown that the secrecy sum-capacity could be achieved by using Gaussian codebooks and stochastic encoders. In [57], Tekin and Yener considered another scenario, two-way wiretap channels. In this situation, two users communicate with each other in the presence of a wiretapper, who has access to the communications through a multiple access channel. They found achievable rates for the Gaussian two-way wiretap channel and the binary additive two-way wiretap channel. The showed that the two-way channels inherently provide a unique advantage for wiretapper scenarios, as the users know their own transmitted message and in effect help encrypt the other user's message, similar to a one-time pad. Note that the Gaussian multiple access wiretap channel [56] and the Gaussian two-way wiretap channel [57] are of interest in wireless communications as they correspond to the case where a single physical channel is utilized by multiple transmitter, such as in an ad-hoc network.

1.2 Thesis outline

Recall that Gel'fand and Pinsker [10] and Heegard and El Gamal [11] proved that the capacity of a discrete memoryless channel with side information V noncausally known at the transmitter is given by the formula (1.20). This result was extended to the Gaussian case by Costa in [7], where he considered the Gaussian channel with side information when side information is known to the transmitter. He showed that the capacity of the Gaussian channel with side information, also called dirty paper channel, is the same as if there is no side information present. Therefore, the side information does not affect the capacity of the channel. Furthermore, he showed that for the dirty paper channel, by choosing codewords orthogonal to the side information, the channel capacity could be reached by dirty paper coding.

Note that the Gaussian wiretap channel with side information is an extension of the dirty paper channel by introducing a wiretapper. If Costa's result shows that the dirty paper could carry as much information as the blank paper, then we wonder whether for the wiretap channel, dirty paper is a better choice than the blank paper to hide information from the wiretapper as one would choose intuitively. Besides, due to Costa's analysis on dirty paper coding, one prefers to send codewords independent of the side information in order to yield the optimal efficiency from the transmitter to the receiver. However, we wonder whether it might be a better choice to send codewords dependent on the side information for the wiretap channel, in order to yield a higher efficiency to the legitimate receiver at a certain security level from the wiretapper.

In order to answer the above questions, we first review some theoretical background on information theory in Chapter 2. Motivated by Costa's method, in Chapter 3, we investigate the discrete memoryless wiretap channel with side information. The model is shown in Figure 1.8. For this model, we give an achievable rate equivocation region. In addition, the secrecy capacity in some special cases is also determined.

In Chapter 4, we extend our result for the discrete memoryless case to the Gaussian case. An achievable rate equivocation region is derived for the Gaussian wiretap channel with side

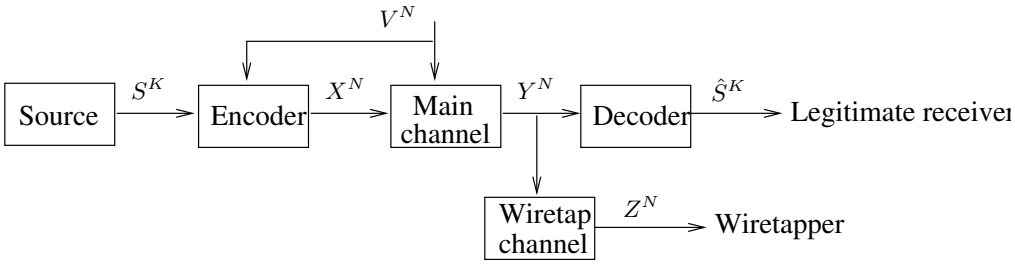


Figure 1.8: Wiretap channel with side information.

information by using the strategy similar to Costa. Then, we compare the performance of the region with the capacity region given by Leung-Yan-Cheong and Hellman [4, Theorem 1] for the wiretap channel without side information. We show that, for the Gaussian wiretap channel, unlike the dirty paper channel, side information helps to get a larger secrecy capacity and achieve a larger rate equivocation region. Furthermore, we generalize Costa's strategy by taking the correlation coefficient of the codeword and side information as another parameter into our consideration. As a consequence of an additional parameter in our optimization, the rate equivocation region is improved by using the generalized Costa's strategy. In other words, for the Gaussian wiretap channel with side information, it might be a better choice in some cases to send codewords dependent on side information, in order to yield a higher efficiency to the legitimate receiver at a certain security level from the wiretapper. As we will see, our region for the Gaussian wiretap channel with side information improves the one given by Mitrpant in [8, Theorem 4.4] or [9, Theorem 3].

In Chapter 5, we focus on the problem of developing forward coding schemes with linear codes for secure communication over the wiretap channel. An example has been provided by Wyner in [1] for the special case when the main channel is noiseless and the wiretap channel is a BSC. Another example is given by Thangaraj et al. [22] for the situation when the main channel is noiseless and the wiretap channel is a binary erasure channel (BEC). We consider the specific case when both the main channel and the wiretap channel are BSCs. We prove that the secrecy capacity can be achieved by using random linear codes[2]. However, the random coding technique used in the proof is rather impractical. For practical purpose, we investigate the performance of the coding schemes when linear codes are used in the construction. The performance is evaluated from the perspectives of the efficiency, reliability and security.

In Chapter 6, we reformulate the security problem in biometrics as a communication problem for the wiretap channel. Two fuzzy commitment schemes based on error correcting codes are reviewed. We characterize the performance of both schemes with the terminologies for the wiretap channel.

In Chapter 7, we summarize the contributions of this thesis and discuss some future research directions.

[2]Refer to [21, Chapter 14] for random linear code.

Chapter 2

Theoretical Background

The communication problem for the wiretap channel with side information is primarily concerned with finding its capacity region. To do this, first we need to prove that a particular region is achievable. Furthermore, a converse should be given to establish that no points outside the region is achievable. The region then is the capacity region. In this chapter, we will introduce most of the basic definitions required for the subsequent development of the analysis on the wiretap channel with side information.

2.1 Basic definitions

First we recall some basic definitions on the information measures of random variables. For discrete random variables, we follow the definitions of *entropy, joint entropy, conditional entropy* and *mutual information* given by Cover and Thomas [19].

Definition 2.1.1 *The entropy of a discrete random variable X with a probability mass function $p_X(x)$ is defined by*

$$H(X) = -\sum_{x\in\mathcal{X}} p_X(x)\log p_X(x) = -\mathrm{E}\log p_X(X). \tag{2.1}$$

Definition 2.1.2 *The joint entropy of a pair of discrete random variables (X,Y) with a joint probability mass function $p_{XY}(x,y)$ is defined as*

$$H(X,Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p_{XY}(x,y)\log p_{XY}(x,y) = -\mathrm{E}\log p_{XY}(X,Y). \tag{2.2}$$

Definition 2.1.3 *The conditional entropy of a pair of discrete random variables (X,Y) with a joint probability mass function $p_{XY}(x,y)$ and a conditional probability mass function $p_{Y|X}(y|x)$ is defined as*

$$H(Y|X) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p_{XY}(x,y)\log p_{Y|X}(y|x) = -\mathrm{E}\log p_{Y|X}(Y|X). \tag{2.3}$$

Definition 2.1.4 *The mutual information of a pair of discrete random variables (X,Y) with a joint probability mass function $p_{XY}(x,y)$ and marginal probability mass functions*

$p_X(x)$ *and* $p_Y(y)$ *is defined as*

$$I(X;Y) = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p_{XY}(x,y)\log\frac{p_{XY}(x,y)}{p_X(x)p_Y(y)} = \mathrm{E}\log\frac{p_{XY}(X,Y)}{p_X(X)p_Y(Y)}. \tag{2.4}$$

Correspondingly, replacing the summations by integrations and the probability mass functions by probability density functions, we have the definitions of *differential entropy, joint differential entropy, conditional differential entropy* and *mutual information* for continuous random variables. In this thesis, the logarithms in these quantities are taken to the base 2 for discrete random variables, and to the base e for continuous random variables.

In particular, applying the definitions of differential entropy, joint differential entropy and mutual information to Gaussian random variables, we have the following:

Definition 2.1.5 *The differential entropy of a Gaussian variable* X*, where* $X \sim \mathcal{N}(0,\sigma_X^2)$ *with mean zero and variance* σ_X^2*, is*

$$H(X) = \frac{1}{2}\log 2\pi e\sigma_X^2. \tag{2.5}$$

Definition 2.1.6 *The joint differential entropy of a pair of Gaussian variable* (X,V)*, where* $(X,V) \sim \mathcal{N}(0,\mathrm{K})$ *with means zero and covariance matrix* K*, is*

$$H(X,V) = \frac{1}{2}\log(2\pi e)^2|\mathrm{K}|, \tag{2.6}$$

where $|K|$ *denotes the determinant of* K*.*

Definition 2.1.7 *Let* X *and* V *be two Gaussian variables, where* $X \sim \mathcal{N}(0,\sigma_X^2)$ *and* $V \sim \mathcal{N}(0,\sigma_V^2)$*. Suppose the covariance matrix of* X *and* V *is* K *with* $|\mathrm{K}| = \sigma_X^2\sigma_V^2(1-\rho_{XV}^2)$*, where* ρ_{XV} *is the correlation coefficient. Then, the mutual information between* X *and* V *is*

$$I(X;V) = \frac{1}{2}\log\frac{1}{1-\rho_{XV}^2}. \tag{2.7}$$

2.2 Asymptotic equipartition property (AEP)

In probability theory, assume that the components of X^N, $X_1, X_2, \cdots, X_N$ are generated independently according to $p_X(x)$. Then the law of large numbers states that, $\frac{1}{N}\sum_{i=1}^N X_i$ is close to its expected value EX for large values of N.

In information theory, as a direct consequence of the weak law of large numbers, the AEP states that $\frac{1}{N}\log\frac{1}{p_{X^N}(x^N)}$ is close to the entropy $H(X)$, where $p_{X^N}(X^N) = \prod_{i=1}^N p_X(x_i)$. Thus the probability assigned to an observed sequence will be close to $2^{-H(X)}$. This enables us to divide the set of all sequences into two sets, the typical set, where the sample entropy is close to the true entropy, and the non-typical set, which contains the other sequences. Most of our attention will be on the typical sequences. The reason is that any property that is proved for the typical sequences will then be true with high probability and will determine the average behavior. Now we recall some basic results concerning typical sequences.

Definition 2.2.1 *The typical set* $T_X^N(\epsilon)$ *with respect to* $p_X(x)$ *is the set of sequences* $x^N \in \mathcal{X}^N$ *with the following property*

$$2^{-N(H(X)+\epsilon)} \le p_{X^N}(x^N) \le 2^{-N(H(X)-\epsilon)}, \tag{2.8}$$

where $p_{X^N}(x^N) = \prod_{i=1}^{N} p_X(x_i)$.

A sequence is said to be ϵ-*typical* with respect to $p_X(x)$ if $x^N \in T_X^N(\epsilon)$. As a direct consequence, we have the following lemma. Refer to [19, Chapter 3] for its proof.

Lemma 2.2.2 *The typical set $T_X^N(\epsilon)$ has the following properties:*

1. *For any $\delta > 0$, $\Pr\{T_X^N(\epsilon)\} > 1 - \delta$ for N sufficiently large.*
2. *$|T_X^N(\epsilon)| \leq 2^{N(H(X)+\epsilon)}$, where $|T_X^N(\epsilon)|$ denotes the number of the elements in the set $T_X^N(\epsilon)$.*
3. *$|T_X^N(\epsilon)| \geq (1-\epsilon)2^{N(H(X)-\epsilon)}$ for N sufficiently large.*

Consider the AEP of Gaussian sequences. The following lemmata show the characteristics of typical Gaussian sequences. Refer to [8, Chapter 2] for their proofs. Note that here we use the natural logarithm.

Lemma 2.2.3 *If X^N is a sequence of random variables i.i.d. according to $\mathcal{N}(0, \sigma_X^2)$, and $x^N \in T_X^N(\epsilon)$ for any $\epsilon > 0$, then*

$$|\frac{1}{N}\sum_{i=1}^{N}\frac{x_i^2}{\sigma_X^2} - 1| < 2\epsilon.$$

Lemma 2.2.4 *Let X^N be a sequence of random variables i.i.d. according to $\mathcal{N}(0, \sigma_X^2)$. If $x^N \in T_X^N(\epsilon)$ for any $\epsilon > 0$, and $\sigma_X^2 \leq \frac{P}{1+2\epsilon}$, then*

$$\frac{1}{N}\sum_{i=1}^{N} x_i^2 \leq P.$$

Lemma 2.2.5 *Let (X^N, Y^N) be a pair of sequences of random variables i.i.d. according to the joint probability density function $p_{XY}(x, y)$ and the marginal probability density functions $p_X(x) \sim \mathcal{N}(0, \sigma_X^2)$ and $p_Y(y) \sim \mathcal{N}(0, \sigma_Y^2)$, where*

$$p_{XY}(x,y) = \frac{1}{2\pi\sigma_X\sigma_Y\sqrt{1-\rho_{XY}^2}}\exp\{-\frac{1}{2(1-\rho_{XY}^2)}[\frac{x^2}{\sigma_X^2} - \frac{2\rho_{XY}xy}{\sigma_X\sigma_Y} + \frac{y^2}{\sigma_Y^2}]\}$$

and ρ_{XY} is the correlation coefficient. If $(x^N, y^N) \in T_{X,Y}^N(\epsilon)$ for any $\epsilon > 0$, then

$$\begin{aligned}
|\frac{1}{N}\sum_{i=1}^{N}\frac{x_i^2}{\sigma_X^2} - 1| &< 2\epsilon, \\
|\frac{1}{N}\sum_{i=1}^{N}\frac{y_i^2}{\sigma_Y^2} - 1| &< 2\epsilon, \\
|\frac{1}{N}\sum_{i=1}^{N}\frac{x_i y_i}{\rho_{XY}\sigma_X\sigma_Y} - 1| &< (\frac{3}{\rho_{XY}^2} - 1)\epsilon.
\end{aligned}$$

In [8, Chapter 2], a special setup, in which $U^N = X^N + \alpha V^N$ for a real constant α, and X^N and V^N are independent Gaussian sequences, is also discussed. Two lemmata regarding it are shown as follows. Refer to [8, Chapter 2] for their proofs.

Lemma 2.2.6 *Let X^N and V^N be two independent sequences of i.i.d. random variables $X \sim \mathcal{N}(0, \sigma_X^2)$ and $V \sim \mathcal{N}(0, \sigma_V^2)$, respectively. Let $U^N = X^N + \alpha V^N$ for a constant real number α. If $(u^N, v^N) \in T_{U,V}^N(\epsilon)$ for any $\epsilon > 0$, then $x^N = u^N - \alpha v^N$ satisfies*

$$\begin{aligned} x^N &\in T_X^N(2\epsilon), \\ |\frac{1}{N}\sum_{i=1}^N x_i v_i| &< \frac{3\sigma_X^2 + 2\alpha^2\sigma_V^2}{\alpha}\epsilon. \end{aligned}$$

Lemma 2.2.7 *Let X^N and V^N be two independent sequences of i.i.d. random variables $X \sim \mathcal{N}(0, \sigma_X^2)$ and $V \sim \mathcal{N}(0, \sigma_V^2)$, respectively. Let $U^N = X^N + \alpha V^N$ for a constant real number α. If $(u^N, v^N) \in T_{U,V}^N(\epsilon)$ for any $\epsilon > 0$ and $\sigma_X^2 \leq \frac{P}{1+4\epsilon}$, then*

$$\frac{1}{N}\sum_{i=1}^N x_i^2 \leq P.$$

We consider a more general setup, in which $U^N = X^N + \alpha V^N$ for a real constant α, and X^N is not necessarily independent of V^N. As a general version of the above two lemmata, we have the following.

Lemma 2.2.8 *Let X^N and V^N be two sequences of i.i.d. random variables $X \sim \mathcal{N}(0, \sigma_X^2)$ and $V \sim \mathcal{N}(0, \sigma_V^2)$, respectively. Let ρ_{XV} be the correlation coefficient between X and V. Let $U^N = X^N + \alpha V^N$ for a constant real number α. If $(u^N, v^N) \in T_{U,V}^N(\epsilon)$ for any $\epsilon > 0$, then $x^N = u^N - \alpha v^N$ satisfies*

$$\begin{aligned} x^N &\in T_X^N(c\epsilon), \\ |\frac{1}{N}\sum_{i=1}^N \frac{x_i v_i}{\sigma_X \sigma_V} - \rho_{XV}| &< \frac{(\frac{3}{\rho_{UV}^2} - 1)|\rho_{UV}|\sigma_U + 2|\alpha|\sigma_V}{\sigma_X}\epsilon. \end{aligned}$$

where $\sigma_U = \sqrt{\sigma_X^2 + \alpha^2\sigma_V^2 + 2\alpha\sigma_X\sigma_V\rho_{XV}}$, $\rho_{UV} = (\sigma_X\sigma_V\rho_{XV} + \alpha\sigma_V^2)/\sigma_U\sigma_V$ and $c = \{\sigma_U^2 + \alpha^2\sigma_V^2 + |\alpha|(\frac{3}{\rho_{UV}^2} - 1)|\rho_{UV}|\sigma_U\sigma_V\}/\sigma_X^2$.

Proof: Note that X^N and V^N are two sequences of i.i.d. Gaussian random variables. Clearly, $U^N = X^N + \alpha V^N$ is a sequence of i.i.d. Gaussian random variables $U \sim \mathcal{N}(0, \sigma_U^2)$, where $\sigma_U^2 = \sigma_X^2 + \alpha^2\sigma_V^2 + 2\alpha\sigma_X\sigma_V\rho_{XV}$. Let ρ_{UV} be the correlation coefficient between U and V. Due to $X = U - \alpha V$, we have $\sigma_X^2 = \sigma_U^2 + \alpha^2\sigma_V^2 - 2\alpha\sigma_U\sigma_V\rho_{UV}$. It is easy to verify that $\sigma_U\sigma_V\rho_{UV} = \sigma_X\sigma_V\rho_{XV} + \alpha\sigma_V^2$.

Since $(u^N, v^N) \in T_{U,V}^N(\epsilon)$, by Lemma 2.2.5, we have

$$|\frac{1}{N}\sum_{i=1}^N \frac{u_i^2}{\sigma_U^2} - 1| < 2\epsilon \Leftrightarrow |\frac{1}{N}\sum_{i=1}^N u_i^2 - \sigma_U^2| < 2\sigma_U^2\epsilon,$$

$$|\frac{1}{N}\sum_{i=1}^N \frac{v_i^2}{\sigma_V^2} - 1| < 2\epsilon \Leftrightarrow |\frac{1}{N}\sum_{i=1}^N v_i^2 - \sigma_V^2| < 2\sigma_V^2\epsilon,$$

$$|\frac{1}{N}\sum_{i=1}^N \frac{u_i v_i}{\rho_{UV}\sigma_U\sigma_V} - 1| < (\frac{3}{\rho_{UV}^2} - 1)\epsilon \Leftrightarrow |\frac{1}{N}\sum_{i=1}^N u_i v_i - \rho_{UV}\sigma_U\sigma_V| < (\frac{3}{\rho_{UV}^2} - 1)|\rho_{UV}|\sigma_U\sigma_V\epsilon.$$

Note that for $i = 1, \cdots, N$, $u_i = x_i + \alpha v_i$. In addition that $\sigma_U \sigma_V \rho_{UV} = \sigma_X \sigma_V \rho_{XV} + \alpha \sigma_V^2$,

$$\begin{aligned} |\frac{1}{N}\sum_{i=1}^{N} u_i v_i - \rho_{UV}\sigma_U\sigma_V| &= |\frac{1}{N}\sum_{i=1}^{N}(x_i v_i + \alpha v_i^2) - (\sigma_X\sigma_V\rho_{XV} + \alpha\sigma_V^2)| \\ &= |\frac{1}{N}\sum_{i=1}^{N} x_i v_i - \sigma_X\sigma_V\rho_{XV} + \frac{1}{N}\sum_{i=1}^{N}\alpha v_i^2 - \alpha\sigma_V^2| \\ &< (\frac{3}{\rho_{UV}^2} - 1)|\rho_{UV}|\sigma_U\sigma_V\epsilon. \end{aligned}$$

Therefore,

$$\begin{aligned} |\frac{1}{N}\sum_{i=1}^{N} x_i v_i - \sigma_X\sigma_V\rho_{XV}| &\leq |\frac{1}{N}\sum_{i=1}^{N} u_i v_i - \rho_{UV}\sigma_U\sigma_V| + |\alpha| \cdot |\frac{1}{N}\sum_{i=1}^{N} v_i^2 - \sigma_V^2| \\ &< [(\frac{3}{\rho_{UV}^2} - 1)|\rho_{UV}|\sigma_U\sigma_V + 2|\alpha|\sigma_V^2]\epsilon. \end{aligned}$$

This is equivalent to

$$|\frac{1}{N}\sum_{i=1}^{N}\frac{x_i v_i}{\sigma_X\sigma_V} - \rho_{XV}| < \frac{(\frac{3}{\rho_{UV}^2} - 1)|\rho_{UV}|\sigma_U + 2|\alpha|\sigma_V}{\sigma_X}\epsilon.$$

Due to $x_i = u_i - \alpha v_i$ for $i = 1, \cdots, N$, $x_i^2 = u_i^2 + \alpha^2 v_i^2 - 2\alpha u_i v_i$. Easily we have

$$\begin{aligned} |\frac{1}{N}\sum_{i=1}^{N} x_i^2 - \sigma_X^2| &= |\frac{1}{N}\sum_{i=1}^{N}(u_i^2 + \alpha^2 v_i^2 - 2\alpha u_i v_i) - (\sigma_U^2 + \alpha^2\sigma_V^2 - 2\alpha\sigma_U\sigma_V\rho_{UV})| \\ &\leq |\frac{1}{N}\sum_{i=1}^{N} u_i^2 - \sigma_U^2| + \alpha^2|\frac{1}{N}\sum_{i=1}^{N} v_i^2 - \sigma_V^2| + 2|\alpha| \cdot |\frac{1}{N}\sum_{i=1}^{N} u_i v_i - \rho_{UV}\sigma_U\sigma_V| \\ &< 2[\sigma_U^2 + \alpha^2\sigma_V^2 + |\alpha|(\frac{3}{\rho_{UV}^2} - 1)|\rho_{UV}|\sigma_U\sigma_V]\epsilon. \end{aligned}$$

Since $\sigma_X^2 > 0$,

$$|\frac{1}{N}\sum_{i=1}^{N}\frac{x_i^2}{2\sigma_X^2} - \frac{1}{2}| < \frac{\sigma_U^2 + \alpha^2\sigma_V^2 + |\alpha|(\frac{3}{\rho_{UV}^2} - 1)|\rho_{UV}|\sigma_U\sigma_V}{\sigma_X^2}\epsilon.$$

Note that $p_{X^N}(x^N) = \prod_{i=1}^{N} p_X(x_i)$ and $P_X(x) = \frac{1}{\sqrt{2\pi}\sigma_X}\exp\{-\frac{x^2}{2\sigma_X^2}\}$. Furthermore, due to $X \sim \mathcal{N}(0, \sigma_X^2)$, $H(X) = \frac{1}{2}\log 2\pi e\sigma_X^2$. Therefore, we have the following.

$$\begin{aligned} |-\frac{1}{N}\log p_{X^N}(x^N) - H(X)| &= |-\frac{1}{N}\sum_{i=1}^{N}\log p_X(x_i) - H(X)| \\ &= |-\frac{1}{N}\sum_{i=1}^{N}\log\frac{1}{\sqrt{2\pi}\sigma_X}\exp\{-\frac{x^2}{2\sigma_X^2}\} - \frac{1}{2}\log 2\pi e\sigma_X^2| \end{aligned}$$

$$
\begin{aligned}
&= |\frac{1}{N}\sum_{i=1}^{N}\frac{x_i^2}{2\sigma_X^2} + \frac{1}{2}\log 2\pi\sigma_X^2 - \frac{1}{2}\log 2\pi e\sigma_X^2| \\
&= |\frac{1}{N}\sum_{i=1}^{N}\frac{x_i^2}{2\sigma_X^2} - \frac{1}{2}| \\
&< \frac{\sigma_U^2 + \alpha^2\sigma_V^2 + |\alpha|(\frac{3}{\rho_{UV}^2} - 1)|\rho_{UV}|\sigma_U\sigma_V}{\sigma_X^2}\epsilon.
\end{aligned}
$$

Let $c = \{\sigma_U^2 + \alpha^2\sigma_V^2 + |\alpha|(\frac{3}{\rho_{UV}^2} - 1)|\rho_{UV}|\sigma_U\sigma_V\}/\sigma_X^2$. The last inequality implies that $x^N \in T_X^N(c\epsilon)$. ■

Lemma 2.2.9 *Let X^N and V^N be two sequences of i.i.d. random variables $X \sim \mathcal{N}(0, \sigma_X^2)$ and $V \sim \mathcal{N}(0, \sigma_V^2)$, respectively. Let ρ_{XV} be the correlation coefficient between X and V. Let $U^N = X^N + \alpha V^N$ for a constant real number α. If $(u^N, v^N) \in T_{U,V}^N(\epsilon)$ for any $\epsilon > 0$ and $\sigma_X^2 \leq \frac{P}{1+2c\epsilon}$, then*

$$\frac{1}{N}\sum_{i=1}^{N} x_i^2 \leq P.$$

Here c is a constant as defined in Lemma 2.2.8.

Proof: Since $(u^N, v^N) \in T_{U,V}^N(\epsilon)$, by Lemma 2.2.8, $x^N \in T_X^N(c\epsilon)$. Due to Lemma 2.2.3, it implies

$$|\frac{1}{N}\sum_{i=1}^{N}\frac{x_i^2}{\sigma_X^2} - 1| < 2c\epsilon \Rightarrow \frac{1}{N}\sum_{i=1}^{N}\frac{x_i^2}{\sigma_X^2} < 1 + 2c\epsilon.$$

Therefore,

$$\frac{1}{N}\sum_{i=1}^{N} x_i^2 < \sigma_X^2(1 + 2c\epsilon) \leq \frac{P}{1+2c\epsilon}(1 + 2c\epsilon) = P.$$

■

2.3 Fano-inequality

In this thesis, the achievability proofs are mostly given in terms of typical sequences. The converse proofs are provided for some special cases. The well-known *Fano-inequality* forms the basis of these proofs. We will now recall this inequality. Refer to [19, Theorem 2.11.1] for its proof.

Lemma 2.3.1 *For discrete random variables $X, Y, \hat{X}$ such that $X \to Y \to \hat{X}$ forms a Markov chain, define the probability of error $P_e = \Pr\{X \neq \hat{X}\}$. Then*

$$h(P_e) + P_e \log(|\mathcal{X}| - 1) \geq H(X|Y), \tag{2.9}$$

where $h(\cdot)$ is the binary entropy function and

$$h(P_e) = -P_e \log P_e - (1 - P_e)\log(1 - P_e). \tag{2.10}$$

Chapter 3

Wiretap Channel with Side Information

3.1 Introduction

In this chapter, we investigate the discrete memoryless wiretap channel with side information. The model is shown in Figure 3.1. We consider the following problems: what is the secrecy capacity and what is the rate equivocation region of a discrete memoryless wiretap channel with side information?

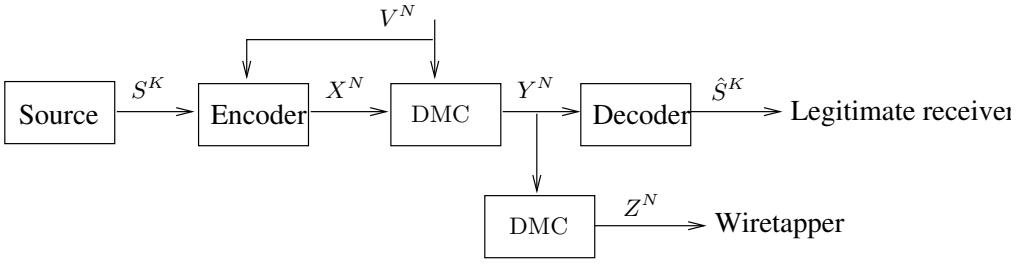


Figure 3.1: Discrete memoryless wiretap channel with side information.

The rest of the chapter is organized as follows. In section 3.2, we present the basic definitions and the main result. In section 3.3, we give the proof of a coding theorem for the discrete memoryless channel with side information. In section 3.4, three corollaries are derived. Finally we conclude in section 3.5.

3.2 Model description

We assume that the source has a finite alphabet. The side information is noncausally known at the encoder and $V_i, 1 \leq i \leq N$, are i.i.d. $\sim p_V(v)$. The encoder examines every K source outputs, s^K. Based on s^K and v^N, the encoder sends a codeword x^N to the main channel. Upon receipt of y^N the decoder at the legitimate receiver makes an estimate $\hat{s}^K$ of the message s^K. Note that y^N is also the input of the wiretap channel. The corresponding

output at the wiretapper is z^N. The channels are *memoryless*, i.e.,

$$p_{Y^N|X^N,V^N}(y^N|x^N,v^N) = \prod_{i=1}^{N} p_{Y|X,V}(y_i|x_i,v_i); \tag{3.1}$$

$$p_{Z^N|Y^N}(z^N|y^N) = \prod_{i=1}^{N} p_{Z|Y}(z_i|y_i). \tag{3.2}$$

Now consider a $(2^{NR}, N)$ code with encoder

$$X^N : \{1, 2, \cdots, 2^{NR}\} \times \mathcal{V}^N \to \mathcal{X}^N$$

and decoder

$$\hat{S}^K : \mathcal{Y}^N \to \{1, 2, \cdots, 2^{NR}\}.$$

Assume that S^K is uniformly distributed. Then the average *probability of error* P_e is

$$P_e = \frac{1}{2^{NR}} \sum_{i=1}^{2^{NR}} \Pr(\hat{S}^K \neq i | S^K = i). \tag{3.3}$$

We define the *rate* of transmission to the legitimate receiver to be

$$R = \frac{H(S^K)}{N}, \tag{3.4}$$

and the fractional *equivocation* of the wiretapper to be

$$d = \frac{H(S^K|Z^N)}{H(S^K)}. \tag{3.5}$$

We say that the pair (R^*, d^*) is *achievable* if, for all $\epsilon > 0$, there exists an encoder-decoder pair such that

$$R \geq R^* - \epsilon, \quad d \geq d^* - \epsilon, \quad P_e \leq \epsilon. \tag{3.6}$$

Define the *secrecy capacity* C_s as the maximum R^* such that $(R^*, 1)$ is achievable.

Denote

$$R_{U1} = I(U;Y) - \max\{I(U;V), I(U;Z)\}, \tag{3.7}$$

$$R_{U2} = I(U;Y) - I(U;V), \tag{3.8}$$

$$d_{U2} = \frac{I(U;Y) - \max\{I(U;V), I(U;Z)\}}{I(U;Y) - I(U;V)}, \tag{3.9}$$

where U is an auxiliary parameter such that $U \to (X, V) \to Y \to Z$ forms a Markov chain. In general, we have the following result.

Theorem 3.2.1 *For the discrete memoryless wiretap channel with side information, we denote $\mathcal{R}_U$ as the set of points (R, d) with*

$$R_{U1} \leq R \leq R_{U2}, \quad 0 \leq d \leq 1, \quad Rd = R_{U1}.$$

Let

$$\mathcal{R}'_U \triangleq \{(R', d') : 0 \le R' \le R, 0 \le d' \le d, (R, d) \in \mathcal{R}_U\}.$$

Then the set $\mathcal{R}$, defined as follows, is achievable:

$$\mathcal{R} = \bigcup_{U \to (X,V) \to Y \to Z} \mathcal{R}'_U. \tag{3.10}$$

The region is already obtained if we limit the cardinality of the range of U by the constraint $|\mathcal{U}| \le |\mathcal{X}||\mathcal{V}| + 3$.

Remarks:

(a) The widely used definition of the achievable rate equivocation pair was first introduced by Wyner [1, (9a)-(9c)]. It implies that if (R, d) is achievable, then for any $0 \le d' \le d$, (R, d') is achievable. Therefore, we concentrate on the problem to achieve as high as possible equivocation for the wiretapper at any fixed rate of reliable transmission to the legitimate receiver.

In addition, if (R, d) is achievable, by time sharing $(0, 0)$ and (R, d), it is easy to prove that for any $0 \le R' \le R$, (R', d) is achievable. Therefore, it is enough to show that $\mathcal{R}_U$ is achievable so as to establish $\mathcal{R}'_U$. Surprisingly, $Rd = c$ corresponds to a time-sharing curve as shown in [4, Lemma 1], where c is a constant.

(b) Recall that the capacity region of the Gaussian wiretap channel given by Leung-Yan-Cheong and Hellman [4, Theorem 1] is defined by

$$R \le C_M, \quad d \le 1, \quad Rd \le C_s,$$

where C_M is the capacity of the main channel and C_s is the secrecy capacity. In order to establish the achievability of the entire region, Leung-Yan-Cheong and Hellman [4] only proved that two extreme points $(C_s, 1)$ and $(C_M, C_s/C_M)$ are achievable. Then time sharing implies the achievability of the region. Thereafter, Mitrpant [8, 9] used similar technique to establish the achievability of the rate equivocation region for the Gaussian wiretap channel with side information. However, our technique is more general. Instead of proving that some particular points are achievable, we introduce an auxiliary parameter U. For each U such that $U \to (X, V) \to Y \to Z$ forms a Markov chain, we show that $(R_{U1}, 1)$ and (R_{U2}, d_{U2}) are achievable. Then time sharing implies the achievability of $\mathcal{R}'_U$. To establish the region $\mathcal{R}$, we go through all possible U.

(c) The constraint on the cardinality of the range of U is implied by [12, Lemma 3]. The proof is given in Appendix II.

(d) The points (R, d) in $\mathcal{R}$ with $d = 1$ is of considerable interest. These correspond to the situation of perfect secrecy. Define

$$R_s = \max_{U \to (X,V) \to Y \to Z} R_{U1}, \tag{3.11}$$

$$C_M = \max_{U \to (X,V) \to Y} [I(U; Y) - I(U; V)]. \tag{3.12}$$

Clearly, we can easily bound the secrecy capacity of the wiretap channel with side information by $R_s \le C_s \le C_M$.

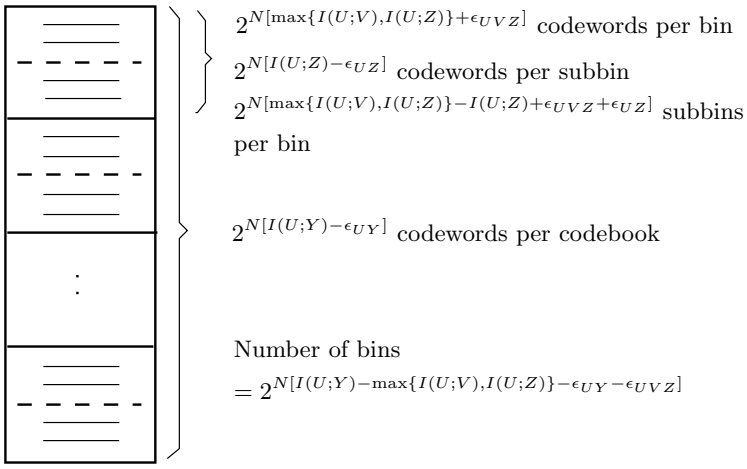


Figure 3.2: The codebook to achieve rate equivocation pair $(R_{U1}, 1)$.

3.3 Achievability proof

In this section, we establish the achievability of the region $\mathcal{R}$. We only need to prove that the rate equivocation pairs $(R_{U1}, 1)$ and (R_{U2}, d_{U2}) are achievable, since time-sharing then implies the achievability of the region $\mathcal{R}'_U$.

3.3.1 $(R_{U1}, 1)$ is achievable

The encoding and decoding strategy is as follows:

1. *Codebook Generation*

   First, generate $2^{N[I(U;Y)-\epsilon_{UY}]}$ i.i.d. sequences u^N, according to the distribution $p_{U^N}(u^N) = \prod_{i=1}^{N} p_U(u_i)$. Next, distribute these sequences at random into 2^{NR} bins such that each bin contains $2^{N[\max\{I(U;V),I(U;Z)\}+\epsilon_{UVZ}]}$ sequences. Here, $R = [R_{U1} - \epsilon_{UY} - \epsilon_{UVZ}]$. Index each bin by $j \in \{1, 2, \cdots, 2^{NR}\}$. Then place the $2^{N[\max\{I(U;V),I(U;Z)\}+\epsilon_{UVZ}]}$ sequences in every bin randomly into $2^{N[\max\{I(U;V),I(U;Z)\}-I(U;Z)+\epsilon_{UVZ}+\epsilon_{UZ}]}$ subbins such that every subbin contains $2^{N[I(U;Z)-\epsilon_{UZ}]}$ sequences. Let W be the random variable to represent the index of the subbin containing U^N. Index each subbin by $w \in \{1, 2, \cdots, 2^{N[\max\{I(U;V),I(U;Z)\}-I(U;Z)+\epsilon_{UVZ}+\epsilon_{UZ}]}\}$.

2. *Encoding*

   To send message j through an interference v^N, the sender looks in bin j for a sequence $u^N(j)$ such that $(u^N(j), v^N)$ is jointly typical, i.e., $(u^N(j), v^N) \in T^N_{U,V}(\epsilon)$. If there is no such $u^N(j)$ jointly typical with v^N, then the sender randomly chooses one sequence in bin j. Send the associated jointly typical $x^N(j)$. ($x^N(j)$ can be generated according to $p_{X^N|U^N,V^N}(x^N(j)|u^N(j), v^N) = \prod_{i=1}^{N} p_{X|U,V}(x_i|u_i, v_i)$.)

3. *Decoding*

   The legitimate receiver receives y^N according to the distribution $\prod_{i=1}^{N} p_{Y|X,V}(y_i|x_i, v_i)$. The receiver looks for the unique sequence u^N in the codebook that is jointly typical with the received sequence y^N, i.e., $(u^N, y^N) \in T^N_{U,Y}(\epsilon)$. Declare the index of the bin containing u^N as the message received.

4. *Wiretapper*

   The wiretapper knows the encoding scheme used at the transmitter and the decoding scheme used by the legitimate receiver. He receives a sequence z^N according to the distribution $\prod_{i=1}^{N} p_{Y|X,V}(y_i|x_i, v_i)p_{Z|Y}(z_i|y_i)$.

For the legitimate receiver, there are three sources of potential error.

- $\mathcal{E}^V(j)$: in the encoding process, given v^N and message j, there is no sequence u^N in the bin j that is jointly typical with v^N.
- $\mathcal{E}^{Y_1}(j)$: in the decoding process, there is no sequence u^N that is jointly typical with the received sequence y^N.
- $\mathcal{E}^{Y_2}(j)$: in the decoding process, there is a sequence $u^N(j')$ in bin j', $j' \neq j$, jointly typical with the received sequence y^N.

From the above encoding and decoding strategy, the codebook we use here is similar to the one used in [7, 10, 11]. Hence, it is easy to show that the information rate R_{U1} from the transmitter to the legitimate receiver is achievable.

Intuitively, a possible decoding strategy for the wiretapper would be to use the same strategy to decode as the legitimate receiver. He will try to find a sequence u^N in the codebook that is jointly typical with the received sequence z^N, and declare the index of the bin in which the sequence is found as the received message. We know that for any z^N, the probability that u^N is jointly typical with z^N is larger than $(1-\epsilon)2^{-N[I(U;Z)+3\epsilon]}$. While in every bin there are $2^{N[\max\{I(U;V),I(U;Z)\}+\epsilon_{UVZ}]}$ sequences, which is more than $2^{N[I(U;Z)+\epsilon_{UVZ}]}$. By choosing appropriate ϵ_{UVZ} and N, we can construct a codebook such that in every bin, with high probability larger than $1-\epsilon$, a sequence u^N is found to be jointly typical with z^N. Therefore, the probability that he decodes the correct message goes to 2^{-NR} as N approaches ∞, which means that $p_{S^K|Z^N}(s^K|z^N) \to p_{S^K}(s^K)$ and $H(S^K|Z^N) \to H(S^K)$. Thus, the equivocation for the wiretapper goes to 1 as N approaches ∞.

We will prove in the following that $(R_{U1}, 1)$ is achievable in two parts, the reliability: $P_e \to 0$, as $n \to \infty$, and the security: $d \to 1$, as $n \to \infty$.

Proof of $P_e \to 0$.

We first analyze the probability of $\mathcal{E}^V(j)$. By the code generating process, u^N and v^N are independent. The probability that a pair (u^N, v^N) is jointly typical is larger than $(1-\epsilon)2^{-N[I(U;V)+3\epsilon]}$ for n sufficiently large. So we have

$$\begin{aligned}
\Pr\{(u^N, v^N) \in T^N_{U,V}(\epsilon)\} &\geq (1-\epsilon)2^{-N[I(U;V)+3\epsilon]} \\
\Pr\{(u^N, v^N) \notin T^N_{U,V}(\epsilon)\} &\leq 1-(1-\epsilon)2^{-N[I(U;V)+3\epsilon]} \\
\Pr\{\mathcal{E}^V(j)|S^K = j\} &\overset{(a)}{\leq} \left[1-(1-\epsilon)2^{-N[I(U;V)+3\epsilon]}\right]^{2^{N[\max\{I(U;V),I(U;Z)\}+\epsilon_{UVZ}]}} \\
&\overset{(b)}{\leq} \exp\left\{-(1-\epsilon)2^{-N[I(U;V)+3\epsilon]}\right\}^{2^{N[\max\{I(U;V),I(U;Z)\}+\epsilon_{UVZ}]}} \\
&= \exp\left\{-(1-\epsilon)2^{N[\max\{I(U;V),I(U;Z)\}-I(U;V)+\epsilon_{UVZ}-3\epsilon]}\right\} \\
&\leq \delta/3,
\end{aligned}$$

where

(a) follows from the fact that there are $2^{N[\max\{I(U;V),I(U;Z)\}+\epsilon_{UVZ}]}$ codewords in a bin;

(b) follows from the inequality $e^a \geq 1+a$.

As shown above, for given ϵ and arbitrary small δ, there exists ϵ_{UVZ} and N_1 such that when $\epsilon_{UVZ} > 3\epsilon$, $N \geq N_1$, both $\Pr\{(u^N, v^N) \in T^N_{U,V}(\epsilon)\} \geq (1-\epsilon)2^{-N[I(U;V)+3\epsilon]}$ and $\Pr\{\mathcal{E}^V(j)|S^K = j\} \leq \delta/3$ hold.

The probability of $\mathcal{E}^{Y_1}(j)$. If the event $\mathcal{E}^V(j)$ does not occur, which means that there is a sequence $u^N(j)$ in bin j and a sequence $x^N(j)$ such that $(u^N(j), x^N(j), v^N)$ is jointly typical, then $(u^N(j), x^N(j), v^N, y^N)$ will be jointly typical with high probability. For given ϵ and arbitrary small δ, there exists N_2 such that when $N \geq N_2$,

$$\Pr\{(u^N, y^N) \in T^N_{U,Y}(\epsilon)\} \geq 1 - \delta/3,$$

which implies that

$$\Pr\{\mathcal{E}^{Y_1}(j)|\mathcal{E}^V(j)^C, S^K = j\} \leq \delta/3.$$

The third source of potential error. If we say that $\mathcal{E}^{Y_2^*}(j)$ occurs when some other u^N is jointly typical with y^N, then it is clear that

$$\Pr\{\mathcal{E}^{Y_2}(j)|\mathcal{E}^V(j)^C, S^K = j\} \leq \Pr\{\mathcal{E}^{Y_2^*}(j)|\mathcal{E}^V(j)^C, S^K = j\}.$$

But a sequence u^N, different from $u^N(j)$, being jointly typical with y^N has probability at most $2^{-N[I(U;Y)-3\epsilon]}$. Since there are only $2^{N[I(U;Y)-\epsilon_{UY}]} - 1$ other sequences, for given ϵ and arbitrary small δ, there exists ϵ_{UY} and N_3 such that when $\epsilon_{UY} > 3\epsilon$, $N \geq N_3$, we have

$$\begin{aligned}
\Pr\{\mathcal{E}^{Y_2}(j)|\mathcal{E}^V(j)^C, S^K = j\} &\leq \Pr\{\mathcal{E}^{Y_2^*}(j)|\mathcal{E}^V(j)^C, S^K = j\} \\
&\leq \sum_{u^N \neq u^N(j)} 2^{-N[I(U;Y)-3\epsilon]} \\
&\leq (2^{N[I(U;Y)-\epsilon_{UY}]} - 1)2^{-N[I(U;Y)-3\epsilon]} \\
&< 2^{N[I(U;Y)-\epsilon_{UY}]-N[I(U;Y)-3\epsilon]} \\
&= 2^{-N[\epsilon_{UY}-3\epsilon]} \\
&\leq \delta/3.
\end{aligned}$$

This shows that all three error events are of arbitrarily small probability. By the union bound [1] on these three probabilities of error, for $\epsilon_{UY}, \epsilon_{UVZ} > 3\epsilon$, $N \geq \max\{N_1, N_2, N_3\}$, the average probability of error

$$\begin{aligned}
P_e &= \frac{1}{2^{nR}} \sum_{j=1}^{2^{nR}} \Pr(\hat{S}^K(Y^N) \neq j|S^K = j) \\
&\leq \frac{1}{2^{nR}} \sum_{j=1}^{2^{nR}} [\Pr\{\mathcal{E}^V(j)|S^K = j\} + \Pr\{\mathcal{E}^{Y_1}(j)|\mathcal{E}^V(j)^C, S^K = j\} \\
&\quad + \Pr\{\mathcal{E}^{Y_2}(j)|\mathcal{E}^V(j)^C, S^K = j\}] \\
&\leq \frac{1}{2^{nR}} \sum_{j=1}^{2^{nR}} [\delta/3 + \delta/3 + \delta/3] \\
&= \delta.
\end{aligned}$$

[1] Let $\mathcal{E}_i$, $i \in \{1, \cdots, N\}$ be events of interest of an experiment. Then $\Pr\{\bigcup_{i=1}^N \mathcal{E}_i\} \leq \sum_{i=1}^N \Pr\{\mathcal{E}_i\}$.

This concludes the proof of reliability.

Proof of $d \to 1$.

Consider the uncertainty of the message to the wiretapper in three steps:

1. show that

$$H(S^K|Z^N) \geq NR_{U1} - N[\epsilon_{UVZ} + \epsilon_{UZ}] - H(U^N|S^K, W, Z^N).$$

   (See the codebook generation in section 3.3.1.)

2. show that

$$H(U^N|S^K, W, Z^N) \leq h(P_{SB}) + P_{SB}N[I(U;Z) - \epsilon_{UZ}].$$

   Here P_{SB} means a wiretapper's error probability in the case where the bin and the subbin number are known to the wiretapper.

3. show that for arbitrary $0 < \lambda < 1/2$, $P_{SB} \leq \lambda$.

Combining the above steps, we have

$$\begin{aligned}
d &= \frac{H(S^K|Z^N)}{H(S^K)} \\
&\geq \frac{NR_{U1} - N[\epsilon_{UVZ} + \epsilon_{UZ}] - H(U^N|S^K, W, Z^N)}{NR} \\
&\geq \frac{NR + N[\epsilon_{UY} - \epsilon_{UZ}] - h(P_{SB}) - P_{SB}N[I(U;Z) - \epsilon_{UZ}]}{NR} \\
&\geq \frac{NR + N[\epsilon_{UY} - \epsilon_{UZ}] - h(\lambda) - \lambda N[I(U;Z) - \epsilon_{UZ}]}{NR} \\
&= 1 - \frac{\epsilon_{UZ} - \epsilon_{UY} + h(\lambda)/N + \lambda[I(U;Z) - \epsilon_{UZ}]}{R_{U1} - \epsilon_{UY} - \epsilon_{UVZ}}.
\end{aligned}$$

We now proceed to step 1 by considering

$$\begin{aligned}
H(S^K|Z^N) &= H(S^K, Z^N) - H(Z^N) \\
&= H(S^K, W, Z^N) - H(W|S^K, Z^N) - H(Z^N) \\
&= H(S^K, W, U^N, Z^N) - H(U^N|S^K, W, Z^N) - H(W|S^K, Z^N) - H(Z^N) \\
&= H(S^K, W|U^N, Z^N) + H(U^N, Z^N) - H(U^N|S^K, W, Z^N) \\
&\quad -H(W|S^K, Z^N) - H(Z^N) \\
&\overset{(a)}{=} H(U^N|Z^N) - H(U^N|S^K, W, Z^N) - H(W|S^K, Z^N) \\
&\overset{(b)}{\geq} H(U^N|Z^N) - H(U^N|S^K, W, Z^N) - \log|W| - H(U^N|Y^N) \\
&\overset{(c)}{=} N[I(U;Y) - I(U;Z)] - H(U^N|S^K, W, Z^N) \\
&\quad -N[\max\{I(U;V), I(U;Z)\} - I(U;Z) + \epsilon_{UVZ} + \epsilon_{UZ}] \\
&= NR_{U1} - N[\epsilon_{UVZ} + \epsilon_{UZ}] - H(U^N|S^K, W, Z^N),
\end{aligned}$$

where

(a) follows from the fact that $H(S^K, W|U^N, Z^N) \geq 0$;

(b) follows from the fact that $H(W|S^K, Z^N) \leq H(W) \leq \log|W|$ and $H(U^N|Y^N) \geq 0$;

(c) follows from the fact that $I(U^N;Y^N) = NI(U;Y)$, $I(U^N;Z^N) = NI(U;Z)$ and $\log|W| = N[\max\{I(U;V), I(U;Z)\} - I(U;Z) + \epsilon_{UVZ} + \epsilon_{UZ}]$.

Thus the proof of step 1 is completed.

To prove step 2, we need to bound the entropy of the codeword conditioned on the bin j, subbin w and the wiretapper's observation z^N. We take the subbin w in bin j as a codebook, U^N in the codebook as the input messages, Z^N as the result of passing U^N through the discrete memoryless channel. From Z^N, we estimate the message U^N that was sent. Let $g(\cdot)$ be the decoder and the estimate be $\hat{U}^N = g(Z^N)$. Define the probability of error

$$P_{SB} = \Pr(\hat{U}^N \neq U^N). \tag{3.13}$$

By the Fano's inequality, we have

$$H(U^N|S^K = j, W = w, Z^N) \overset{(a)}{\leq} h(P_{SB}) + P_{SB}N[I(U;Z) - \epsilon_{UZ}],$$

where (a) follows from the fact that, in bin j, subbin w, the number of the possible sequences is at most $2^{N[I(U;Z)-\epsilon_{UZ}]}$. Hence,

$$H(U^N|S^K, W, Z^N) \leq h(P_{SB}) + P_{SB}N[I(U;Z) - \epsilon_{UZ}].$$

Thus we complete the proof of step 2.

Now we proceed to step 3. Note that given the codebook described in the proof of step 2,

- the decoder $g(\cdot)$ knows the indices of the bin and the subbin, i.e., j and w;
- the estimate $g(z^N)$ can be arbitrary.

Here we set $g(z^N)$ as u^N, the one in the codebook which is jointly typical with z^N, i.e., $(u^N, z^N) \in T^N_{U,Z}(\epsilon)$. When one of the following events occurs, an error is declared.

- $\mathcal{E}^{Z_1}(j,w)$: there is no sequence u^N in the codebook (i.e., subbin w in bin j) that is jointly typical with the received sequence z^N.
- $\mathcal{E}^{Z_2}(j,w)$: some other sequence in the codebook (i.e., subbin w in bin j) is jointly typical with the received sequence z^N.

Then, P_{SB} can be bounded as follows:

$$P_{SB} \leq \Pr\{\mathcal{E}^{Z_1}(j,w)\} + \Pr\{\mathcal{E}^{Z_2}(j,w)\}.$$

First we analyze the probability $\Pr\{\mathcal{E}^{Z_1}(j,w)\}$. For given ϵ and λ, there exists N_4 such that, when $N \geq N_4$, $\Pr\{(u^N, z^N) \in T^N_{U,Z}(\epsilon)\} \geq 1 - \lambda/2$, which implies $\Pr\{\mathcal{E}^{Z_1}(j,w)\} \leq \lambda/2$.

The probability $\Pr\{\mathcal{E}^{Z_2}(j,w)\}$. When there is other sequence u^N which is jointly typical with z^N, clearly such u^N is independent with z^N. Since there are only $2^{N[I(U;Z)-\epsilon_{UZ}]} - 1$ other sequences in the codebook, for given ϵ and λ, there exists ϵ_{UZ} and N_5, so that when

$\epsilon_{UZ} > 3\epsilon$, $N \geq N_5$, we have

$$\begin{aligned}
\Pr\{(u^N, z^N) \in T^N_{U,Z}(\epsilon)\} &\leq 2^{-N[I(U;Z)-3\epsilon]} \\
\Pr\{\mathcal{E}^{Z_2}(j,w)\} &< \sum_{u^N} 2^{-N[I(U;Z)-3\epsilon]} \\
&= 2^{N[I(U;Z)-\epsilon_{UZ}]} 2^{-N[I(U;Z)-3\epsilon]} \\
&= 2^{-N[\epsilon_{UZ}-3\epsilon]} \\
&\leq \lambda/2.
\end{aligned}$$

Thus, we have bounded P_{SB} for given ϵ and λ, when $\epsilon_{UZ} > 3\epsilon$ and $N > \max\{N_4, N_5\}$,

$$\begin{aligned}
P_{SB} &\leq \Pr\{\mathcal{E}^{Z_1}(j,w)\} + \Pr\{\mathcal{E}^{Z_2}(j,w)\} \\
&\leq \lambda/2 + \lambda/2 \\
&= \lambda.
\end{aligned}$$

This completes the proof of step 3 and consequently also the security $d \to 1$, as $N \to \infty$.

Now we have given an encoding-decoding scheme such that, when $N \geq \max\{N_1, N_2, N_3, N_4, N_5\}$,

$$\begin{aligned}
R &= R_{U1} - \epsilon_{UY} - \epsilon_{UVZ}, \\
P_e &\leq \delta, \\
d &\geq 1 - \frac{\epsilon_{UZ} - \epsilon_{UY} + h(\lambda)/N + \lambda[I(U;Z) - \epsilon_{UZ}]}{R_{U1} - \epsilon_{UY} - \epsilon_{UVZ}}.
\end{aligned} \tag{3.14}$$

Choosing $\epsilon, \epsilon_{UY}, \epsilon_{UVZ}, \epsilon_{UZ}, \delta$ and λ arbitrarily small and $\epsilon_{UY}, \epsilon_{UVZ}, \epsilon_{UZ} > 3\epsilon$, we have completed the proof that $(R_{U1}, 1)$ is achievable. In this case, although the wiretapper knows the decoding strategy used by the legitimate receiver, it can not help him since the equivocation goes to 1.

3.3.2 (R_{U2}, d_{U2}) is achievable

From (3.7), (3.8) and (3.9) it follows that if $I(U;V) \geq I(U;Z)$, then the rate equivocation pair (R_{U_2}, d_{U_2}) coincides with $(R_{U_1}, 1)$. So we only need to prove that, when $I(U;V) < I(U;Z)$, (R_{U_2}, d_{U_2}) is achievable. While if $I(U;V) < I(U;Z)$, then

$$R_{U_2} = I(U;Y) - I(U;V), \tag{3.15}$$

$$d_{U_2} = \frac{I(U;Y) - I(U;Z)}{I(U;Y) - I(U;V)}. \tag{3.16}$$

The encoding and decoding strategy is as follows:

1. *Codebook Generation*

   First, generate $2^{N[I(U;Y)-\epsilon_{UY}]}$ independent sequences u^N, according to the distribution $p_{U^N}(u^N) = \prod_{i=1}^N p_U(u_i)$. Next, distribute these sequences at random into 2^{NR} bins such that each bin contains $2^{N[I(U;V)+\epsilon_{UV}]}$ sequences. Here, $R = [R_{U2} - \epsilon_{UY} - \epsilon_{UV}]$. Index each bin by $j \in \{1, 2, \cdots, 2^{NR}\}$. Since $I(U;V) < I(U;Z)$, without loss of generality, we assume that $I(U;V) + \epsilon_{UV} \leq I(U;Z) - \epsilon_{UZ}$.

2. *Encoding*

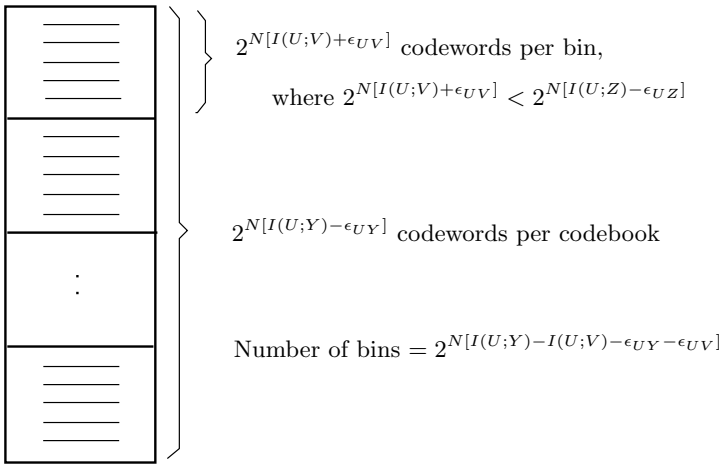


Figure 3.3: The codebook to achieve rate equivocation pair (R_{U2}, d_{U2}), when $I(U;V) < I(U;Z)$.

To send message j through an interference v^N, the sender looks in bin j for a sequence $u^N(j)$ such that $(u^N(j), v^N)$ is jointly typical, i.e., $(u^N(j), v^N) \in T^N_{U,V}(\epsilon)$., If there is no such $u^N(j)$ jointly typical with v^N, then the sender randomly chooses one sequence in bin j. Send the associated jointly typical $x^N(j)$. ($x^N(j)$ can be generated according to $p_{X^N|U^N,V^N}(x^N(j)|u^N(j), v^N) = \prod_{i=1}^N p_{X|U,V}(x_i|u_i, v_i)$.)

3. *Decoding*

   The legitimate receiver receives y^N according to the distribution $\prod_{i=1}^N p_{Y|X,V}(y_i|x_i, v_i)$. The receiver looks for the unique sequence u^N in the codebook that is jointly typical with the received sequence y^N, i.e., $(u^N, y^N) \in T^N_{U,Y}(\epsilon)$. Declare the index of the bin containing u^N as the message received.

4. *Wiretapper*

   The wiretapper knows the encoding scheme used at the transmitter and the decoding scheme used by the legitimate receiver. He receives a sequence z^N, according to the distribution $\prod_{i=1}^N p_{Y|X,V}(y_i|x_i, v_i)p_{Z|Y}(z_i|y_i)$.

For the legitimate receiver, there are three sources of potential error.

- $\mathcal{E}^V(j)$: in the encoding process, given v^N and message j, there is no sequence u^N in the bin j that is jointly typical with v^N.
- $\mathcal{E}^{Y_1}(j)$: in the decoding process, there is no sequence u^N that is jointly typical with the received sequence y^N.
- $\mathcal{E}^{Y_2}(j)$: in the decoding process, there is a sequence $u^N(j')$ in bin j', $j' \neq j$, jointly typical with the received sequence y^N.

The encoding and decoding strategy shown above is almost the same as the one to achieve the rate equivocation pair $(R_{U1}, 1)$. Only the codebook is different. In this codebook, the number of the sequences in every bin is less and thus there are more bins, which means that we can transmit more messages. So the rate $R_{U2} = I(U;Y) - I(U;V)$ is larger

than $R_{U1} = I(U;Y) - \max\{I(U;V), I(U;Z)\}$. However, R_{U2} is still not larger than the capacity of the main channel: $C_M = \max_{p_{U,X|V}(u,x|v)} [I(U;Y) - I(U;V)]$. By similar arguments as in [7, 10, 11], it is easy to show that the information rate R_{U2} is achievable.

Intuitively, a possible decoding strategy for the wiretapper would be to use the same strategy to decode as the legitimate receiver. He will try to find a sequence u^N in the codebook that is jointly typical with the received sequence z^N, and declare the index of the bin in which the sequence is found as the received message. We know that for any z^N, the probability that u^N is jointly typical with z^N is larger than $(1-\epsilon)2^{-N[I(U;Z)+3\epsilon]}$. In the codebook, there are $2^{N[I(U;Y)-\epsilon_{UY}]}$ sequences uniformly distributed. Thus, with high probability the wiretapper will find approximately $2^{N[I(U;Y)-I(U;Z)-\epsilon_{UY}-3\epsilon]}$ sequences that are jointly typical with z^N. These sequences are also uniformly distributed in the codebook. However, there are $2^{N[I(U;Y)-I(U;V)-\epsilon_{UY}-\epsilon_{UV}]}$ bins in the codebook. Since $I(U;V) < I(U;Z)$, choosing appropriate ϵ, ϵ_{UY}, ϵ_{UV}, for example, $\epsilon < \frac{I(U;Z)-I(U;V)}{10}$, $\epsilon_{UY}, \epsilon_{UV} = 4\epsilon$, we can have a codebook such that

$$2^{N[I(U;Y)-I(U;V)-\epsilon_{UY}-\epsilon_{UV}]} \geq 2^{N[I(U;Y)-I(U;Z)-\epsilon_{UY}-3\epsilon]}.$$

So, in every bin there is at most one sequence that is jointly typical with z^N. That is, there are $2^{N[I(U;Y)-I(U;Z)-\epsilon_{UY}-3\epsilon]}$ bins that have such a sequence that is jointly typical with z^N. Hence, for the wiretapper, the number of possible messages is about $2^{N[I(U;Y)-I(U;Z)-\epsilon_{UY}-3\epsilon]}$. The probability that he decodes the correct message goes to $2^{-N[I(U;Y)-I(U;Z)]}$ as N approaches ∞. Therefore, we have $p_{S^K|Z^N}(s^K|z^N) \to 2^{-N[I(U;Y)-I(U;Z)]}$ and $H(S^K|Z^N) \to N[I(U;Y) - I(U;Z)]$. Since $H(S^K) \to N[I(U;Y) - I(U;V)]$, the normalized equivocation d_{U2} goes to $\frac{I(U;Y)-I(U;Z)}{I(U;Y)-I(U;V)}$ as N approaches ∞. So, we reach more rate for the legitimate receiver, but less equivocation for the wiretapper. The perfect security can not be guaranteed.

In the following we will prove that when $I(U;V) < I(U;Z)$, (R_{U2}, d_{U2}) is achievable in two parts, the reliability: $P_e \to 0$, as $N \to \infty$, and the security: $d_{U2} \to \frac{I(U;Y)-I(U;Z)}{I(U;Y)-I(U;V)}$, as $N \to \infty$.

Proof of $P_e \to 0$.

We first analyze the probability of $\mathcal{E}^V(j)$. By the code generating process, u^N and v^N are independent. The probability that a pair (u^N, v^N) is jointly typical is greater than $(1-\epsilon)2^{-N[I(U;V)+3\epsilon]}$ for N sufficiently large. So we have

$$\begin{aligned}
\Pr\{(u^N, v^N) \in T^N_{U,V}(\epsilon)\} &\geq (1-\epsilon)2^{-N[I(U;V)+3\epsilon]} \\
\Pr\{(u^N, v^N) \notin T^N_{U,V}(\epsilon)\} &\leq 1 - (1-\epsilon)2^{-N[I(U;V)+3\epsilon]} \\
\Pr\{\mathcal{E}^V(j)|S^K = j\} &\overset{(a)}{\leq} [1 - (1-\epsilon)2^{-N[I(U;V)+3\epsilon]}]^{2^{N[I(U;V)+\epsilon_{UV}]}} \\
&\overset{(b)}{\leq} \exp\{-(1-\epsilon)2^{-N[I(U;V)+3\epsilon]}\}^{2^{N[I(U;V)+\epsilon_{UV}]}} \\
&= \exp\{-(1-\epsilon)2^{N[I(U;V)-I(U;V)+\epsilon_{UV}-3\epsilon]}\} \\
&= \exp\{-(1-\epsilon)2^{N[\epsilon_{UV}-3\epsilon]}\} \\
&\leq \delta/3,
\end{aligned}$$

where

(a) follows from the fact that there are $2^{N[I(U;V)+\epsilon_{UV}]}$ codewords in a bin;

(b) follows from the inequality $e^a \geq 1 + a$.

As shown above, for given ϵ and arbitrary small δ, there exists ϵ_{UV} and N_1 such that when $\epsilon_{UV} > 3\epsilon$, $N \geq N_1$, both $\Pr\{(u^N, v^N) \in T^N_{U,V}(\epsilon)\} \geq (1-\epsilon)2^{-N[I(U;V)+3\epsilon]}$ and $\Pr\{\mathcal{E}^V(j)|S^K = j\} \leq \delta/3$ are satisfied.

The probability of $\mathcal{E}^{Y_1}(j)$. If the event $\mathcal{E}^V(j)$ does not occur, which means that there is a sequence $u^N(j)$ in bin j and a sequence sent $x^N(j)$ such that $(u^N(j), x^N(j), v^N) \in T^N_{U,V}(\epsilon)$ is jointly typical, then $(u^N(j), x^N(j), v^N, y^N)$ will be jointly typical with high probability. For given ϵ and arbitrary small δ, there exists N_2 such that when $N \geq N_2$,

$$\Pr\{(u^N, y^N) \in T^N_{U,Y}(\epsilon)\} \geq 1 - \delta/3,$$

which implies that

$$\Pr\{\mathcal{E}^{Y_1}(j)|\mathcal{E}^V(j)^C, S^K = j\} \leq \delta/3.$$

The third source of potential error. If we say that $\mathcal{E}^{Y_2^*}(j)$ occurs when some other u^N is jointly typical with y^N, then it is clear that

$$\Pr\{\mathcal{E}^{Y_2}(j)|\mathcal{E}^V(j)^C, S^K = j\} \leq \Pr\{\mathcal{E}^{Y_2^*}(j)|\mathcal{E}^V(j)^C, S^K = j\}.$$

But a sequence u^N, different from $u^N(j)$, being jointly typical with y^N has probability at most $2^{-N[I(U;Y)-3\epsilon]}$. Since there are only $2^{N[I(U;Y)-\epsilon_{UY}]} - 1$ other u^N sequences, for given ϵ and arbitrary small δ, there exists ϵ_{UY} and N_3 such that when $\epsilon_{UY} > 3\epsilon$, $N \geq N_3$, we have

$$\begin{aligned}
\Pr\{\mathcal{E}^{Y_2}(j)|\mathcal{E}^V(j)^C, S^K = j\} &\leq \Pr\{\mathcal{E}^{Y_2^*}(j)|\mathcal{E}^V(j)^C, S^K = j\} \\
&\leq \sum_{u^N \neq u^N(j)} 2^{-N[I(U;Y)-3\epsilon]} \\
&\leq (2^{N[I(U;Y)-\epsilon_{UY}]} - 1)2^{-N[I(U;Y)-3\epsilon]} \\
&< 2^{N[I(U;Y)-\epsilon_{UY}]-N[I(U;Y)-3\epsilon]} \\
&= 2^{-N[\epsilon_{UY}-3\epsilon]} \\
&\leq \delta/3.
\end{aligned}$$

This shows all three error events are of arbitrarily small probability. By the union bound on these three probabilities of error, for $\epsilon_{UY}, \epsilon_{UV} > 3\epsilon$ and $N \geq \max\{N_1, N_2, N_3\}$, the average probability of error

$$\begin{aligned}
P_e &= \frac{1}{2^{nR}} \sum_{j=1}^{2^{nR}} \Pr(\hat{S}^K(Y^N) \neq j|S^K = j) \\
&\leq \frac{1}{2^{nR}} \sum_{j=1}^{2^{nR}} [\Pr\{\mathcal{E}^V(j)|S^K = j\} + \Pr\{\mathcal{E}^{Y_1}(j)|\mathcal{E}^V(j)^C, S^K = j\} \\
&\quad + \Pr\{\mathcal{E}^{Y_2}(j)|\mathcal{E}^V(j)^C, S^K = j\}] \\
&\leq \frac{1}{2^{nR}} \sum_{j=1}^{2^{nR}} [\delta/3 + \delta/3 + \delta/3] \\
&= \delta.
\end{aligned}$$

This concludes the proof that the rate R_{U2} is achievable.

Proof of $d_{U2} \to \frac{I(U;Y)-I(U;Z)}{I(U;Y)-I(U;V)}$.
Consider the uncertainty of the message to the wiretapper in three steps:

1. show that
$$H(S^K|Z^N) \geq N[I(U;Y) - I(U;Z)] - H(U^N|S^K, Z^N).$$

2. show that
$$H(U^N|S^K, Z^N) \leq h(P_B) + P_B N[I(U;V) + \epsilon_{UV}].$$
Here P_B means a wiretapper's error probability in the case where the bin number is known to the wiretapper.

3. show that for arbitrary $0 < \lambda < 1/2$, $P_B \leq \lambda$.

Combining the above steps, we have

$$\begin{aligned} d &= \frac{H(S^K|Z^N)}{H(S^K)} \\ &\geq \frac{N[I(U;Y) - I(U;Z)] - H(U^N|S^K, Z^N)}{NR} \\ &\geq \frac{NR_{U2}d_{U2} - h(P_B) - P_B N[I(U;V) + \epsilon_{UV}]}{NR} \\ &\geq \frac{NR_{U2}d_{U2} - h(\lambda) - \lambda N[I(U;V) + \epsilon_{UV}]}{NR} \\ &= \frac{R_{U2}}{R_{U2} - \epsilon_{UY} - \epsilon_{UV}} d_{U2} - \frac{h(\lambda)/N + \lambda[I(U;V) + \epsilon_{UV}]}{R_{U2} - \epsilon_{UY} - \epsilon_{UV}}. \end{aligned}$$

We now proceed to step 1 by considering

$$\begin{aligned} H(S^K|Z^N) &= H(S^K, Z^N) - H(Z^N) \\ &= H(S^K, U^N, Z^N) - H(U^N|S^K, Z^N) - H(Z^N) \\ &= H(S^K|U^N, Z^N) + H(U^N, Z^N) \\ &\quad -H(U^N|S^K, Z^N) - H(Z^N) \\ &\overset{(a)}{\geq} H(U^N, Z^N) - H(U^N|S^K, Z^N) - H(Z^N) \\ &= H(U^N|Z^N) - H(U^N|S^K, Z^N) \\ &\overset{(b)}{\geq} H(U^N|Z^N) - H(U^N|Y^N) - H(U^N|S^K, Z^N) \\ &= I(U^N;Y^N) - I(U^N;Z^N) - H(U^N|S^K, Z^N) \\ &\overset{(c)}{=} N[I(U;Y) - I(U;Z)] - H(U^N|S^K, Z^N), \end{aligned}$$

where
(a) follows from the fact that $H(S^K|U^N, Z^N) \geq 0$;
(b) follows from the fact that $H(U^N|Y^N) \geq 0$;
(c) follows from the fact that $I(U^N;Y^N) = NI(U;Y)$ and $I(U^N;Z^N) = NI(U;Z)$.
Thus the proof of step 1 is completed.

To prove step 2, we need to bound the entropy of the codeword conditioned on the bin j and the wiretapper's observation z^N. We take the bin j as a codebook, U^N in the codebook as the input messages, Z^N as the result of passing U^N through the discrete memoryless

channel. From Z^N, we estimate the message U^N that was sent. Let $g(\cdot)$ be the decoder and the estimate be $\hat{U}^N = g(Z^N)$. Define the probability of error

$$P_B = \Pr(\hat{U}^N \neq U^N). \tag{3.17}$$

By the Fano's inequality, we have

$$H(U^N|S^K = j, Z^N) \overset{(a)}{\leq} h(P_B) + P_B N[I(U;V) + \epsilon_{UV}],$$

where (a) follows from the fact that, in bin j, the number of the possible sequences is at most $2^{N[I(U;V)+\epsilon_{UV}]}$. Hence

$$H(U^N|S^K, Z^N) \leq h(P_B) + P_B N[I(U;V) + \epsilon_{UV}].$$

Thus we complete the proof of step 2.

Now we proceed to step 3.Note that given the codebook described in the proof of step 2,

- the decoder $g(\cdot)$ knows the index of the bin, i.e., j;
- the estimate $g(z^N)$ can be arbitrary.

Here we set $g(z^N)$ as u^N, the one in the codebook which is jointly typical with z^N, i.e., $(u^N, z^N) \in T^N_{U,Z}(\epsilon)$. This decoding strategy is good enough to bound P_B. When one of the following events occurs, an error is declared.

- $\mathcal{E}^{Z_1}(j)$: there is no sequence u^N in the codebook (i.e., bin j) that is jointly typical with the received sequence z^N.
- $\mathcal{E}^{Z_2}(j)$: in the codebook (i.e., bin j) some other sequence is jointly typical with the received sequence z^N.

Then, P_B can be bounded as follows:

$$P_B \quad \leq \quad \Pr\{\mathcal{E}^{Z_1}(j)\} + \Pr\{\mathcal{E}^{Z_2}(j)\}.$$

First we analyze the probability $\Pr\{\mathcal{E}^{Z_1}(j)\}$. For given ϵ and λ, there exists N_4 such that, when $N \geq N_4$, $\Pr\{(u^N, z^N) \in T^N_{U,Z}(\epsilon)\} \geq 1 - \lambda/2$, which implies $\Pr\{\mathcal{E}^{Z_1}(j)\} \leq \lambda/2$.

The probability $\Pr\{\mathcal{E}^{Z_2}(j)\}$. When there is other sequence u^N which is jointly typical with z^N, it is easy to see that such u^N is independent with z^N. Since there are at most $2^{N[I(U;V)+\epsilon_{UV}]} - 1$ other sequences u^N in the codebook, and $2^{N[I(U;V)+\epsilon_{UV}]} \leq 2^{N[I(U;Z)-\epsilon_{UZ}]}$, for given ϵ and λ, there exists ϵ_{UZ} and N_5, so that when $\epsilon_{UZ} > 3\epsilon$, $N \geq N_5$, we have

$$\begin{aligned}
\Pr\{(u^N, z^N) \in T^N_{U,Z}(\epsilon)\} &\leq 2^{-N[I(U;Z)-3\epsilon]} \\
\Pr\{\mathcal{E}^{Z_2}(j)\} &< \sum_{u^N} 2^{-N[I(U;Z)-3\epsilon]} \\
&< 2^{N[I(U;V)+\epsilon_{UV}]} 2^{-N[I(U;Z)-3\epsilon]} \\
&\leq 2^{N[I(U;Z)-\epsilon_{UZ}]} 2^{-N[I(U;Z)-3\epsilon]} \\
&= 2^{-N[\epsilon_{UZ}-3\epsilon]} \\
&\leq \lambda/2.
\end{aligned}$$

Thus, we have bounded P_B for given ϵ and λ, when $\epsilon_{UZ} > 3\epsilon$ and $N > \max\{N_4, N_5\}$,

$$\begin{aligned} P_B &\leq \Pr\{\mathcal{E}^{Z_1}(j)\} + \Pr\{\mathcal{E}^{Z_2}(j)\} \\ &\leq \lambda/2 + \lambda/2 \\ &= \lambda. \end{aligned}$$

This completes the proof of step 3.

Now we have proved that when $I(U;V) + \epsilon_{UV} \leq I(U;Z) - \epsilon_{UZ}$, there is an encoding-decoding scheme such that, when $N \geq \max\{N_1, N_2, N_3, N_4, N_5\}$,

$$\begin{aligned} R &= R_{U2} - \epsilon_{UY} - \epsilon_{UV}, \\ P_e &\leq \delta, \\ d &\geq \frac{R_{U2}}{R_{U2} - \epsilon_{UY} - \epsilon_{UV}} d_{U2} - \frac{h(\lambda)/N + \lambda[I(U;V) + \epsilon_{UV}]}{R_{U2} - \epsilon_{UY} - \epsilon_{UV}}. \end{aligned} \tag{3.18}$$

We choose $\epsilon, \epsilon_{UY}, \epsilon_{UV}, \epsilon_{UZ}, \delta$ and λ arbitrarily small, such that $\epsilon_{UY}, \epsilon_{UV}, \epsilon_{UZ} > 3\epsilon$ and $\epsilon_{UV} + \epsilon_{UZ} < I(U;Z) - I(U;V)$. From this it follows that (R_{U2}, d_{U2}) is achievable.

Note that when ϵ_{UV} and ϵ_{UZ} approach zero, then the condition $I(U;V) + \epsilon_{UV} \leq I(U;Z) - \epsilon_{UZ}$ can be written as $I(U;V) < I(U;Z)$. Therefore, when $I(U;V) < I(U;Z)$, (R_{U2}, d_{U2}) is achievable.

3.4 Discussion

In section 3.3, we have proved the achievability of the region $\mathcal{R}$. In this section, we are interested in the secrecy capacity of the wiretap channel we investigated.

Let

$$R_{Ws} = \max_{U \to (X,V) \to Y \to Z} [I(U;Y) - I(U;Z)\}]. \tag{3.19}$$

We have the following theorem.

Theorem 3.4.1 *For the discrete memoryless wiretap channel with side information,*

$$R_s \leq C_s \leq \min\{C_M, R_{Ws}\},$$

where C_M is the capacity of the main channel.

We give the following two corollaries, which may be useful for the calculation of secrecy capacities of some particular wiretap channels with side information. Besides, their proofs also establish the proof of Theorem 3.4.1.

Corollary 3.4.2 *For the discrete memoryless wiretap channel with side information, if there is an auxiliary parameter U_M such that*

1. *$U_M \to (X,V) \to Y \to Z$ forms a Markov chain;*
2. *$I(U_M;Y) - I(U_M;V) = C_M$;*
3. *$I(U_M;V) \geq I(U_M;Z)$,*

then the secrecy capacity C_s is equal to C_M.

Corollary 3.4.3 *For the discrete memoryless wiretap channel with side information, if there is an auxiliary parameter U_W such that*

1. *$U_W \to (X, V) \to Y \to Z$ forms a Markov chain;*
2. *$I(U_W; Y) - I(U_W; Z) = R_{Ws}$;*
3. *$I(U_W; Z) \geq I(U_W; V)$,*

then the secrecy capacity C_s is equal to R_{Ws}.

Proof: We know from the definitions of R_s and R_{Ws}, $R_s \leq R_{Ws}$. And, since $I(U_W; Z) \geq I(U_W; V)$ and U_W maximizes $I(U; Y) - I(U; Z)$, it follows that

$$\begin{aligned} R_{Ws} &= I(U_W; Y) - I(U_W; Z) \\ &= I(U_W; Y) - \max\{I(U_W; V), I(U_W; Z)\} \\ &\leq R_s. \end{aligned}$$

Thus, we have $R_s = R_{Ws}$.

Furthermore, it is known that $C_s \geq R_s = R_{Ws}$. Now we only need to prove that $C_s \leq R_{Ws}$.

First, by the data processing theorem and Fano's inequality,

$$H(S^K|Y^N, Z^N) \leq H(S^K|Y^N) \leq H(S^K|\hat{S}^K) \leq h(P_e) + NRP_e.$$

Then, using the definitions (3.4) and (3.5), we obtain

$$\begin{aligned} NRd &= H(S^K|Z^N) \\ &\leq H(S^K|Z^N) - H(S^K|Y^N, Z^N) + h(P_e) + NRP_e \\ &= I(S^K; Y^N|Z^N) + h(P_e) + NRP_e \\ &\overset{(a)}{\leq} \sum_{i=1}^{N} I(S^K; Y_i|Y_1^{i-1}, Z^N) + h(P_e) + NRP_e \\ &\overset{(b)}{=} \sum_{i=1}^{N} I(S^K; Y_i|Y_1^{i-1}, Z^N, V_1^{i-1}, V_{i+1}^N) + h(P_e) + NRP_e \\ &\overset{(c)}{\leq} \sum_{i=1}^{N} I(U_i; Y_i|Z_i) + h(P_e) + NRP_e \\ &\overset{(d)}{=} \sum_{i=1}^{N} [I(U_i; Y_i) - I(U_i; Z_i)] + h(P_e) + NRP_e, \end{aligned}$$

where

(a) follows from the fact of chain rule for information;

(b) follows from the fact that V^N is independent of S^K;

(c) follows from the assumption that
$U_i = (S^K, Y_1^{i-1}, Z_1^{i-1}, Z_{i+1}^N, V_1^{i-1}, V_{i+1}^N)$;

(d) follows from the fact that $(U_i, V_i) \to Y_i \to Z_i$ forms a Markov chain.

Now choosing i^* to be the index i such that

$$I(U_{i^*}; Y_{i^*}) - I(U_{i^*}; Z_{i^*}) = \max_{1 \le j \le N} [I(U_j; Y_j) - I(U_j; Z_j)],$$

we have

$$\begin{aligned} Rd &\le I(U_{i^*}; Y_{i^*}) - I(U_{i^*}; Z_{i^*}) + \frac{h(P_e)}{N} + RP_e \\ &\le R_{Ws} + \frac{h(P_e)}{N} + RP_e. \end{aligned}$$

C_s is the maximum value of R when d approaches to 1, so we have

$$C_s \le R_{Ws} + \frac{h(P_e)}{N} + RP_e.$$

Thus $C_s \le R_{Ws}$ has been proved. This also completes the proof of this corollary. ■

3.5 Concluding remarks

In this chapter, we give an achievable rate equivocation region for the discrete memoryless wiretap channel with side information. Furthermore, the secrecy capacities in some special cases are also determined. However, it is still an open problem whether R_s completely characterizes the achievable rate equivocation region of the discrete memoryless wiretap channel with side information.

It should be pointed out that our restriction to finite alphabets is just a matter of convenience. Theorem 3.2.1 here can be readily extended to memoryless channels with discrete time and continuous alphabets by the standard technique of discrete approximations [18, Ch. 7]. It is very interesting that the situation described in Corollary 3.4.2 happens in the Gaussian case. Such an example is given in [8, Theorem 4.2].

Chapter 4

Gaussian Wiretap Channel with Side Information

4.1 Introduction

In Chapter 3, we give a coding theorem for the discrete memoryless wiretap channel with side information. In this chapter, we focus on the Gaussian wiretap channel with side information as shown in Figure 1.7. Recall that Costa [7] has shown that the Gaussian channel with side information, also called dirty paper channel, has the same capacity as the corresponding standard Gaussian channel. Therefore, the side information does not affect the capacity of the channel. Here we wonder, how does side information influence the secrecy capacity of the wiretap channel? Especially in the Gaussian case, can we get a similar result as for the dirty paper channel?

On the other hand, Costa has shown that for the dirty paper channel, by choosing codewords orthogonal to the side information, the channel capacity could be reached by dirty paper coding. That is, one prefers to send codewords independent of the side information in order to yield the optimal transmission rate. Note that the coding strategy used for the wiretap channel with side information is similar to the one used for the dirty paper channel. However, we wonder whether it might be a better choice to send codewords dependent on the side information in some cases, in order to yield higher rate with the same equivocation.

The rest of the chapter is organized as follows. In section 4.2, we derive an achievable region for the Gaussian wiretap channel with side information. In section 4.3, we generalize Costa's strategy and show a general result for the dirty paper channel. In section 4.4, for the Gaussian wiretap channel with side information, an extended rate equivocation region is derived by applying the generalized Costa's strategy.

4.2 An achievable rate equivocation

In this section, we extend Theorem 3.2.1 to the Gaussian case and derive an achievable region for the Gaussian wiretap channel with side information. Furthermore, we compare the performance of the region with the capacity region of the Gaussian wiretap channel given by Leung-Yan-Cheong and Hellman [4, Theorem 1] and show how side information influences the secrecy capacity and the rate equivocation region.

As we have discussed in Remark (b) after the statement of Theorem 3.2.1, the technique we use to establish the region $\mathcal{R}$ is more general compared with the one used by Mitrpant

[8,9] for the Gaussian wiretap channel with side information. Here we make use of the same auxiliary random variable U as Mitrpant in [8,9], which is similar to Costa [7]. Applying our technique given in Section 3.3, we provide a straightforward proof to extend Theorem 3.2.1 to the Gaussian case as follows.

Theorem 4.2.1 *Consider the Gaussian wiretap channel with side information as shown in Figure 1.7. We make use of the auxiliary random variable $U = X + \alpha V$, where α is a real number and X is independent of V. Denote $\mathcal{R}_U$ as the set of points (R, d) with*

$$R_{U1} \leq R \leq R_{U2}, \quad 0 \leq d \leq 1, \quad Rd = R_{U1},$$

where R_{U1} and R_{U2} are defined in (3.7) and (3.8). Let

$$\mathcal{R}'_U \stackrel{\Delta}{=} \{(R', d') : 0 \leq R' \leq R, 0 \leq d' \leq d, (R, d) \in \mathcal{R}_U\}.$$

Then the set $\mathcal{R}_\perp$, defined as follows, is achievable:

$$\mathcal{R}_\perp = \bigcup_{U=X+\alpha V, \alpha \in \mathbb{R}} \mathcal{R}'_U,$$

where $\mathbb{R}$ represents the set of all real numbers.

Proof: The proof is almost the same as the proof of Theorem 3.2.1 given in section 3.3. We only need to show that $\mathcal{R}_U$ is achievable for the specified α and U. Assume that the channel has power constraint P and the side information satisfies $V \sim \mathcal{N}(0, Q)$. For a fixed ϵ, let $P' = P(1 + 4\epsilon)^{-1}$. Due to the Gaussian characteristic of the channel, we make slight modifications in the achievability proof of $\mathcal{R}_U$ as follows:

- In the codebook generation, sequences u^N are generated according to $f(u^N) = \prod_{i=1}^N f(u_i)$. Here we specify $f(u_i) \sim \mathcal{N}(0, P' + \alpha^2 Q)$ for all $i \in \{1, 2, \cdots, N\}$.
- In the encoding process, $x^N(j) = u^N(j) - \alpha v^N$.
- The legitimate receiver observes $y^N = x^N(j) + v^N + \eta_1^N$ and the wiretapper observes $z^N = y^N + \eta_2^N$.

As a consequence of these modifications, there is one more source of potential error for the legitimate receiver.

- $\mathcal{E}^X(j)$: in the encoding process, $x^N(j) = u^N(j) - \alpha v^N$ does not satisfy the power constraint.

However, provided that there is at least one sequence $u^N(j)$ jointly typical with v^N, the probability that $\mathcal{E}^X(j)$ occurs is 0 according to Lemma 2.2.7 or [9, Lemma A.1]. Therefore, the modifications do not influence the achievability proof of $\mathcal{R}_U$. Let ϵ be arbitrarily small. Since $P' \to P$ as $\epsilon \to 0$, we have shown that R_U is asymptotically achievable for $\alpha \in \mathbb{R}$ and $U = X + \alpha V$, where X is independent of V and $X \sim \mathcal{N}(0, P)$. Thus we conclude our proof. ■

As a direct consequence of the technique improvement, our region $\mathcal{R}_\perp$ is better than the one given by Mitrpant in [8, Theorem 4.4] or [9, Theorem 3]. You can find the comparison in Subsection 4.2.4.

4.2.1 Model description

As depicted in Figure 1.7, the Gaussian wiretap channel with side information is extended from the Gaussian wiretap channel by adding an interference (i.e., side information) in the main channel. Assume that the interference is independent of the channel noise and the message. Further assume that the interference is noncausally known to the transmitter. Let X be the input to the main channel. Then the output of the main channel is $Y = X + V + \eta_1$ and the output of the wiretap channel is $Z = Y + V + \eta_2$, where $\eta_1 \sim \mathcal{N}(0, N_1)$ and $\eta_2 \sim \mathcal{N}(0, N_2)$ are independent noises of the main channel and the wiretap channel, respectively.

We note that the main channel of the Gaussian wiretap channel with side information is a dirty paper channel as investigated in [7]. Simlarly to Costa [7], we consider $U = X + \alpha V$, where X and V are independent random variables distributed according to $\mathcal{N}(0, P)$ and $\mathcal{N}(0, Q)$, respectively, and α is a parameter to be determined. Note that there could be a loss of generality in restricting attention to such U, but we shall see that the derived answer is clearly optimal in some special cases. For convenience, we use the following notations:

$$\begin{aligned} U_* &= X + *V, && (4.1)\\ R_s(*) &= I(U_*;Y) - \max\{I(U_*;V), I(U_*;Z)\}, && (4.2)\\ R(*) &= I(U_*;Y) - I(U_*;V), && (4.3)\\ R_Z(*) &= I(U_*;Y) - I(U_*;Z), && (4.4)\\ d(*) &= R_s(*)/R(*). && (4.5) \end{aligned}$$

First, we calculate the values of $I(U,V)$, $I(U,Y)$ and $I(U,Z)$ with respect to $U = X + \alpha V$. Note that here X is independent of V. We have the following:

$$\begin{aligned} I(U;V) &= I(X+\alpha V; V)\\ &= H(X+\alpha V) + H(V) - H(X+\alpha V, V)\\ &= \frac{1}{2}\log\frac{(P+\alpha^2 Q)Q}{(P+\alpha^2 Q)Q - \alpha^2 Q^2}\\ &= \frac{1}{2}\log\frac{(P+\alpha^2 Q)}{P}; \end{aligned}$$

$$\begin{aligned} I(U;Y) &= I(X+\alpha V; X+V+\eta_1)\\ &= H(X+\alpha V) + H(X+V+\eta_1) - H(X+\alpha V, X+V+\eta_1)\\ &= \frac{1}{2}\log\frac{(P+\alpha^2 Q)(P+Q+N_1)}{((P+\alpha^2 Q)(P+Q+N_1) - (P+\alpha Q)^2}\\ &= \frac{1}{2}\log\frac{(P+\alpha^2 Q)(P+Q+N_1)}{PQ(1-\alpha)^2 + (P+\alpha^2 Q)N_1}; \end{aligned}$$

$$\begin{aligned} I(U;Z) &= I(X+\alpha V; X+V+\eta_1+\eta_2)\\ &= H(X+\alpha V) + H(X+V+\eta_1+\eta_2) - H(X+\alpha V, X+V+\eta_1+\eta_2)\\ &= \frac{1}{2}\log\frac{(P+\alpha^2 Q)(P+Q+N_1+N_2)}{((P+\alpha^2 Q)(P+Q+N_1+N_2) - (P+\alpha Q)^2}\\ &= \frac{1}{2}\log\frac{(P+\alpha^2 Q)(P+Q+N_1+N_2)}{PQ(1-\alpha)^2 + (P+\alpha^2 Q)(N_1+N_2)}. \end{aligned}$$

It is a straightforward consequence that

$$I(U;Y) - I(U;V) = \frac{1}{2}\log\frac{P(P+Q+N_1)}{(1-\alpha)^2PQ + N_1(P+\alpha^2Q)}; \tag{4.6}$$

$$I(U;Z) - I(U;V) = \frac{1}{2}\log\frac{P(P+Q+N_1+N_2)}{(1-\alpha)^2PQ + (N_1+N_2)(P+\alpha^2Q)}; \tag{4.7}$$

$$I(U;Y) - I(U;Z) = \frac{1}{2}\log\frac{(P+Q+N_1)\{(1-\alpha)^2PQ + (N_1+N_2)(P+\alpha^2Q)\}}{(P+Q+N_1+N_2)\{(1-\alpha)^2PQ + N_1(P+\alpha^2Q)\}} \tag{4.8}$$

Note that Z is a degraded version of Y. Thus, we have $I(U;Y) \geq I(U;Z)$. You can also find a proof of it in Appendix III. So we distinguish the following three cases:

(1) $I(U;V) > I(U;Y) > I(U;Z)$;

(2) $I(U;Y) \geq I(U;V) \geq I(U;Z)$;

(3) $I(U;Y) \geq I(U;Z) > I(U;V)$.

Case 1: $I(U;V) > I(U;Y) > I(U;Z)$

Consider the inequality $I(U;V) > I(U;Y)$.

$$\begin{aligned}
I(U;V) &> I(U;Y) \\
\frac{1}{2}\log\frac{P+\alpha^2Q}{P} &> \frac{1}{2}\log\frac{(P+\alpha^2Q)(P+Q+N_1)}{PQ(1-\alpha)^2 + (P+\alpha^2Q)N_1} \\
\frac{P+\alpha^2Q}{P} &> \frac{(P+\alpha^2Q)(P+Q+N_1)}{PQ(1-\alpha)^2 + (P+\alpha^2Q)N_1} \\
\frac{1}{P} &> \frac{P+Q+N_1}{PQ(1-\alpha)^2 + (P+\alpha^2Q)N_1} \\
PQ(1-\alpha)^2 + (P+\alpha^2Q)N_1 &> P(P+Q+N_1) \\
\alpha^2Q(P+N_1) - 2\alpha PQ &> P^2 \\
Q(P+N_1)(\alpha^2 - \frac{2\alpha P}{P+N_1} + (\frac{P}{P+N_1})^2) &> P^2 + \frac{P^2Q}{P+N_1} \\
(\alpha - \frac{P}{P+N_1})^2 &> \frac{P^2(P+Q+N_1)}{Q(P+N_1)^2}.
\end{aligned}$$

Therefore, under the assumption that $P, Q, N_1, N_2 > 0$, we have

$$I(U;V) > I(U;Y) \iff \alpha > \alpha_{00} \quad \text{or} \quad \alpha < \alpha_{-00},; \tag{4.9}$$

$$I(U;Y) \geq I(U;V) \iff \alpha_{-00} \leq \alpha \leq \alpha_{00}, \tag{4.10}$$

where

$$\alpha_{00} = \frac{P}{P+N_1}(1 + \sqrt{\frac{P+Q+N_1}{Q}}); \tag{4.11}$$

$$\alpha_{-00} = \frac{P}{P+N_1}(1 - \sqrt{\frac{P+Q+N_1}{Q}}). \tag{4.12}$$

By Theorem 4.2.1, the rate equivocation pair $(I(U;Y) - \max(I(U;V), I(U;Z)), 1)$ is achievable. If $I(U;V) > I(U;Y) > I(U;Z)$, then the information rate from transmitter to the receiver, $I(U;Y) - I(U;V)$, will be smaller than 0. For practical reasons, we only need to consider Case 2 and Case 3 when $\alpha_{-00} \leq \alpha \leq \alpha_{00}$.

Case 2: $I(U;Y) \geq I(U;V) \geq I(U;Z)$

As shown in (4.10), when $\alpha_{-00} \leq \alpha \leq \alpha_{00}$, $I(U;Y) \geq I(U;V)$. Now let us consider the inequality $I(U;V) \geq I(U;Z)$.

$$\begin{aligned}
I(U;V) &\geq I(U;Z) \\
\frac{1}{2}\log\frac{P+\alpha^2 Q}{P} &\geq \frac{1}{2}\log\frac{(P+\alpha^2Q)(P+Q+N_1+N_2)}{PQ(1-\alpha)^2+(P+\alpha^2Q)(N_1+N_2)} \\
\frac{P+\alpha^2Q}{P} &> \frac{(P+\alpha^2Q)(P+Q+N_1+N_2)}{PQ(1-\alpha)^2+(P+\alpha^2Q)(N_1+N_2)} \\
\frac{1}{P} &> \frac{P+Q+N_1+N_2}{PQ(1-\alpha)^2+(P+\alpha^2Q)(N_1+N_2)} \\
PQ(1-\alpha)^2+(P+\alpha^2Q)N_1 &> P(P+Q+N_1+N_2) \\
\alpha^2Q(P+N_1+N_2)-2\alpha PQ &> P^2 \\
(\alpha^2-\frac{2\alpha P}{P+N_1+N_2}+(\frac{P}{P+N_1+N_2})^2) &> \frac{1}{Q(P+N_1+N_2)}(P^2+\frac{P^2Q}{P+N_1+N_2}) \\
(\alpha-\frac{P}{P+N_1+N_2})^2 &> \frac{P^2(P+Q+N_1+N_2)}{Q(P+N_1+N_2)^2}.
\end{aligned}$$

Therefore, we have

$$I(U;V) \geq I(U;Z) \iff \alpha \geq \alpha_0 \quad \text{or} \quad \alpha \leq \alpha_{-0}; \tag{4.13}$$

$$I(U;Z) > I(U;V) \iff \alpha_{-0} < \alpha < \alpha_0, \tag{4.14}$$

where

$$\alpha_0 = \frac{P}{P+N_1+N_2}(1+\sqrt{\frac{P+Q+N_1+N_2}{Q}}); \tag{4.15}$$

$$\alpha_{-0} = \frac{P}{P+N_1+N_2}(1-\sqrt{\frac{P+Q+N_1+N_2}{Q}}). \tag{4.16}$$

In particular, when $I(U;V) = I(U;Z)$,

$$I(U;Y) - I(U;V) = I(U;Y) - I(U;Z) \iff \alpha = \alpha_0 \text{ or } \alpha_{-0}.$$

So we have

$$R(\alpha_0) = R_Z(\alpha_0); \tag{4.17}$$

$$R(\alpha_{-0}) = R_Z(\alpha_{-0}). \tag{4.18}$$

In Case 2, $I(U;Y) - \max(I(U;V), I(U;Z)) = I(U;Y) - I(U;V)$. By Theorem 4.2.1, the rate equivocation pair $(I(U;Y) - I(U;V), 1)$ is achievable. Therefore, we have the following lemma.

Lemma 4.2.2 *For any α such that $\alpha \geq \alpha_0$ or $\alpha \leq \alpha_{-0}$, the rate equivocation pair $(R(\alpha), 1)$ is achievable. Here $U = X + \alpha V$ and X is independent of V.*

Note that the expression of the secret rate $R(\alpha)$ and the code strategy here are similar to those for the dirty paper channel. It is well known that in the dirty paper channel, the rate $R(\alpha) = I(U;Y) - I(U;V)$ is maximized at $\alpha = \frac{P}{P+N_1}$. However, since in our case the range of α is limited, we are not sure whether the optimal result, the secrecy capacity will be achieved at the point $\alpha = \frac{P}{P+N_1}$.

Case 3: $I(U;Y) \geq I(U;Z) > I(U;V)$

From (4.14) and the fact that $I(U;Y) \geq I(U;Z)$, we have

$$I(U;Y) \geq I(U;Z) > I(U;V) \Longleftrightarrow \alpha_{-0} < \alpha < \alpha_0.$$

In this case, $I(U;Y) - \max(I(U;V), I(U;Z)) = I(U;Y) - I(U;Z)$. By Theorem 4.2.1, the rate equivocation pair $(I(U;Y) - I(U;Z), 1)$ is achievable. Therefore, we have the following lemma.

Lemma 4.2.3 *For any α such that $\alpha_{-0} \leq \alpha \leq \alpha_0$, the rate equivocation pair $(R_Z(\alpha), 1)$ is achievable. Here $U = X + \alpha V$ and X is independent of V.*

Note that the expression of the secret rate $R_Z(\alpha)$ is similar to the one for the Gaussian wiretap channel [4]. However, here U is an auxiliary parameter. If we take $U = X + \alpha V$, according to different values of α, U has different so-called power constraints. In the Gaussian wiretap channel, the expression of the secret rate is different. It is shown in [4] that, the rate equivocation pair $(I(X;Y) - I(X;Z), 1)$ is achievable. In that case, X has a constant power constraint P. The difference of $I(X;Y)$ and $I(X;Z)$ is maximized when X is Gaussian. Here, since U is a linear combination of two Gaussian variables X and V, U is also Gaussian. Our problem is: which U maximizes the secret rate $R_Z(\alpha) = I(U;Y) - I(U;Z)$?

4.2.2 Analysis of R and R_Z

In this subsection, we will investigate the properties of $R(\alpha)$ and $R_Z(\alpha)$ with respect to α. We also denote $R(\alpha)$ as R, $R_Z(\alpha)$ as R_Z for brevity.

Consider $R = I(U;Y) - I(U;V)$ as defined in (4.6).

$$\begin{aligned} R &= \frac{1}{2}\log\frac{P(P+Q+N_1)}{(1-\alpha)^2PQ + N_1(P+\alpha^2Q)} \\ &= \frac{1}{2}\log\frac{P(P+Q+N_1)}{Q(P+N_1)\alpha^2 - 2PQ\alpha + P(Q+N_1)} \\ &= \frac{1}{2}\log\frac{P(P+Q+N_1)}{Q(P+N_1)(\alpha - \frac{P}{P+N_1})^2 - \frac{P^2Q}{P+N_1} + P(Q+N_1)} \\ &= \frac{1}{2}\log\frac{P(P+Q+N_1)}{Q(P+N_1)(\alpha - \frac{P}{P+N_1})^2 + \frac{PN_1(P+Q+N_1)}{P+N_1}}. \end{aligned}$$

Let

$$\alpha_{max} = \frac{P}{P+N_1}. \tag{4.19}$$

As shown in Figure 4.1, we have the following lemma.

Lemma 4.2.4 *R, which is defined in (4.6), is an increasing function with respect to α as $\alpha < \alpha_{max}$; a decreasing function as $\alpha > \alpha_{max}$; maximized at $\alpha = \alpha_{max}$. In particular,*

$$R(\alpha_{max}) = C_M = \frac{1}{2}\log(1 + \frac{P}{N_1}). \tag{4.20}$$

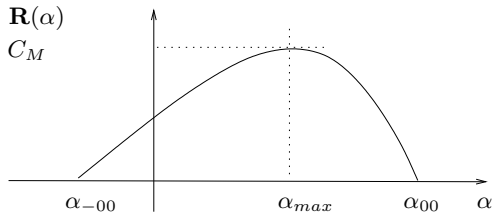


Figure 4.1: Function R when $U = X + \alpha V$, X and V are independent.

Consider $R_Z = I(U;Y) - I(U;Z)$ as defined in (4.8).

$$R_Z = \frac{1}{2}\log\frac{(P+Q+N_1)\{(1-\alpha)^2PQ + (N_1+N_2)(P+\alpha^2Q)\}}{(P+Q+N_1+N_2)\{(1-\alpha)^2PQ + N_1(P+\alpha^2Q)\}}.$$

Define

$$\alpha_{min} = -\frac{P}{Q}. \tag{4.21}$$

An easy calculation shows the following lemma. See also Figure 4.2.

Lemma 4.2.5 *R_Z, which is defined in (4.8), is an increasing function with respect to α as $\alpha_{min} < \alpha < 1$; a decreasing function as $\alpha < \alpha_{min}$ or $\alpha > 1$; minimized at $\alpha = \alpha_{min}$ and maximized at $\alpha = 1$. In particular,*

$$R_Z(\alpha_{min}) = 0; \tag{4.22}$$

$$R_Z(1) = \frac{1}{2}\log\frac{(P+Q+N_1)(N_1+N_2)}{(P+Q+N_1+N_2)N_1}. \tag{4.23}$$

Proof: See the proof in Appendix IV. ■

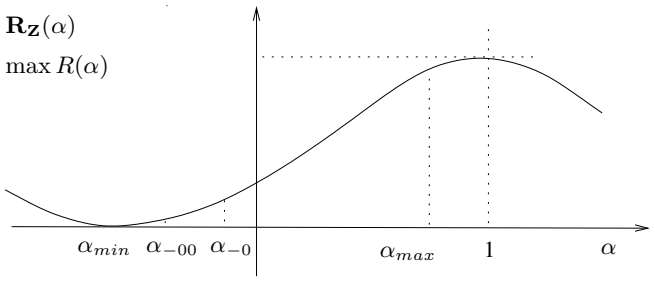
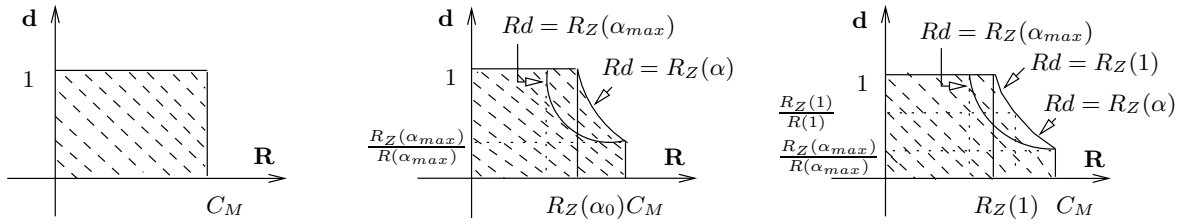


Figure 4.2: Function R_Z when $U = X + \alpha V$, X and V are independent.

4.2.3 Achievable region

So far, from Lemma 4.2.2 and Lemma 4.2.3, we know that at perfect secrecy, R is achievable when $\alpha \geq \alpha_0$ or $\alpha \leq \alpha_{-0}$; R_Z is achievable when $\alpha_{-0} \leq \alpha \leq \alpha_0$. In particular, $R = R_Z$ when $\alpha = \alpha_0$ or α_{-0}.



(**a**) $0 < P \leq P_{low}$ (**b**) $P_{low} \leq P \leq P_{high}$ (**c**) $P \geq P_{high}$

Figure 4.3: An achievable rate equivocation region for Gaussian wiretap channel with side information.

Easy comparisons show the following lemma.

Lemma 4.2.6 *$\alpha_{min} \leq \alpha_{-0} \leq \alpha_{max} < 1$, $\alpha_0 \leq \alpha_{00}$ and $\alpha_{min} \leq \alpha_{-00}$.*

By Lemma 4.2.6, we know that $\alpha_{-0} \leq \alpha_0 \leq \alpha_{00}$. According to the different possible positions of α_0, we have the following situations.

(1) $\alpha_{-0} \leq \alpha_0 \leq \alpha_{max}$.

It is clear that $\alpha_{-0} \leq \alpha_0$. Let us consider the inequality $\alpha_{max} \geq \alpha_0$.

$$\begin{aligned}
\alpha_{max} &\geq \alpha_0 \\
\frac{P}{P+N_1} &\geq \frac{P}{P+N_1+N_2}\left(1+\sqrt{\frac{P+Q+N_1+N_2}{Q}}\right) \\
\frac{PN_2}{(P+N_1)(P+N_1+N_2)} &\geq \frac{P\sqrt{Q(P+Q+N_1+N_2)}}{Q(P+N_1+N_2)} \\
\frac{N_2}{(P+N_1)} &\geq \frac{\sqrt{Q(P+Q+N_1+N_2)}}{Q} \\
QN_2 &\geq (P+N_1)\sqrt{Q(P+Q+N_1+N_2)} \\
QN_2{}^2 &\geq (P+N_1)^2(P+Q+N_1+N_2) \\
QN_2{}^2-(P+N_1)^2N_2 &\geq (P+N_1)^2(P+Q+N_1) \\
N_2 \leq -(P+N_1) \quad &\text{or} \quad N_2 \geq P+N_1+\frac{(P+N_1)^2}{Q}.
\end{aligned}$$

If we define

$$N_{high} = P+N_1+\frac{(P+N_1)^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}; \tag{4.24}$$

$$Q_{high} = \frac{(P+N_1)^2}{N_2-(P+N_1)}; \tag{4.25}$$

$$P_{low} = -N_1-\frac{Q}{2}+\frac{\sqrt{Q^2+4QN_2}}{2}. \tag{4.26}$$

Under the assumption that $P, Q, N_1, N_2 \geq 0$, it is easy to verify that

$$N_2 \geq N_{high} \Longleftrightarrow Q \geq Q_{high} \Longleftrightarrow 0 \leq P \leq P_{low}. \tag{4.27}$$

Therefore, we have the following lemma.

Lemma 4.2.7

$$N_2 \geq N_{high} \Longrightarrow \alpha_{-0} \leq \alpha_0 \leq \alpha_{max},$$

where

$$N_2 \geq N_{high} \Longleftrightarrow Q \geq Q_{high} \Longleftrightarrow 0 \leq P \leq P_{low}.$$

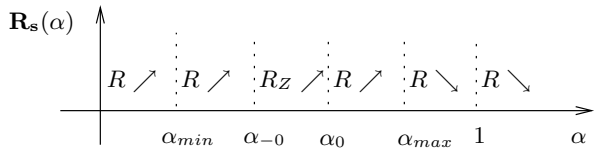


Figure 4.4: $R_s(\alpha)$ when X and V are independent and $N_2 \geq N_{high}$.

As shown in Figure 4.4, the maximal achievable secret rate in this case is $R(\alpha_{max}) = C_M$. That is, the secrecy capacity in this case is the capacity of the main channel.

The achievable rate equivocation region in this case is shown in Figure 4.3 (a). Clearly, in this case, the achievable region is in fact the capacity region.

(2) $\alpha_{max} \leq \alpha_0 \leq 1$.

Consider the inequality $\alpha_0 \leq 1$.

$$\begin{aligned}
\alpha_0 &\leq 1 \\
\frac{P}{P+N_1+N_2}(1+\sqrt{\frac{P+Q+N_1+N_2}{Q}}) &\leq 1 \\
\frac{P\sqrt{Q(P+Q+N_1+N_2)}}{Q(P+N_1+N_2)} &\leq \frac{N_1+N_2}{P+N_1+N_2} \\
P\sqrt{Q(P+Q+N_1+N_2)} &\leq Q(N_1+N_2) \\
P^2(P+Q+N_1+N_2) &\leq Q(N_1+N_2)^2 \\
P^2(P+Q) &\leq Q(N_1+N_2)^2 - P^2(N_1+N_2) \\
N_2 \leq -P \quad &\text{or} \quad N_2 \geq P - N_1 + \frac{P^2}{Q}.
\end{aligned}$$

Similarly to the analysis of the inequality $\alpha_{max} \geq \alpha_0$, we have

$$\begin{aligned}
\alpha_{max} &\leq \alpha_0 \\
QN_2{}^2 - (P+N_1)^2 N_2 &\leq (P+N_1)^2(P+Q+N_1) \\
-(P+N_1) \leq N_2 &\leq P+N_1+\frac{(P+N_1)^2}{Q}.
\end{aligned}$$

Thus we have the following:

$$\begin{array}{rcl} \alpha_{max} \leq & \alpha_0 & \leq 1 \\ -(P+N_1) \leq N_2 \leq -P & \text{or} & P - N_1 + \dfrac{P^2}{Q} \leq N_2 \leq P + N_1 + \dfrac{(P+N_1)^2}{Q}. \end{array}$$

If we define

$$N_{low} = P - N_1 + \frac{P^2}{Q}; \tag{4.28}$$

$$Q_{low} = \frac{P^2}{N_1 + N_2 - P}; \tag{4.29}$$

$$P_{high} = -\frac{Q}{2} + \frac{\sqrt{Q^2 + 4Q(N_1+N_2)}}{2}. \tag{4.30}$$

Under the assumption that $P, Q, N_1, N_2 \geq 0$, it is easy to verify that

$$N_{low} \leq N_2 \leq N_{high} \Longrightarrow Q_{low} \leq Q \leq Q_{high} \Longleftrightarrow P_{low} \leq P \leq P_{high}. \tag{4.31}$$

Therefore, we have the following lemma.

Lemma 4.2.8

$$N_{low} \leq N_2 \leq N_{high} \Longrightarrow \alpha_{max} \leq \alpha_0 \leq 1,$$

where

$$N_{low} \leq N_2 \leq N_{high} \Longleftrightarrow Q_{low} \leq Q \leq Q_{high} \Longleftrightarrow P_{low} \leq P \leq P_{high}.$$

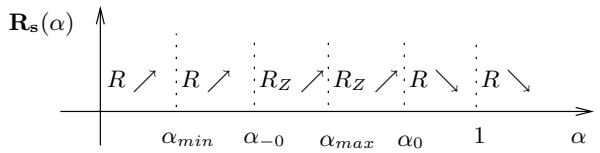


Figure 4.5: $R_s(\alpha)$ when X and V are independent and $N_{low} \leq N_2 \leq N_{high}$.

As shown in Figure 4.5, the maximal achievable secret rate in this case is $R_Z(\alpha_0)$.

The achievable rate equivocation region in this case is shown in Figure 4.3 (b). The curve which bounds the region can be divided into two parts. The first part is the line $d = 1$ as R goes from 0 to $R_Z(\alpha_0)$. The second part is the curve $Rd = R_Z(\alpha)$ as R goes from $R_Z(\alpha_0)$ to $R(\alpha_{max})$. Note that $R_Z(\alpha_0) = R(\alpha_0)$. Correspondingly, α, the parameter used to achieve (R, d) on the curve, goes from α_0 to α_{max}. The property of the curve follows immediately from the fact that $R_Z(\alpha)$ is non-increasing as α goes from α_0 to α_{max}.

(3) $\alpha_0 \geq 1$.

Similarly to the analysis of the inequality $\alpha_0 \leq 1$, we have

$$\begin{aligned} \alpha_0 &\geq 1 \\ P^2(P+Q) &\geq Q(N_1+N_2)^2 - P^2(N_1+N_2) \\ -P \leq N_2 &\leq P - N_1 + \frac{P^2}{Q}. \end{aligned}$$

Under the assumption that $P, Q, N_1, N_2 \geq 0$, it is easy to verify that

$$0 \leq N_2 \leq N_{low} \Longleftrightarrow 0 \leq Q \leq Q_{low} \Longleftrightarrow P \geq P_{high}. \tag{4.32}$$

Therefore, we have the following lemma.

Lemma 4.2.9

$$0 \leq N_2 \leq N_{low} \Longrightarrow \alpha_0 \geq 1,$$

where

$$0 \leq N_2 \leq N_{low} \Longleftrightarrow 0 \leq Q \leq Q_{low} \Longleftrightarrow P \geq P_{high}.$$

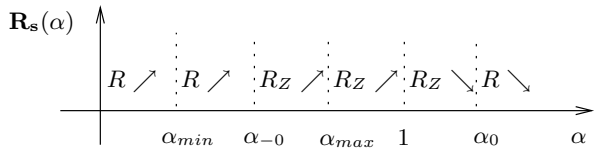


Figure 4.6: $R_s(\alpha)$ when X and V are independent and $N_2 \leq N_{low}$.

As shown in Figure 4.6, the maximal achievable secret rate in this case is $R_Z(1)$.

The achievable rate equivocation region in this case is shown in Figure 4.3 (c). The curve which bounds the region can be divided into three parts. The first part is the line $d = 1$ as R goes from 0 to $R_Z(1)$. The second part is the curve $Rd = R_Z(1)$ as R goes from $R_Z(1)$ to $R(1)$. This part is achieved by time sharing the two rate equivocation pairs $(R_Z(1), 1)$ and $(R(1), \frac{R_Z(1)}{R(1)})$. Note that $R_Z(1)$ is a constant. The third part is the curve $Rd = R_Z(\alpha)$ as R goes from $R(1)$ to $R(\alpha_{max})$. Correspondingly, α, the parameter used to achieve (R, d) on the curve, goes from 1 to α_{max}. The property of the curve follows immediately from the fact that $R_Z(\alpha)$ is non-increasing as α goes from 1 to α_{max}.

4.2.4 Discussion

As a result of the analysis in last subsection, we have the following theorem.

Theorem 4.2.10 *For the Gaussian wiretap channel with side information, a rate equivocation pair (R, d) is achievable if*

$$\begin{aligned} R &\leq C_M, \\ d &\leq 1, \end{aligned}$$

$$Rd \leq \begin{cases} C_M & 0 < P \leq P_{low} \\ \begin{cases} R(\alpha_0) & R \leq R(\alpha_0) \\ R_Z(\alpha) & R(\alpha_0) \leq R \leq C_M \end{cases} & P_{low} \leq P \leq P_{high} \\ \begin{cases} R_Z(1) & R \leq R(1) \\ R_Z(\alpha) & R(1) \leq R \leq C_M \end{cases} & P \geq P_{high} \end{cases}.$$

Furthermore,

$$\begin{aligned} 0 \leq P \leq P_{low} &\iff N_2 \geq N_{high} &&\iff Q \geq Q_{high}; \\ P_{low} \leq P \leq P_{high} &\iff N_{low} \leq N_2 \leq N_{high} &&\iff Q_{low} \leq Q \leq Q_{high}; \\ P \geq P_{high} &\iff 0 \leq N_2 \leq N_{low} &&\iff 0 \leq Q \leq Q_{low}. \end{aligned}$$

Denote the region as $\mathcal{R}_\perp$. It is shown in Figure 4.3. Note that for fixed points (R, d) on the curve $Rd = R_Z(\alpha)$, α can be determined by the value of R. Unlike the region for some special wiretap channels shown in [3,4], here $R_Z(\alpha)$ is not a constant. In addition, it is easy to verify that $R_Z(\alpha)$ is decreasing, as R goes from $R(\alpha_0)$ to C_M when $P_{low} \leq P \leq P_{high}$ and as R goes from $R(1)$ to C_M when $P \geq P_{high}$.

We define a rate equivocation region is *better* or *larger* than another one, if at the same rate of reliable transmission to the legitimate receiver, a larger equivocation for the wiretapper can be achieved.

Recall that the entire rate equivocation region $\mathcal{R}_L$ for the Gaussian wiretap channel given by Leung-Yan-Cheong and Hellman [4, Theorem 1] is defined by

$$R \leq C_M, \quad d \leq 1, \quad Rd \leq C'_s, \tag{4.33}$$

where C_M is the capacity of the main channel and

$$C'_s = \frac{1}{2} \log \frac{(P + N_1)(N_1 + N_2)}{(P + N_1 + N_2)N_1} \tag{4.34}$$

is the secrecy capacity.

Compare our region $\mathcal{R}_\perp$ with $\mathcal{R}_L$ for the corresponding Gaussian wiretap channel without side information. The following results show that the side information plays a positive role in the secret communication over the Gaussian wiretap channel.

Theorem 4.2.11 *For the Gaussian wiretap channel, the side information helps to get a larger secrecy capacity.*

Proof: By Theorem 4.2.1, the rate equivocation pair $(\min\{R_Z(\alpha_{max}), C_M\}, 1)$ is achievable, where α_{max} is defined in (4.19). So we have $C_s \geq \min\{R_Z(\alpha_{max}), C_M\}$. If we can show that both $R_Z(\alpha_{max})$ and C_M are larger than C'_s, which is the secrecy capacity of the Gaussian wiretap channel as defined in (4.34), then the proof is a straightforward consequence. It is clear that $C_M \geq C'_s$. Now let us prove that $R_Z(\alpha_{max}) \geq C'_s$.

$$\begin{aligned} R_Z(\alpha_{max}) &= \frac{1}{2} \log \frac{(P + Q + N_1)(PQ(1 - \alpha_{max})^2 + (P + \alpha_{max}^2 Q)(N_1 + N_2))}{(P + Q + N_1 + N_2)(PQ(1 - \alpha_{max})^2 + (P + \alpha_{max}^2 Q)N_1)} \\ &= \frac{1}{2} \log \frac{(P + Q + N_1)(PQ(1 - \frac{P}{P+N_1})^2 + (P + (\frac{P}{P+N_1})^2 Q)(N_1 + N_2))}{(P + Q + N_1 + N_2)(PQ(1 - \frac{P}{P+N_1})^2 + (P + (\frac{P}{P+N_1})^2 Q)N_1)} \\ &= \frac{1}{2} \log \frac{QN_1^2 + ((P + N_1)^2 + PQ)(N_1 + N_2)}{(P + Q + N_1 + N_2)(P + N_1)N_1}. \end{aligned}$$

In order to prove that $R_Z(\alpha_{max}) \geq C'_s$, we need:

$$\begin{aligned}
\frac{1}{2}\log\frac{QN_1^2+((P+N_1)^2+PQ)(N_1+N_2)}{(P+Q+N_1+N_2)(P+N_1)N_1} &\geq \frac{1}{2}\log\frac{(P+N_1)(N_1+N_2)}{(P+N_1+N_2)N_1} \\
\frac{QN_1^2+((P+N_1)^2+PQ)(N_1+N_2)}{(P+Q+N_1+N_2)(P+N_1)N_1} &\geq \frac{(P+N_1)(N_1+N_2)}{(P+N_1+N_2)N_1} \\
\frac{QN_1^2+((P+N_1)^2+PQ)(N_1+N_2)}{(P+Q+N_1+N_2)(P+N_1)} &\geq \frac{(P+N_1)(N_1+N_2)}{P+N_1+N_2} \\
(QN_1^2+((P+N_1)^2+PQ)(N_1+N_2))(P+N_1+N_2) &\geq (P+Q+N_1+N_2)(P+N_1)^2(N_1+N_2) \\
(QN_1^2+PQ(N_1+N_2))(P+N_1+N_2) &\geq Q(P+N_1)^2(N_1+N_2) \\
QN_1^2(P+N_1+N_2)+PQ(N_1+N_2)N_2 &\geq N_1Q(P+N_1)(N_1+N_2) \\
QN_1^2P+PQ(N_1+N_2)N_2 &\geq N_1QP(N_1+N_2) \\
PQ(N_1+N_2)N_2 &\geq N_1QPN_2 \\
PQN_2^2 &\geq 0,
\end{aligned}$$

which is always valid under the assumption that $P, Q, N_1, N_2 \geq 0$. ■

Theorem 4.2.12 *For the Gaussian wiretap channel, the side information helps to achieve a larger rate equivocation region.*

Proof: Compare the region $\mathcal{R}_\perp$ with $\mathcal{R}_L$ as defined by (4.33).

(a) When $0 < P \leq P_{low}$, $C_M \geq C'_s$.

(b) When $P_{low} \leq P \leq P_{high}$, $R_Z(\alpha)$ is decreasing as R goes from $R(\alpha_0)$ to C_M. Therefore, $R_Z(\alpha) \geq R_Z(\alpha_{max}) \geq C'_s$.

(c) When $P \geq P_{high}$, $R_Z(\alpha)$ is decreasing as R goes from $R(1)$ to C_M. Therefore, $R_Z(1) \geq R_Z(\alpha) \geq R_Z(\alpha_{max}) \geq C'_s$.

As we have discussed above, the theorem is concluded. ■

Recall that the region $\mathcal{R}_M$ given by Mitrpant in [8, Theorem 4.4] or [9, Theorem 3] can be expressed as follows:

$$\begin{aligned}
R &\leq C_M, \\
d &\leq 1, \\
Rd &\leq \begin{cases} C_M & 0 < P \leq P_{low} \\ \min\{C_M d_C, R(\alpha_0)\} & P_{low} \leq P \leq P_{high} \\ \min\{C_M d_C, R_Z(1)\} & P \geq P_{high} \end{cases},
\end{aligned}$$

where

$$d_C = 1 - I(U_{\alpha_{max}}; Z)/C_M. \tag{4.35}$$

An easy comparison shows the following result.

Corollary 4.2.13 *The region $\mathcal{R}_\perp$ is better than $\mathcal{R}_M$.*

Proof: We compare the region $\mathcal{R}_\perp$ with $\mathcal{R}_M$. Since $C_M d_C = C_M - I(U_{\alpha_{max}}; Z) = R_Z(\alpha_{max}) - I(U_{\alpha_{max}}; V)$, then

(a) When $P_{low} \leq P \leq P_{high}$, as R goes from $R(\alpha_0)$ to C_M, $R_Z(\alpha_0) \geq R_Z(\alpha) \geq R_Z(\alpha_{max}) \geq C_M d_C$;

(b) When $P \geq P_{high}$, as R goes from $R(1)$ to C_M, $R_Z(1) \geq R_Z(\alpha) \geq R_Z(\alpha_{max}) \geq C_M d_C$. In addition that when $0 < P \leq P_{low}$, $\mathcal{R}_\perp$ and $\mathcal{R}_M$ are the same, we complete the proof. ■

From above proof, $\min\{C_M d_C, R(\alpha_0)\} = C_M d_C$ exists in both cases when $P_{low} \leq P \leq P_{high}$ and $P \geq P_{high}$. Hence, the region $\mathcal{R}_M$ can be simplified as follows:

$$\begin{aligned} R &\leq C_M, \\ d &\leq 1, \\ Rd &\leq \begin{cases} C_M & 0 < P \leq P_{low} \\ C_M d_C & P \geq P_{low} \end{cases}. \end{aligned}$$

It is very interesting to find that, for the wiretap channel in Gaussian case, unlike the dirty paper channel, the side information helps to get a larger secrecy capacity and a larger capacity region. Therefore, the side information provides an advantage to achieve secure communication over the Gaussian wiretap channel. Furthermore, we extend our result for the dicrete memoryless wiretap channel with side information to the Gaussian case by applying Costa's strategy [7] to the auxiliary parameter U. As a straightforward consequence of the technique improvement as shown in the proof of Theorem 4.2.1, we derive an achievable rate equivocation region which is better than the one given by Mitrpant in [8, Theorem 4.4] or [9, Theorem 3].

4.3 A general result on dirty paper channel

Note that in Costa's strategy, the codewords chosen to send to the channel are independent of the side information. In this section, we generalize Costa's strategy by taking codewords dependent on the side information into our consideration. In addition, for easy calculations, we develop a geometric interpretation of the mutual information of Gaussian variables. Then, reconsidering the communication problem for the dirty paper channel, we give a more general result.

4.3.1 Preliminaries

Let X and V be two random variables with expected values u_X and u_Y and standard deviation σ_X and σ_V. The *covariance* between X and V is defined as:

$$\mathrm{cov}(X, V) = \mathrm{E}((X - u_x)(V - u_v)). \tag{4.36}$$

It is clear that $\mathrm{cov}(X, V) = \mathrm{cov}(V, X)$. The *correlation coefficient* ρ_{XV} between X and V is defined as:

$$\rho_{XV} = \frac{\mathrm{cov}(X, V)}{\sigma_X \sigma_V}. \tag{4.37}$$

Note that the correlation coefficient cannot exceed 1 in absolute value by applying the Cauchy-Schwarz inequality [1]. The *covariance matrix* is defined as:

$$\mathrm{K} = \begin{bmatrix} \mathrm{cov}(X, X) & \mathrm{cov}(X, V) \\ \mathrm{cov}(V, X) & \mathrm{cov}(V, V) \end{bmatrix} = \begin{bmatrix} \sigma_X^2 & \rho_{XV}\sigma_X\sigma_V \\ \rho_{XV}\sigma_X\sigma_V & \sigma_V^2 \end{bmatrix}. \tag{4.38}$$

[1] For any variables X and V, the Cauchy-Schwarz inequality states that $[\mathrm{E}(XV)]^2 \leq \mathrm{E}(X^2)\mathrm{E}(V^2)$.

If X, V are jointly Gaussian and with zero-mean, and $U = X + \alpha V = (1, \alpha)(X, V)^{\mathrm{T}}$, where $(X, V)^{\mathrm{T}}$ is the transpose of the vector (X, V), then U also has a Gaussian distribution with mean u_U and variance σ_U^2, where

$$\begin{aligned} u_U &= (1,\alpha)(u_X, u_V)^{\mathrm{T}} = (1,\alpha)(0,0)^{\mathrm{T}} = 0 \qquad (4.39) \\ \sigma_U^2 &= (1,\alpha)K(1,\alpha)^{\mathrm{T}} \\ &= (1,\alpha)\begin{bmatrix} \sigma_X^2 & \rho_{XV}\sigma_X\sigma_V \\ \rho_{XV}\sigma_X\sigma_V & \sigma_V^2 \end{bmatrix}\begin{pmatrix} 1 \\ \alpha \end{pmatrix} \\ &= \sigma_X^2 + 2\alpha\rho_{XV}\sigma_X\sigma_V + \alpha^2\sigma_V^2. \qquad (4.40) \end{aligned}$$

In particular, when $\alpha = 1$, then $u_U = 0$ and $\sigma_U^2 = \sigma_X^2 + 2\rho_{XV}\sigma_X\sigma_V + \sigma_V^2$.

4.3.2 Geometric interpretation of Gaussian mutual information

Consider a standard AWGN channel with input $X \sim \mathcal{N}(0, P)$, noise $\eta \sim \mathcal{N}(0, N)$ and output $Y = X + \eta \sim \mathcal{N}(0, P + N)$.

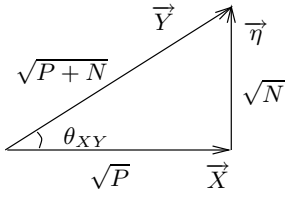


Figure 4.7: Geometric interpretation of mutual information.

It is known that the correlation coefficient can also be viewed as the cosine of the angle between the two vectors X and Y, when both X and Y are zero-mean. As shown in Figure 4.7, we define the angel θ_{XY} as the angel anti-clockwise from vector $\overrightarrow{X}$ to vector $\overrightarrow{Y}$. The symmetric property of the correlation coefficient follows immediately: $\rho_{XY} = \rho_{YX}$, since $\cos\theta_{XY} = \cos(2\pi - \theta_{XY}) = \cos\theta_{YX}$. Then, by the definition of the two Gaussian variables and $\cos\theta_{XY} = \frac{\sqrt{P}}{\sqrt{P+Q}}$, we have

$$\begin{aligned} I(X;Y) &= \frac{1}{2}\log\frac{1}{1-{\rho_{XY}}^2} \\ &= \frac{1}{2}\log\frac{1}{1-\cos^2\theta_{XY}} \\ &= \frac{1}{2}\log\frac{1}{1-\frac{P}{P+N}} \\ &= \frac{1}{2}\log(1+\frac{P}{N}). \end{aligned}$$

Thus, we get the capacity of the AWGN channel.

So far, we can re-denote the mutual information of two zero-mean Gaussian signals X and Y as follow:

$$I(X;Y) = \frac{1}{2}\log\frac{1}{1-\cos^2\theta_{XY}} = \frac{1}{2}\log\frac{1}{\sin^2\theta_{XY}}. \qquad (4.41)$$

Furthermore, the formula (4.40) can also be derived in a geometric way easily. If X, V are jointly Gaussian and with zero-mean and $U = X + \alpha V$, then U also has a Gaussian

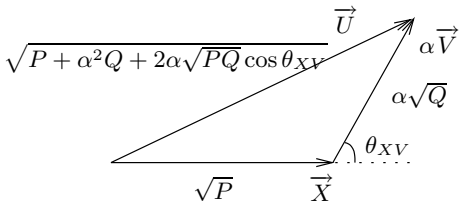


Figure 4.8: Geometric interpretation of $U = X + \alpha V$, when X and V are dependent.

distribution with mean 0 and variance σ_U^2. As shown in Figure 4.8, if we take the length of the vector as its standard deviation, since $\rho_{XV} = \cos\theta_{XV}$,

$$\begin{aligned} \sigma_U^2 &= |\overrightarrow{U}|^2 \\ &= P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV} \\ &= P + \alpha^2 Q + 2\alpha\rho_{XV}\sqrt{PQ}. \end{aligned} \tag{4.42}$$

4.3.3 Rate

Now we return to the communication problem for the dirty paper channel. Proceeding similarly to Costa's approach, we use the result on the capacity of the discrete memoryless channel with side information noncausally available at the transmitter by Gel'fand and Pinsker [10] and Heegard and El Gamal [11], the formula (1.20). Extending the result to Gaussian case, instead of looking for an appropriate auxiliary variable U, we try to go through more possible auxiliary variable U, in the matter that U is also Gaussian.

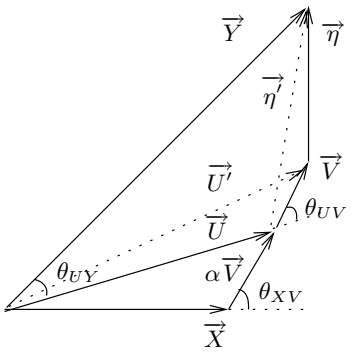


Figure 4.9: Geometric interpretation of dirty paper coding, when X and V are dependent.

Similarly to Costa [7], we consider $U = X + \alpha V$, where X and V are normally distributed according to $\mathcal{N}(0, P)$ and $\mathcal{N}(0, Q)$, respectively; α is a parameter. Here we generalize Costa's strategy by taking the correlation coefficient of X and V, ρ_{XV} into our consideration. Referring to Figure 4.9, we have the followings:

$$\begin{aligned} |\overrightarrow{X}| &= \sqrt{P}, \\ |\overrightarrow{V}| &= \sqrt{Q}, \\ |\overrightarrow{\eta}| &= \sqrt{N}, \\ |\overrightarrow{\eta'}| &= \sqrt{(1-\alpha)^2 Q + N}, \end{aligned}$$

$$
\begin{aligned}
|\overrightarrow{U'}| &= \sqrt{P+Q+2\sqrt{PQ}\cos\theta_{XV}},\\
|\overrightarrow{U}| &= \sqrt{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}},\\
|\overrightarrow{Y}| &= \sqrt{P+Q+N_1+2\sqrt{PQ}\cos\theta_{XV}}.
\end{aligned}
$$

By the law of cosines, it is easy to get that

$$
\begin{aligned}
\cos\theta_{UY} &= \frac{|\overrightarrow{U}|^2+|\overrightarrow{Y}|^2-|\overrightarrow{\eta'}|^2}{2|\overrightarrow{U}|\cdot|\overrightarrow{Y}|}\\
&= \frac{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}+P+Q+N+2\sqrt{PQ}\cos\theta_{XV}-(1-\alpha)^2Q-N}{2\sqrt{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}}\cdot\sqrt{P+Q+N+2\sqrt{PQ}\cos\theta_{XV}}}\\
&= \frac{P+\alpha Q+(1+\alpha)\sqrt{PQ}\cos\theta_{XV}}{\sqrt{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}}\cdot\sqrt{P+Q+N+2\sqrt{PQ}\cos\theta_{XV}}};\\
\cos\theta_{UV} &= \frac{|\overrightarrow{U}|^2+|\alpha\overrightarrow{V}|^2-|\overrightarrow{X}|^2}{2|\overrightarrow{U}|\cdot|\alpha\overrightarrow{V}|}\\
&= \frac{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}+\alpha^2Q-P}{2\sqrt{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}}\cdot\alpha\sqrt{Q}}\\
&= \frac{\alpha\sqrt{Q}+\sqrt{P}\cos\theta_{XV}}{\sqrt{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}}}.
\end{aligned}
$$

By Pythagorean identity, for any θ, $\sin^2\theta+\cos^2\theta=1$, we have

$$
\begin{aligned}
\sin^2\theta_{UY} &= 1-\cos^2\theta_{UY}\\
&= 1-(\frac{P+\alpha Q+(1+\alpha)\sqrt{PQ}\cos\theta_{XV}}{\sqrt{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}}\cdot\sqrt{P+Q+N+2\sqrt{PQ}\cos\theta_{XV}}})^2\\
&= \frac{(1-\alpha)^2PQ(1-\cos^2\theta_{XV})+N(P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV})}{(P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV})(P+Q+N+2\sqrt{PQ}\cos\theta_{XV})};\\
\sin^2\theta_{UV} &= 1-\cos^2\theta_{UV}\\
&= 1-(\frac{\alpha\sqrt{Q}+\sqrt{P}\cos\theta_{XV}}{\sqrt{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}}})^2\\
&= \frac{P(1-\cos^2\theta_{XV})}{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}}.
\end{aligned}
$$

Recalling (4.41), the difference of mutual information can be calculated to yield

$$
I(U;Y)-I(U;V)=\frac{1}{2}\log\frac{1}{\sin^2\theta_{UY}}-\frac{1}{2}\log\frac{1}{\sin^2\theta_{UV}}=\frac{1}{2}\log\frac{\sin^2\theta_{UV}}{\sin^2\theta_{UY}}.
$$

Taking $\rho_{XV}=\cos\theta_{XV}$, we have

$$
I(U;Y)-I(U;V)=\frac{1}{2}\log\frac{P(1-\rho_{XV}^2)(P+Q+N+2\sqrt{PQ}\rho_{XV})}{(1-\alpha)^2PQ(1-\rho_{XV}^2)+N(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})}.
$$

Let

$$R = I(U;Y) - I(U;V). \tag{4.43}$$

Then

$$R = \frac{1}{2}\log\frac{P(1-\rho_{XV}^2)(P+Q+N+2\sqrt{PQ}\rho_{XV})}{(1-\alpha)^2PQ(1-\rho_{XV}^2)+N(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})}$$

$$= \frac{1}{2}\log\frac{P(1-\rho_{XV}^2)(P+Q+N+2\sqrt{PQ}\rho_{XV})}{Q[P(1-\rho_{XV}^2)+N]\alpha^2-2[PQ(1-\rho_{XV}^2)-N\sqrt{PQ}\rho_{XV}]\alpha+P[Q(1-\rho_{XV}^2)+N]}$$

$$= \frac{1}{2}\log\frac{P(1-\rho_{XV}^2)(P+Q+N+2\sqrt{PQ}\rho_{XV})}{Q[P(1-\rho_{XV}^2)+N](\alpha-\alpha_{max})^2+\frac{PN(1-\rho_{XV}^2)(P+Q+N+2\sqrt{PQ}\rho_{XV})}{P(1-\rho_{XV}^2)+N}},$$

where

$$\alpha_{max} = \frac{PQ(1-\rho_{XV}^2)-N\sqrt{PQ}\rho_{XV}}{Q(P(1-\rho_{XV}^2)+N)}. \tag{4.44}$$

Maximizing R over α, we get

$$\max_{\alpha} R = \frac{1}{2}\log(1+\frac{P(1-\rho_{XV}^2)}{N}) \tag{4.45}$$

obtained at $\alpha = \alpha_{max}$. Therefore, we have the following theorem.

Theorem 4.3.1 *For the dirty paper channel, generalizing Costa's strategy [7], we choose the auxiliary variable U in the form of $U = X + \alpha V$, where the correlation coefficient of X and V is ρ_{XV}. Then the maximal rate we could achieve by dirty paper coding is*

$$\max_{\alpha} R = \frac{1}{2}\log(1+\frac{P(1-\rho_{XV}^2)}{N}).$$

The maximum is achieved at $\alpha = \alpha_{max}$, where α_{max} is defined in (4.45).

4.3.4 Discussion

The value of the correlation coefficient indicates the degree of linear dependence between the variables. The closer the coefficient is to either -1 or 1, the stronger the correlation between the variables. If the variables are independent, then the correlation is 0. But the converse is not true, because the correlation coefficient detects only linear dependencies between two variables. However, in the special case when X and V are jointly normal distributed, independence is equivalent to uncorrelatedness.

Theorem 4.3.1 shows that, in order to achieve reliable transmission with as high as possible rate by dirty paper coding, the best choice of X is orthogonal to the side information V. In particular, when X is dependent on V, here we use the correlation coefficient ρ_{XV} to represent their dependency, so far the best we can do, can be achieved with less power by the way of sending codewords orthogonal to V but only with power $P(1-{\rho_{XV}}^2)$. That is, if the chosen X is dependent on V, in fact, only $1-{\rho_{XV}}^2$ part of the power is efficient in the transmission.

4.4 An extended rate equivocation region

In this section, we think of the best choice of codewords sent to the channel for the Gaussian wiretap channel with side information. Recall that Costa [7] showed that for dirty paper channel, the optimal encoder adapts to the side information and uses it to his advantage, rather than attempting to fight and cancel it. By choosing codewords orthogonal to the side information, the channel capacity could be reached by dirty paper coding. Note that the coding strategy used for the wiretap channel with side information is similar to the one for the dirty paper channel. However, we wonder whether it might be a better choice to send codewords dependent on the side information in some cases, in order to yield higher rate with the same equivocation. We will show in this section that it is true, as a consequence of an additional parameter ρ_{XV} in our optimization.

Differently from Mitrpant in [8, 9] and more general than Costa in [7], we make use of the auxiliary random variable $U = X + \alpha V$, where α is a real number and X can be dependent on V. Using our technique given in Section 3.3, we provide a straightforward proof to extend Theorem 3.2.1 to the Gaussian case by applying the generalized Costa's strategy to the auxiliary parameter U as follows.

Theorem 4.4.1 *Consider the Gaussian wiretap channel with side information as shown in Figure 1.7. We make use of the auxiliary random variable $U = X + \alpha V$, where α is a real number and X can be dependent on V. Let ρ_{XV} be the correlation coefficient of X and V. For fixed $\alpha \in \mathbb{R}$ and $\rho_{XV} \in [-1, 1]$, denote $\mathcal{R}_U$ as the set of points (R, d) with*

$$R_{U1} \leq R \leq R_{U2}, \quad 0 \leq d \leq 1, \quad Rd = R_{U1},$$

where R_{U1} and R_{U2} are defined in (3.7) and (3.8). Here $\mathbb{R}$ represents the set of all real numbers. Let

$$\mathcal{R}'_U \triangleq \{(R', d') : 0 \leq R' \leq R, 0 \leq d' \leq d, (R, d) \in \mathcal{R}_U\},$$

and

$$\mathcal{R}_{\rho_{XV}} = \bigcup_{U=X+\alpha V, \alpha \in \mathbb{R}} \mathcal{R}'_U.$$

Then the set $\mathcal{R}$, defined as follows, is achievable:

$$\mathcal{R} = \bigcup_{\rho_{XV} \in [-1,1]} \mathcal{R}_{\rho_{XV}}.$$

Proof: The proof is almost the same as the proof of Theorem 3.2.1 given in section 3.3. We only need to show that $\mathcal{R}_U$ is achievable for the specified α, ρ_{XV} and U. Assume that the channel has power constraint P and the side information satisfies $V \sim \mathcal{N}(0, Q)$. For a fixed ϵ, let $P' = P(1+2c\epsilon)^{-1}$, where c is a constant as defined in Lemma 2.2.8. Due to the Gaussian characteristic of the channel, we make slight modifications in the achievability proof of $\mathcal{R}_U$ as follows:

- In the codebook generation, sequences u^N are generated according to $f(u^N) = \prod_{i=1}^{N} f(u_i)$. Here we specify $f(u_i) \sim \mathcal{N}(0, P' + \alpha^2 Q)$ for all $i \in \{1, 2, \cdots, N\}$.
- In the encoding process, $x^N(j) = u^N(j) - \alpha v^N$.
- The legitimate receiver observes $y^N = x^N(j) + v^N + \eta_1^N$ and the wiretapper observes $z^N = y^N + \eta_2^N$.

As a consequence of these modifications, there is one more source of potential error for the legitimate receiver.

- $\mathcal{E}^X(j)$: in the encoding process, $x^N(j) = u^N(j) - \alpha v^N$ does not satisfy the power constraint.

However, provided that there is at least one sequence $u^N(j)$ jointly typical with v^N, the probability that $\mathcal{E}^X(j)$ occurs is 0 according to Lemma 2.2.9. Therefore, the modifications do not influence the achievability proof of $\mathcal{R}_U$. Let ϵ be arbitrarily small. Since $P' \to P$ as $\epsilon \to 0$, we have shown that R_U is asymptotically achievable for $\alpha \in \mathbb{R}$ and $U = X + \alpha V$, where $X \sim \mathcal{N}(0, P)$ and the correlation coefficient of X and V is ρ_{XV}. Thus we conclude our proof. ■

As you will see in Section 4.2.4, the extended region by applying the generalized Costa's strategy to the auxiliary parameter U improves the region $\mathcal{R}_\perp$ which is derived by applying Costa's strategy to U.

4.4.1 Model description

For the dirty paper channel, Costa [7] considers $U = X + \alpha V$, where X and V are independent random variables distributed according to $\mathcal{N}(0, P)$ and $\mathcal{N}(0, Q)$, respectively, and α is a parameter to be determined. Here we use the generalized Costa's strategy as introduced in last section. We take $U = X + \alpha V$ and investigate the more general situation when the correlation coefficient of X and V is ρ_{XV}. It is clear that $\rho_{XV} = 0$ when X and V are independent. With an abuse of the notation, we still use the notations $U_*, R_s(*), R(*), R_Z(*)$ and $d(*)$ as defined in (4.1)$\sim$(4.5) for convienence. We need to keep in mind that in this section, the correlation coefficient of X and V is ρ_{XV}. For a fixed ρ_{XV}, we denote the *maximal secret rate* as

$$R_s = \max_{\alpha}\{I(U;Y) - \max\{I(U:V), I(U;Z)\}\}. \tag{4.46}$$

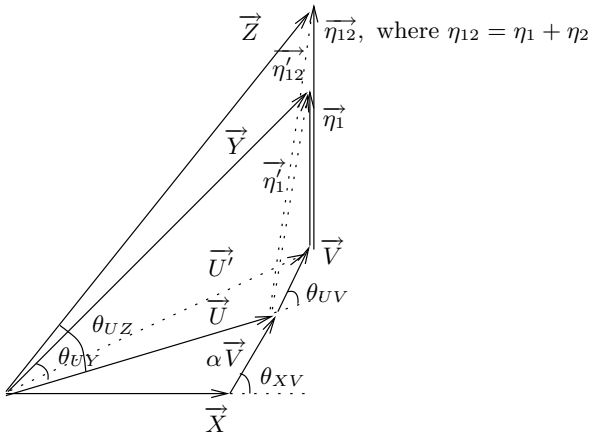


Figure 4.10: Geometric interpretation of dirty paper coding in the wiretap channel with side information, when X and V are dependent.

Now Let us calculate the values of $I(U, V)$, $I(U, Y)$ and $I(U, Z)$ with respect to $U = X + \alpha V$. Note that here X and V can be dependent and their correlation coefficient is ρ_{XV}.

Referring to Figure 4.10 and the calculations in Appendix I, we have the following:

$$\begin{aligned} I(U;Y) &= \frac{1}{2}\log\frac{(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{(1-\alpha)^2PQ(1-\rho_{XV}^2)+N_1(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})}; \\ I(U;Z) &= \frac{1}{2}\log\frac{(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})(P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})}{(1-\alpha)^2PQ(1-\rho_{XV}^2)+(N_1+N_2)(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})}; \\ I(U;V) &= \frac{1}{2}\log\frac{P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV}}{P(1-\rho_{XV}^2)}. \end{aligned}$$

It is a straightforward consequence that

$$I(U;Y)-I(U;V) = \frac{1}{2}\log\frac{P(1-\rho_{XV}^2)(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{(1-\alpha)^2PQ(1-\rho_{XV}^2)+N_1(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})}; \tag{4.47}$$

$$I(U;Z)-I(U;V) = \frac{1}{2}\log\frac{P(1-\rho_{XV}^2)(P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})}{(1-\alpha)^2PQ(1-\rho_{XV}^2)+(N_1+N_2)(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})}; \tag{4.48}$$

$$\begin{aligned} I(U;Y)-I(U;Z) = \frac{1}{2}\log\Big(&\frac{(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{(P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})}\cdot \\ &\frac{\{(1-\alpha)^2PQ(1-\rho_{XV}^2)+(N_1+N_2)(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})\}}{\{(1-\alpha)^2PQ(1-\rho_{XV}^2)+N_1(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})\}}\Big). \end{aligned} \tag{4.49}$$

Note that Z is a degraded version of Y. Thus, we have $I(U;Y)\geq I(U;Z)$. You can also find a proof of it in Appendix V. So we distinguish the following three cases:

(1) $I(U;V)>I(U;Y)>I(U;Z)$;

(2) $I(U;Y)\geq I(U;V)\geq I(U;Z)$;

(3) $I(U;Y)\geq I(U;Z)>I(U;V)$.

Case 1: $I(U;V)>I(U;Y)>I(U;Z)$

From (4.47), through easy calculation, we obtain that

$$I(U;V)>I(U;Y) \iff \alpha>\alpha_{00} \quad \text{or} \quad \alpha<\alpha_{-00}; \tag{4.50}$$

$$I(U;Y)\geq I(U;V) \iff \alpha_{-00}\leq\alpha\leq\alpha_{00}, \tag{4.51}$$

where

$$\begin{aligned} \alpha_{00} &= \frac{P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1)}}{Q[P(1-\rho_{XV}^2)+N_1]} \\ &\quad +\frac{PQ(1-\rho_{XV}^2)-N_1\sqrt{PQ}\rho_{XV}}{Q[P(1-\rho_{XV}^2)+N_1]}; \end{aligned} \tag{4.52}$$

$$\begin{aligned} \alpha_{-00} &= -\frac{P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1)}}{Q[P(1-\rho_{XV}^2)+N_1]} \\ &\quad +\frac{PQ(1-\rho_{XV}^2)-N_1\sqrt{PQ}\rho_{XV}}{Q[P(1-\rho_{XV}^2)+N_1]}. \end{aligned} \tag{4.53}$$

See the proof of (4.50) and (4.51) in Appendix VI.

In Case 1, $I(U;Y) - \max(I(U;V), I(U;Z)) = I(U;Y) - I(U;V)$ is less than 0. For practical purpose, we only need to consider the situation when $\alpha_{-00} \leq \alpha \leq \alpha_{00}$.

Case 2: $I(U;Y) \geq I(U;V) \geq I(U;Z)$

From (4.48), through easy calculation, we obtain that

$$I(U;V) \geq I(U;Z) \iff \alpha \geq \alpha_0 \quad \text{or} \quad \alpha \leq \alpha_{-0}, \tag{4.54}$$

$$I(U;Z) > I(U;V) \iff \alpha_{-0} < \alpha < \alpha_0. \tag{4.55}$$

where

$$\begin{aligned} \alpha_0 &= \frac{P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)}}{Q[P(1-\rho_{XV}^2)+N_1+N_2]} \\ &\quad + \frac{PQ(1-\rho_{XV}^2) - (N_1+N_2)\sqrt{PQ}\rho_{XV}}{Q[P(1-\rho_{XV}^2)+N_1+N_2]}; \end{aligned} \tag{4.56}$$

$$\begin{aligned} \alpha_{-0} &= -\frac{P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)}}{Q[P(1-\rho_{XV}^2)+N_1+N_2]} \\ &\quad + \frac{PQ(1-\rho_{XV}^2) - (N_1+N_2)\sqrt{PQ}\rho_{XV}}{Q[P(1-\rho_{XV}^2)+N_1+N_2]}. \end{aligned} \tag{4.57}$$

We can derive (4.54) in the way similar to the proof of (4.50). Note that when $I(U;V) = I(U;Z)$,

$$I(U;Y) - I(U;V) = I(U;Y) - I(U;Z) \iff \alpha = \alpha_0 \text{ or } \alpha_{-0}.$$

Thus,

$$R(\alpha_0) = R_Z(\alpha_0); \tag{4.58}$$

$$R(\alpha_{-0}) = R_Z(\alpha_{-0}). \tag{4.59}$$

Due to (4.51) and (4.54), we have

$$I(U;Y) \geq I(U;V) \geq I(U;Z) \iff \alpha_{-00} \leq \alpha \leq \alpha_{00} \quad \text{and} \quad \alpha \geq \alpha_0 \quad \text{or} \quad \alpha \leq \alpha_{-0},$$

In Case 2, $I(U;Y) - \max(I(U;V), I(U;Z)) = I(U;Y) - I(U;V)$. By Theorem 4.4.1, the rate equivocation pair $(I(U;Y) - I(U;V), 1)$ is achievable. Therefore, we have the following lemma.

Lemma 4.4.2 *For any α such that $\alpha_{-00} \leq \alpha \leq \alpha_{00}$, and $\alpha \geq \alpha_0$ or $\alpha \leq \alpha_{-0}$, the rate equivocation pair $(R(\alpha), 1)$ is achievable. Here $U = X + \alpha V$, and the correlation coefficient of X and V is ρ_{XV}.*

Note that the expression of the secret rate $R(\alpha)$ and the code strategy here are similar to those for the dirty paper channel. It is well known that in the dirty paper channel, $R(\alpha) = I(U;Y) - I(U;V)$ is maximized at $\alpha = \frac{P}{P+N_1}$. The codeword sent by the optimal encoder is orthogonal to V. However, in our case, we are not sure whether this α and $\rho_{XV} = 0$ still yield the optimal result.

Case 3: $I(U;Y) \geq I(U;Z) > I(U;V)$

From (4.55) and the fact that $I(U;Y) \geq I(U;Z)$, we obtain that

$$I(U;Y) \geq I(U;Z) > I(U;V) \Longleftrightarrow \alpha_{-0} < \alpha < \alpha_0.$$

In this case, $I(U;Y) - \max(I(U;V), I(U;Z)) = I(U;Y) - I(U;Z)$. By Theorem 4.4.1, the rate equivocation pair $(I(U;Y) - I(U;Z), 1)$ is achievable. Therefore, we have the following lemma.

Lemma 4.4.3 *For any α such that $\alpha_{-0} \leq \alpha \leq \alpha_0$, the rate equivocation pair $(I(U;Y) - I(U;Z), 1)$ is achievable. Here $U = X + \alpha V$, and the correlation coefficient of X and V is ρ_{XV}.*

Here, the expression of the secret rate $R_Z(\alpha)$ is similar to the one for the Gaussian wiretap channel [4]. However, note that U is an auxiliary parameter. If we take $U = X + \alpha V$, according to different values of α, U has different so-called power constraints. In the Gaussian wiretap channel, the expression of the secret rate is different. It is shown in [4] that, the rate equivocation pair $(I(X;Y) - I(X;Z), 1)$ is achievable. In that case, X has a constant power constraint P. The difference of $I(X;Y)$ and $I(X;Z)$ is maximized when X is Gaussian. Here we only consider the situation when U is Gaussian. Now we can state the following problems: which U maximizes the secret rate $R_Z(\alpha) = I(U;Y) - I(U;Z)$? Is $\rho_{XV} = 0$ still a best choice to achieve higher rate with the same equivocation, as it is optimal to yield the channel capacity in the dirty paper channel?

4.4.2 Analysis of R and R_Z

In this subsection, we will investigate for a fixed ρ_{XV}, the properties of $R(\alpha)$ and $R_Z(\alpha)$ with respect to α. We also denote $R(\alpha)$ as R, $R_Z(\alpha)$ as R_Z for brevity.

Consider $R = I(U;Y) - I(U;V)$ as defined in (4.47).

$$R = \frac{1}{2}\log\frac{P(1-\rho_{XV}^2)(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{(1-\alpha)^2PQ(1-\rho_{XV}^2)+N_1(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})}$$

$$= \frac{1}{2}\log\frac{P(1-\rho_{XV}^2)(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{Q[P(1-\rho_{XV}^2)+N_1](\alpha-\alpha_{max})^2+\frac{PN_1(1-\rho_{XV}^2)(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{P(1-\rho_{XV}^2)+N_1}}, \tag{4.60}$$

where

$$\alpha_{max} = \frac{PQ(1-\rho_{XV}^2) - N_1\sqrt{PQ}\rho_{XV}}{Q[P(1-\rho_{XV}^2)+N_1]}. \tag{4.61}$$

An easy calculation shows the following lemma. See also Figure 4.11.

Lemma 4.4.4 *R, which is defined in (4.47). is an increasing function with respect to α as $\alpha < \alpha_{max}$; a decreasing function as $\alpha > \alpha_{max}$; is maximized at $\alpha = \alpha_{max}$. In particular,*

$$R(\alpha_{max}) = \frac{1}{2}\log(1+\frac{P(1-\rho_{XV}^2)}{N_1}). \tag{4.62}$$

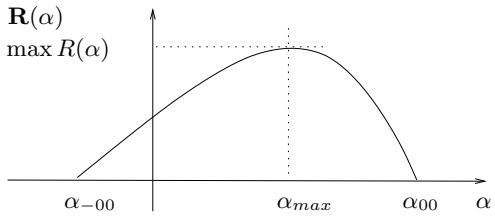


Figure 4.11: Function R when $U = X + \alpha V$, the correlation coefficient of X and V is ρ_{XV}.

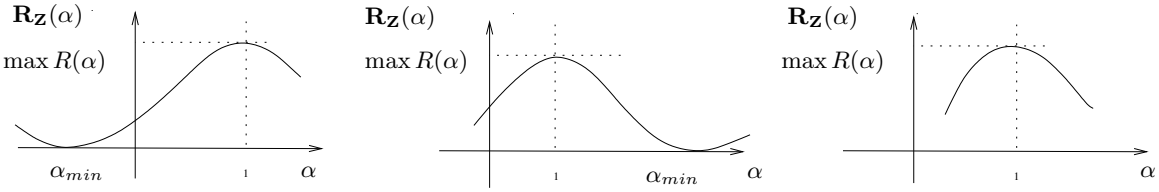
Consider $R_Z = I(U;Y) - I(U;Z)$ as defined in (4.49).

$$R_Z = \frac{1}{2}\log\frac{(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{(P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})}$$

$$+\frac{1}{2}\log\frac{(1-\alpha)^2PQ(1-\rho_{XV}^2)+(N_1+N_2)(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})}{(1-\alpha)^2PQ(1-\rho_{XV}^2)+N_1(P+\alpha^2Q+2\alpha\sqrt{PQ}\rho_{XV})}.$$

Define

$$\alpha_{min} = -\frac{\sqrt{P}(\sqrt{P}+\sqrt{Q}\rho_{XV})}{\sqrt{Q}(\sqrt{P}\rho_{XV}+\sqrt{Q})}. \tag{4.63}$$



(a) $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$ (b) $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$ (c) $\sqrt{P}\rho_{XV} + \sqrt{Q} = 0$

Figure 4.12: Function R_Z when $U = X + \alpha V$, the correlation coefficient of X and V is ρ_{XV}.

An easy calculation shows the following lemma. See also Figure 4.12.

Lemma 4.4.5 *R_Z, which is defined in (4.49), is maximized at $\alpha = 1$ and minimized at $\alpha = \alpha_{min}$. Furthermore,*

(a) when $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$, R_Z is
a non-increasing function with respect to α as $\alpha \le \alpha_{min}$;
a non-decreasing function as $\alpha_{min} \le \alpha \le 1$;
a non-increasing function as $\alpha \ge 1$.

(b) when $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$, R_Z is
a non-decreasing function with respect to α as $\alpha \le 1$;
a non-increasing function as $1 \le \alpha \le \alpha_{min}$;
a non-decreasing function as $\alpha \ge \alpha_{min}$.

(c) when $\sqrt{P}\rho_{XV} + \sqrt{Q} = 0$, R_Z is
a non-decreasing function with respect to α as $\alpha \le 1$ and a non-increasing function as $\alpha > 1$.

In particular,

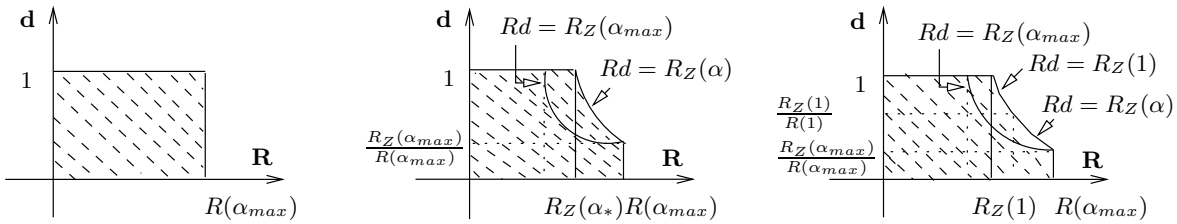
$$R_Z(\alpha_{min}) = 0; \tag{4.64}$$

$$R_Z(1) = \frac{1}{2}\log\frac{(P+Q+2\sqrt{PQ}\rho_{XV}+N_1)(N_1+N_2)}{(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)N_1}. \tag{4.65}$$

Proof: See the proof in Appendix VII. ■

4.4.3 Achievable region

So far, from Lemma 4.4.2 and Lemma 4.4.3, we know that at perfect secrecy, R is achievable when $\alpha \geq \alpha_0$ or $\alpha \leq \alpha_{-0}$; R_Z is achievable when $\alpha_{-0} \leq \alpha \leq \alpha_0$. In particular, $R = R_Z$ when $\alpha = \alpha_0$ or α_{-0}. Note that, according to the sign of $\sqrt{P}\rho_{XV} + \sqrt{Q}$, R_Z with respect to α has different property. Hence, we investigate the achievable region in the following three cases.



(**a**) $N_2 \geq N_{high}$ (**b**) $N_{low} \leq N_2 \leq N_{high}$ (**c**) $N_2 \leq N_{low}$

Figure 4.13: The general achievable rate equivocation region for Gaussian wiretap channel with side information. If $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$, $\alpha_* = \alpha_0$; else if $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$, $\alpha_* = \alpha_{-0}$.

A: $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$

Easy comparisons show the following lemma.

Lemma 4.4.6 *If* $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$,

$$\alpha_{min} \leq \alpha_{-0} \leq \alpha_{max} < 1, \quad \alpha_0 \leq \alpha_{00}, \quad \alpha_{min} \leq \alpha_{-00}.$$

Proof: See the proof in Appendix VIII. ■

By Lemma 4.4.6, we know that $\alpha_{-0} \leq \alpha_0 \leq \alpha_{00}$. According to the different possible positions of α_0, we have the following situations.

(1) $\alpha_{-0} \leq \alpha_0 \leq \alpha_{max}$.

Lemma 4.4.7 *If* $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$,

$$N_2 \geq N_{high} \Longrightarrow \alpha_{-0} \leq \alpha_0 \leq \alpha_{max},$$

where

$$N_{high} = P(1-\rho_{XV}^2) + N_1 + \frac{[P(1-\rho_{XV}^2)+N_1]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}. \tag{4.66}$$

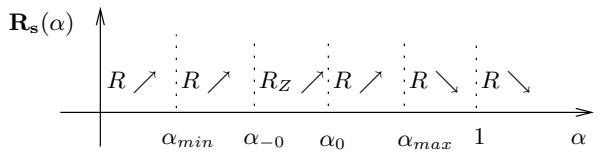


Figure 4.14: $R_s(\alpha)$ when $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$ and $N_2 \geq N_{high}$.

Proof: See the proof in Appendix X. ■

As shown in Figure 4.14, the maximal achievable secret rate in this case is $R(\alpha_{max})$.

The achievable rate equivocation region in this case is shown in Figure 4.13 (a).

(2) $\alpha_{max} \leq \alpha_0 \leq 1$.

Lemma 4.4.8 *If* $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$,

$$N_{low} \leq N_2 \leq N_{high} \Longrightarrow \alpha_{max} \leq \alpha_0 \leq 1,$$

where N_{high} *is defined in (4.66) and*

$$N_{low} = P(1-\rho_{XV}^2) - N_1 + \frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}. \tag{4.67}$$

Proof: See the proof in Appendix XI. ■

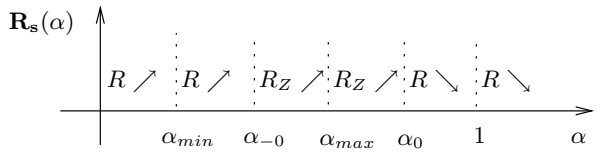


Figure 4.15: $R_s(\alpha)$ when $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$ and $N_{low} \leq N_2 \leq N_{high}$.

As shown in Figure 4.15, the maximal achievable secret rate in this case is $R_Z(\alpha_0)$.

The achievable rate equivocation region in this case is shown in Figure 4.13 (b). The curve which bounds the region can be divided into two parts. The first part is the line $d = 1$ as R goes from 0 to $R_Z(\alpha_0)$. The second part is the curve $Rd = R_Z(\alpha)$ as R goes from $R_Z(\alpha_0)$ to $R(\alpha_{max})$. Note that $R_Z(\alpha_0) = R(\alpha_0)$. Correspondingly, α, the parameter used to achieve (R, d) on the curve, goes from α_0 to α_{max}. The property of the curve follows immediately from the fact that $R_Z(\alpha)$ is non-increasing as α goes from α_0 to α_{max}.

(3) $\alpha_0 \geq 1$.

Lemma 4.4.9 *If* $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$,

$$N_2 \leq N_{low} \Longrightarrow \alpha_0 \geq 1,$$

where N_{low} *is defined in (4.67).*

Proof: See the proof in Appendix XII. ■

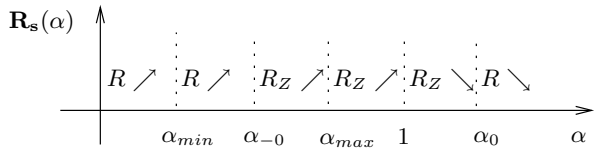


Figure 4.16: $R_s(\alpha)$ when $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$ and $N_2 \leq N_{low}$.

As shown in Figure 4.16, the maximal achievable secret rate in this case is $R_Z(1)$. The achievable rate equivocation region in this case is shown in Figure 4.13 (c). The curve which bounds the region can be divided into three parts. The first part is the line $d = 1$ as R goes from 0 to $R_Z(1)$. The second part is the curve $Rd = R_Z(1)$ as R goes from $R_Z(1)$ to $R(1)$. This part is achieved by time sharing the two rate equivocation pairs $(R_Z(1), 1)$ and $(R(1), \frac{R_Z(1)}{R(1)})$. Note that $R_Z(1)$ is a constant. The third part is the curve $Rd = R_Z(\alpha)$ as R goes from $R(1)$ to $R(\alpha_{max})$. Correspondingly, α, the parameter used to achieve (R, d) on the curve, goes from 1 to α_{max}. The property of the curve follows immediately from the fact that $R_Z(\alpha)$ is non-increasing as α goes from 1 to α_{max}.

B: $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$

Easy comparisons show the following lemma.

Lemma 4.4.10 *If* $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$,

$$1 < \alpha_{max} \leq \alpha_0 \leq \alpha_{min}, \quad \alpha_{-00} \leq \alpha_{-0}, \quad \alpha_{00} \leq \alpha_{min}.$$

Proof: See the proof in Appendix IX. ■

By Lemma 4.4.10, we know that $\alpha_{-00} \leq \alpha_{-0} \leq \alpha_0$. According to the different possible positions of α_{-0}, we have the following situations.

(1) $\alpha_{max} \leq \alpha_{-0} \leq \alpha_0$.

Lemma 4.4.11 *If* $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$,

$$N_2 \geq N_{high} \Longrightarrow \alpha_{max} \leq \alpha_{-0} \leq \alpha_0,$$

where N_{high} *is defined in (4.66).*

Proof: See the proof in Appendix XIII. ■

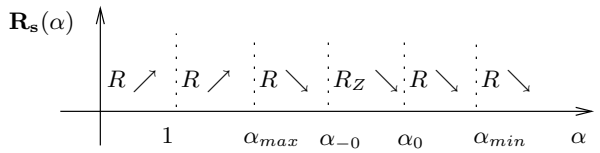


Figure 4.17: $R_s(\alpha)$ when $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$ and $N_2 \geq N_{high}$.

As shown in Figure 4.17, the maximal achievable secret rate in this case is $R(\alpha_{max})$.
The achievable rate equivocation region in this case is shown in Figure 4.13 (a).

(2) $1 \leq \alpha_{-0} \leq \alpha_{max}$.

Lemma 4.4.12 *If* $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$,

$$N_{low} \leq N_2 \leq N_{high} \Longrightarrow 1 \leq \alpha_{-0} \leq \alpha_{max}.$$

where N_{high} *and* N_{low} *are defined in (4.66) and (4.67), respectively.*

Proof: See the proof in Appendix XIV. ■

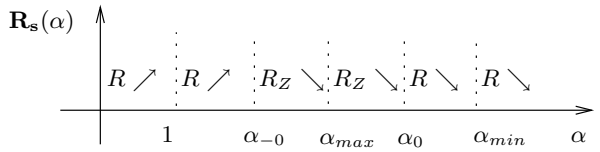


Figure 4.18: $R_s(\alpha)$ when $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$ and $N_{low} \leq N_2 \leq N_{high}$.

As shown in Figure 4.18, the maximal achievable secret rate in this case is $R_Z(\alpha_{-0})$.
The achievable rate equivocation region in this case is shown in Figure 4.13 (b). The curve which bounds the region can be divided into two parts. The first part is the line $d = 1$ as R goes from 0 to $R_Z(\alpha_0)$. The second part is the curve $Rd = R_Z(\alpha)$ as R goes from $R_Z(\alpha_{-0})$ to $R(\alpha_{max})$. Note that $R_Z(\alpha_{-0}) = R(\alpha_{-0})$. Correspondingly, α, the parameter used to achieve (R, d) on the curve, goes from α_{-0} to α_{max}. The property of the curve follows immediately from the fact that $R_Z(\alpha)$ is non-increasing as α goes from α_{-0} to α_{max}.

(3) $\alpha_{-0} \leq 1$.

Lemma 4.4.13 *If* $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$,

$$N_2 \leq N_{low} \Longrightarrow \alpha_{-0} \leq 1.$$

where N_{low} *is define in (4.67).*

Proof: See the proof in Appendix XV. ■

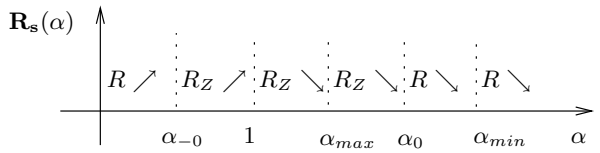


Figure 4.19: $R_s(\alpha)$ when $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$ and $N_2 \leq N_{low}$.

As shown in Figure 4.19, the maximal achievable secret rate in this case is $R_Z(1)$.
The achievable rate equivocation region in this case is shown in Figure 4.13 (c). The curve which bounds the region can be divided into three parts. The first part is the line $d = 1$ as R goes from 0 to $R_Z(1)$. The second part is the curve $Rd = R_Z(1)$ as R goes from $R_Z(1)$ to $R(1)$. This part is achieved by time sharing the two rate equivocation pairs $(R_Z(1), 1)$ and $(R(1), \frac{R_Z(1)}{R(1)})$. Note that $R_Z(1)$ is a constant. The third part is the curve $Rd = R_Z(\alpha)$ as R goes from $R(1)$ to

$R(\alpha_{max})$. Correspondingly, α, the parameter used to achieve (R, d) on the curve, goes from 1 to α_{max}. The property of the curve follows immediately from the fact that $R_Z(\alpha)$ is non-increasing as α goes from 1 to α_{max}.

C: $\sqrt{P}\rho_{XV} + \sqrt{Q} = 0$

Assume that the values of P and Q satisfy $P \geq Q$ so that the equality $\sqrt{P}\rho_{XV} + \sqrt{Q} = 0$ may exist. Taking $\rho_{XV} = -\frac{\sqrt{Q}}{\sqrt{P}}$, we could simplify the expressions of $\alpha_{max}, \alpha_{-0}, \alpha_0, \alpha_{-00}$ and α_{00} as follows:

$$\begin{aligned}
\alpha_{max} &= 1; \\
\alpha_{-0} &= 1 - \frac{(P-Q)}{\sqrt{Q(P-Q+N_1+N_2)}}; \\
\alpha_0 &= 1 + \frac{(P-Q)}{\sqrt{Q(P-Q+N_1+N_2)}}; \\
\alpha_{-00} &= 1 - \frac{(P-Q)}{\sqrt{Q(P-Q+N_1)}}; \\
\alpha_{00} &= 1 + \frac{(P-Q)}{\sqrt{Q(P-Q+N_1)}}.
\end{aligned}$$

We can also simplify the expressions of $R(\alpha_{max})$ and $R_Z(1)$ as:

$$R(\alpha_{max}) = \frac{1}{2}\log(1 + \frac{P-Q}{N}); \tag{4.68}$$

$$R_Z(1) = \frac{1}{2}\log\frac{(P-Q+N_1)(N_1+N_2)}{(P-Q+N_1+N_2)N_1}. \tag{4.69}$$

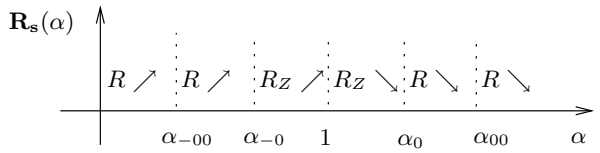


Figure 4.20: $R_s(\alpha)$ when $P \geq Q$ and $\sqrt{P}\rho_{XV} + \sqrt{Q} = 0$.

It is easy to verify that in this case, $\alpha_{-00} \leq \alpha_{-0} \leq 1 \leq \alpha_0 \leq \alpha_{00}$. As shown in Figure 4.20, the maximal achievable secret rate in this case is $R_Z(1)$.

In this case, the achievable rate equivocation region is a degraded version of Figure 4.13 (c). The curve $Rd = R_Z(\alpha)$ is degenerated to one point, since $R(\alpha_{max}) = R(1)$. The curve $Rd = R_Z(1)$ gives a bound on the rate equivocation. Note that $R_Z(1)$ is a constant. In fact, this rate equivocation region is equivalent to the region of the corresponding Gaussian wiretap channel channel with power constraint $P - Q$ at the transmitter. However, in this case, the rate does not reach the channel capacity and the secret rate is also smaller than the secrecy capacity. The reason is that the transmitter always give some power out to cancel the side information.

4.4.4 Discussion

As a result of our analysis in last subsection, if we define

$$R(\alpha_*) = \begin{cases} R(\alpha_0) & \text{if } \sqrt{P}\rho_{XV} + \sqrt{Q} > 0 \\ R(\alpha_{-0}) & \text{if } \sqrt{P}\rho_{XV} + \sqrt{Q} < 0 \end{cases}, \tag{4.70}$$

then we have the following theorems.

Theorem 4.4.14 *For the Gaussian wiretap channel with side information, when the correlation coefficient of X and V is ρ_{XV}, then the following rate is achievable at perfect secrecy:*

$$R_s = \begin{cases} R(\alpha_{max}) & N_2 \geq N_{high} \\ R(\alpha_*) & N_{low} \leq N_2 \leq N_{high} \\ R_Z(1) & N_2 \leq N_{low} \end{cases}. \tag{4.71}$$

Theorem 4.4.15 *For the Gaussian wiretap channel with side information, when the correlation coefficient of X and V is ρ_{XV}, a rate equivocation pair is achievable if*

$$\begin{aligned} R &\leq R(\alpha_{max}) \\ d &\leq 1 \end{aligned}$$

$$Rd \leq \begin{cases} R & & N_2 \geq N_{high} \\ \begin{cases} R & R \leq R(\alpha_*) \\ R_Z(\alpha) & R(\alpha_*) \leq R \leq R(\alpha_{max}) \end{cases} & & N_{low} \leq N_2 \leq N_{high} \\ \begin{cases} R & R \leq R_Z(1) \\ R_Z(1) & R_Z(1) \leq R \leq R(1) \\ R_Z(\alpha) & R(1) \leq R \leq R(\alpha_{max}) \end{cases} & & N_2 \leq N_{low} \end{cases}. \tag{4.72}$$

Denote the set of above achievable rate equivocation pair as $\mathcal{R}_{\rho_{XV}}$. For the Gaussian wiretap channel with side information, we give an achievable rate equivocation region $\mathcal{R}$ as follows:

$$\mathcal{R} = \bigcup_{\rho_{XV} \in [-1,1]} \mathcal{R}_{\rho_{XV}}. \tag{4.73}$$

Note that the region $\mathcal{R}_{\rho_{XV}=0}$ is exactly $\mathcal{R}_\perp$, the one given in Theorem 4.2.10. In Figure 4.21, we give an example that $\mathcal{R}_\perp$ is a proper subset of $\mathcal{R}$. Recall the capacity region $\mathcal{R}_L$ given by Leung-Yan-Cheong and Hellman [4, Theorem 1], for the corresponding Gaussian wiretap channel without side information. Here we define $\mathcal{R}_L^{'}$ to be the capacity region for the Gaussian wiretap channel with power constraint $P + Q + 2\sqrt{PQ}$, i.e.,

$$R \leq C_M, \quad d \leq 1, \quad Rd \leq \frac{1}{2}\log\frac{(P+Q+2\sqrt{PQ}+N_1)(N_1+N_2)}{(P+Q+2\sqrt{PQ}+N_1+N_2)N_1}.$$

Clearly, $\mathcal{R}_L^{'}$ is an outer bound of $\mathcal{R}$. As we see in Figure 4.21, we have

$$\mathcal{R}_L \subset \mathcal{R}_\perp \subset \mathcal{R} \subset \mathcal{R}_L^{'},$$

which shows that side information helps to get larger rate equivocation region of the Gaussian wiretap channel; Furthermore, for a given wiretap channel with side information, we can get a rate equivocation region $\mathcal{R}$ larger than $\mathcal{R}_\perp$ by applying the generalized Costa's

strategy in the encoding scheme; At last, $\mathcal{R}_L^{'}$ gives an outer bound of the capacity region of the Gaussian wiretap channel with side information.

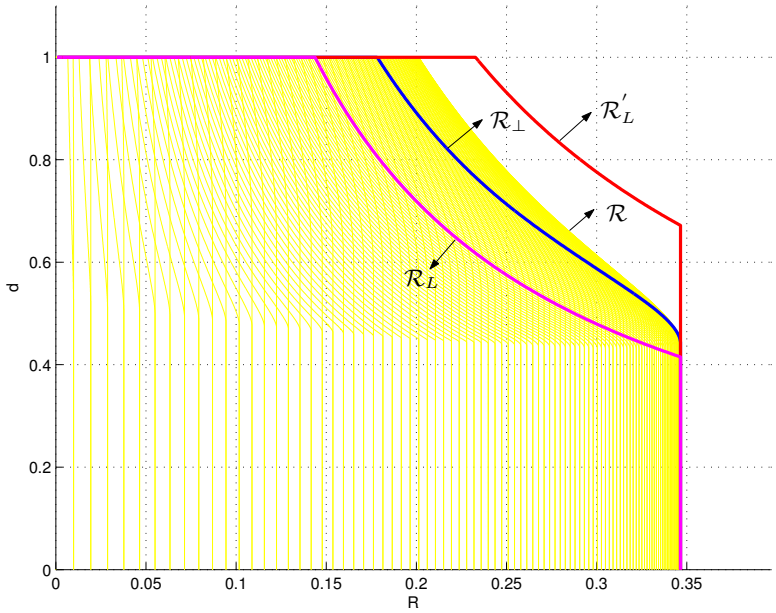


Figure 4.21: (R, d) region when $Q = 1, P = N_1 = N_2 = 10$.

Given a wiretap channel, the maximal secret rate $\max_{\rho_{XV}} R_s$ is of considerable interest. We try to find the optimum correlation coefficient of X and V to send the information as efficient as possible at the perfect secrecy. In order to use Theorem 4.4.14 for this purpose, We give the following lemata to show the properties of N_{low}, N_{high}, $R(\alpha_{max})$, $R_Z(1)$ and $R(\alpha_*)$ with respect to ρ_{XV}.

Lemma 4.4.16 *N_{low}, which is defined in (4.67), with respect to ρ_{XV} has the following properties:*

(a) when $P = Q$, N_{low} is decreasing as $-1 \leq \rho_{XV} \leq 1$;

(b) when $P > Q$, N_{low} is increasing as $-1 \leq \rho_{XV} \leq -\frac{\sqrt{Q}}{\sqrt{P}}$ and decreasing as $-\frac{\sqrt{Q}}{\sqrt{P}} \leq \rho_{XV} \leq 1$;

(c) when $P < Q$, N_{low} is increasing as $-1 \leq \rho_{XV} \leq \delta_0$ and decreasing as $\delta_0 \leq \rho_{XV} \leq 1$, where

$$\delta_0 = \frac{2\sqrt{6}}{3}\sqrt{\frac{Q-P}{P}}\cos\frac{\theta-\pi}{3} - \sqrt{\frac{Q}{P}}, \qquad \theta = \arccos\frac{3\sqrt{6}}{8}\sqrt{\frac{Q-P}{Q}}.$$

Proof: See the proof in Appendix XVIII. ■

Lemma 4.4.17 *N_{high}, which is defined in (4.66), with respect to ρ_{XV} has the following properties:*

(a) when $P = Q$, N_{high} is decreasing as $-1 \leq \rho_{XV} \leq 1$;

(b) *when* $P > Q$, N_{high} *is increasing as* $-1 \leq \rho_{XV} \leq -\frac{\sqrt{Q}}{\sqrt{P}}$ *and decreasing as* $-\frac{\sqrt{Q}}{\sqrt{P}} \leq \rho_{XV} \leq 1$;

(c) *when* $P < Q$, *if* $N_1 \geq \sqrt[4]{P}(\sqrt[4]{P}+\sqrt[4]{Q})(\sqrt{Q}-\sqrt{P})$, N_{high} *is increasing as* $-1 \leq \rho_{XV} \leq \delta_{00}$ *and decreasing as* $\delta_{00} \leq \rho_{XV} \leq 1$; *otherwise,* N_{high} *is decreasing as* $-1 \leq \rho_{XV} \leq 1$. *Here*

$$\delta_{00} = \frac{2\sqrt{6}}{3}\sqrt{\frac{Q-P-N_1}{P}}\cos\frac{\phi-\pi}{3} - \sqrt{\frac{Q}{P}}, \qquad \phi = \arccos\frac{3\sqrt{6}}{8}\sqrt{\frac{Q-P-N_1}{Q}}.$$

Proof: See the proof in Appendix XIX. ■

Given a wiretap channel, when $N_2 \leq \max_{\rho_{XV}} N_{low}$, let δ_1 be the correlation coefficient satisfying $N_2 = N_{low}|_{\rho_{XV}=\delta_1}$. If there are two solutions to $N_2 = N_{low}|_{\rho_{XV}}$, let δ_1 be the larger one and δ_1^- be the smaller one. Similarly, when $N_2 \geq \min_{\rho_{XV}} N_{high}$, let δ_2 be the only correlation coefficient or the larger solution to $N_2 = N_{high}|_{\rho_{XV}}$. If there are two solutions, let δ_2^- be the smaller one.

Lemma 4.4.18 $R(\alpha_{max})$, $R_Z(1)$ *and* $R(\alpha_*)$ *with respect to* ρ_{XV} *have the following properties:*

(a) $R(\alpha_{max})$ *is increasing as* $-1 \leq \rho_{XV} \leq 0$; *decreasing as* $0 \leq \rho_{XV} \leq 1$; *maximized at* $\rho_{XV} = 0$.

(b) $R_Z(1)$ *is increasing as* $-1 \leq \rho_{XV} \leq 1$.

(c) $R(\alpha_*)$ *satisfies the following inequalities.*

$$\begin{aligned}
R(\alpha_0)|_{\rho_{XV}} &\leq R(\alpha_0)|_{\rho_{XV}=\delta_1} && \text{if } \rho_{XV} \leq \delta_1,\\
R(\alpha_0)|_{\rho_{XV}} &\leq R(\alpha_0)|_{\rho_{XV}=\delta_2} && \text{if } |\rho_{XV}| \geq \delta_2,\\
R(\alpha_{-0})|_{\rho_{XV}} &\leq R(\alpha_{-0})|_{\rho_{XV}=\delta_2^-} && \text{if } -1 \leq \rho_{XV} \leq \delta_2^- < -\sqrt{Q}/\sqrt{P},\\
R(\alpha_{-0})|_{\rho_{XV}} &\leq R(\alpha_{-0})|_{\rho_{XV}=\delta_1^-} && \text{if } -1 \leq \rho_{XV} \leq \delta_1^- < -\sqrt{Q}/\sqrt{P}.
\end{aligned}$$

In particular,

$$\begin{aligned}
R(\alpha_0)|_{\rho_{XV}=\delta_1} &= R_Z(1)|_{\rho_{XV}=\delta_1}, & R(\alpha_0)|_{\rho_{XV}=\delta_2} &= R(\alpha_{max})|_{\rho_{XV}=\delta_2},\\
R(\alpha_{-0})|_{\rho_{XV}=\delta_1^-} &\leq R(\alpha_0)|_{\rho_{XV}=\delta_1}, & R(\alpha_{-0})|_{\rho_{XV}=\delta_2^-} &\leq R(\alpha_0)|_{\rho_{XV}=\delta_2}.
\end{aligned}$$

Proof: See the proof in Appendix XX. ■

By Lemma 4.4.17, it is easy to verify that

$$\min_{\rho_{XV}} N_{high} = N_{high}|_{\rho_{XV}=1} = N_1 + \frac{N_1^2}{(\sqrt{P}+\sqrt{Q})^2}. \tag{4.74}$$

Furthermore, by Lemma 4.4.16, we could bound N_{low} as follows:

$$\max_{\rho_{XV}} N_{low} = \begin{cases} \infty & \text{if } P > Q \\ N_{low}|_{\rho_{XV}=\delta_0} & \text{if } P \leq Q \end{cases}. \tag{4.75}$$

Consider R_s with respect to ρ_{XV} as given in (4.71). As a result of our optimization on R_s over ρ_{XV}, we have the following theorem.

Theorem 4.4.19 *For the Gaussian wiretap channel with side information, the following secret rate is achievable at perfect secrecy:*

$$\max_{\rho_{XV}} R_s = \begin{cases} C_M & \text{if } N_2 \geq N_{high}|_{\rho_{XV}=0} \\ \max\limits_{\rho_{XV}\in[\delta_*,\delta']} R(\alpha_0)|_{\rho_{XV}} & \text{else,} \end{cases} \tag{4.76}$$

where

$$\delta_* = \begin{cases} -1 & \text{if } N_2 > \max\limits_{\rho_{XV}} N_{low} \\ \delta_1 & \text{else} \end{cases},$$

$$\delta' = \begin{cases} 1 & \text{if } N_2 < \min\limits_{\rho_{XV}} N_{high} \\ \delta_2 & \text{else} \end{cases}.$$

Proof: Consider the following situations.

(a) $N_2 \geq N_{high}|_{\rho_{XV}=0}$.

By Theorem 4.4.14,

$$\max_{\rho_{XV}} R_s \geq R(\alpha_{max})|_{\rho_{XV}=0} = C_M.$$

In addition that C_M is an outer bound of the secret rate R_s, so we have in this case, $\max\limits_{\rho_{XV}} R_s = C_M$.

(b) $\max\limits_{\rho_{XV}} N_{low} < N_2 < \min\limits_{\rho_{XV}} N_{high} < N_{high}|_{\rho_{XV}=0}$.

Clearly, for any $\rho_{XV} \in [-1,1]$, we have $N_{low}|_{\rho_{XV}} < N_2 < N_{high}|_{\rho_{XV}}$. Therefore, by Theorem 4.4.14, we have in this case,

$$\max_{\rho_{XV}} R_s = \max_{\rho_{XV}\in[-1,1]} R(\alpha_0)|_{\rho_{XV}}.$$

(c) $N_2 > \max\limits_{\rho_{XV}} N_{low}$ and $\min\limits_{\rho_{XV}} N_{high} \leq N_2 < N_{high}|_{\rho_{XV}=0}$.

Clearly, this situation exists only when $P \leq Q$. For any $\rho_{XV} \in [-1,1]$, we have $\sqrt{P}\rho_{XV} + \sqrt{Q} \geq 0$ and $N_2 > N_{low}|_{\rho_{XV}}$.

Suppose that there is only one $\rho_{XV} \in [-1,1]$ satisfying $N_2 = N_{high}|_{\rho_{XV}}$. Then $N_2 = N_{high}|_{\rho_{XV}=\delta_2}$. Due to $\min\limits_{\rho_{XV}} N_{high} \leq N_2 < N_{high}|_{\rho_{XV}=0}$, we have $\delta_2 > 0$. By Lemma 4.4.17, we know that if $\rho_{XV} \in [\delta_2, 1]$, then $N_2 \geq N_{high}|_{\rho_{XV}}$; if $\rho_{XV} \in [-1, \delta_2]$, then $N_2 \leq N_{high}|_{\rho_{XV}}$. Therefore, by Theorem 4.4.14, we have

$$R_s = \begin{cases} R(\alpha_{max})|_{\rho_{XV}} & \text{for } \rho_{XV} \in [\delta_2, 1] \\ R(\alpha_0)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [-1, \delta_2] \end{cases}.$$

In addition, for $\delta_2 \leq \rho_{XV} \leq 1$, by Lemma 4.4.18, $R(\alpha_{max})|_{\rho_{XV}} \leq R(\alpha_{max})|_{\rho_{XV}=\delta_2} = R(\alpha_0)|_{\rho_{XV}=\delta_2}$. So we have in this case,

$$\max_{\rho_{XV}} R_s = \max_{\rho_{XV}\in[-1,\delta_2]} R(\alpha_0)|_{\rho_{XV}}.$$

If there are two solutions $\rho_{XV} \in [-1,1]$ to the equation $N_2 = N_{high}|_{\rho_{XV}}$, then we have $N_2 = N_{high}|_{\rho_{XV}=\delta_2} = N_{high}|_{\rho_{XV}=\delta_2^-}$. Furthermore, $\delta_2 > 0 > \delta_2^-$ and $|\delta_2^-| > \delta_2$. By Lemma 4.4.17, we know that if $\rho_{XV} \in [\delta_2, 1] \cup [-1, \delta_2^-]$, then $N_2 \geq N_{high}|_{\rho_{XV}}$; if $\rho_{XV} \in [\delta_2^-, \delta_2]$, then $N_2 \leq N_{high}|_{\rho_{XV}}$. Therefore, by Theorem 4.4.14, we have

$$R_s = \begin{cases} R(\alpha_{max})|_{\rho_{XV}} & \text{for } \rho_{XV} \in [\delta_2, 1] \cup [-1, \delta_2^-] \\ R(\alpha_0)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [\delta_2^-, \delta_2] \end{cases}.$$

Note that $|\delta_2^-| > \delta_2$. By Lemma 4.4.18, for $\rho_{XV} \in [\delta_2, 1] \cup [-1, \delta_2^-]$, $R(\alpha_{max})|_{\rho_{XV}} \leq R(\alpha_{max})|_{\rho_{XV}=\delta_2} = R(\alpha_0)|_{\rho_{XV}=\delta_2}$. Thus, we have in this case,

$$\max_{\rho_{XV}} R_s = \max_{\rho_{XV} \in [\delta_2^-, \delta_2]} R(\alpha_0)|_{\rho_{XV}}.$$

However, by Lemma 4.4.18, if $-1 \leq \rho_{XV} \leq \delta_2^-$, $R(\alpha_0)|_{\rho_{XV}} \leq R(\alpha_0)|_{\rho_{XV}=\delta_2^-}$. Therefore,

$$\max_{\rho_{XV}} R_s = \max_{\rho_{XV} \in [\delta_2^-, \delta_2]} R(\alpha_0)|_{\rho_{XV}} = \max_{\rho_{XV} \in [-1, \delta_2]} R(\alpha_0)|_{\rho_{XV}}.$$

(d) $N_2 \leq \max_{\rho_{XV}} N_{low}$ and $N_2 < \min_{\rho_{XV}} N_{high} < N_{high}|_{\rho_{XV}=0}$.

Clearly, for any $\rho_{XV} \in [-1,1]$, we have $N_2 < N_{high}|_{\rho_{XV}}$.

Suppose that there is only one $\rho_{XV} \in [-1,1]$ satisfying $N_2 = N_{low}|_{\rho_{XV}}$. Then $N_2 = N_{low}|_{\rho_{XV}=\delta_1}$. Furthermore, $\delta_1 > -\frac{\sqrt{Q}}{\sqrt{P}}$. By Lemma 4.4.17, we know that if $\rho_{XV} \in [\delta_1, 1]$, then $N_2 \geq N_{low}|_{\rho_{XV}}$; if $\rho_{XV} \in [-1, \delta_1]$, then $N_2 \leq N_{low}|_{\rho_{XV}}$. Therefore, by Theorem 4.4.14, we have

$$R_s = \begin{cases} R(\alpha_0)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [\delta_1, 1] \\ R_Z(1)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [-1, \delta_1] \end{cases}.$$

Note that for $-1 \leq \rho_{XV} \leq \delta_1$, by Lemma 4.4.18, $R_Z(1)|_{\rho_{XV}} \leq R_Z(1)|_{\rho_{XV}=\delta_1} = R(\alpha_0)|_{\rho_{XV}=\delta_1}$. So we have in this case,

$$\max_{\rho_{XV}} R_s = \max_{\rho_{XV} \in [\delta_1, 1]} R(\alpha_0)|_{\rho_{XV}}.$$

If there are two solutions $\rho_{XV} \in [-1,1]$ to the equation $N_2 = N_{low}|_{\rho_{XV}}$, then we have $N_2 = N_{low}|_{\rho_{XV}=\delta_1} = N_{high}|_{\rho_{XV}=\delta_1^-}$. Furthermore, $\delta_1 > -\frac{\sqrt{Q}}{\sqrt{P}}$ and $|\delta_1^-| > \delta_1$. By Lemma 4.4.17, we know that if $\rho_{XV} \in [\delta_1, 1] \cup [-1, \delta_1^-]$, then $N_2 \geq N_{low}|_{\rho_{XV}}$; if $\rho_{XV} \in [\delta_1^-, \delta_1]$, then $N_2 \leq N_{low}|_{\rho_{XV}}$. Therefore, by Theorem 4.4.14, we have

$$R_s = \begin{cases} R(\alpha_*)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [-1, \delta_1^-] \\ R(\alpha_0)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [\delta_1, 1] \\ R_Z(1)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [\delta_1^-, \delta_1] \end{cases}$$

It is easy to verify that if $P > Q$, then $\delta_1^- < -\frac{\sqrt{Q}}{\sqrt{P}}$. Thus we have for $\rho_{XV} \in [-1, \delta_1^-]$,

$$R_s = R(\alpha_*)|_{\rho_{XV}} = \begin{cases} R(\alpha_{-0})|_{\rho_{XV}} & \text{if } P > Q \\ R(\alpha_0)|_{\rho_{XV}} & \text{else} \end{cases}.$$

Note that for $\rho_{XV} \in [-1, \delta_1^-]$, by Lemma 4.4.18, if $P > Q$, we have $R(\alpha_{-0})|_{\rho_{XV}} \leq R(\alpha_{-0})|_{\rho_{XV}=\delta_1^-} < R(\alpha_0)|_{\rho_{XV}=\delta_1}$; otherwise, $R(\alpha_0)|_{\rho_{XV}} \leq R(\alpha_0)|_{\rho_{XV}=\delta_1}$. In addition, for $\rho_{XV} \in [\delta_1^-, \delta_1]$, $R_Z(1)|_{\rho_{XV}} \leq R_Z(1)|_{\rho_{XV}=\delta_1} = R(\alpha_0)|_{\rho_{XV}=\delta_1}$. Therefore, in this case, we have

$$\max_{\rho_{XV}} R_s = \max_{\rho_{XV} \in [\delta_1, 1]} R(\alpha_0)|_{\rho_{XV}}.$$

(e) $N_2 \leq \max_{\rho_{XV}} N_{low}$ and $\min_{\rho_{XV}} \leq N_2 < N_{high}|_{\rho_{XV}=0}$.

First, we consider the case if there is only one solution δ_1 to $N_2 = N_{low}|_{\rho_{XV}}$ and one solution δ_2 to $N_2 = N_{high}|_{\rho_{XV}}$. Then $\delta_2 > \delta_1 > -\frac{\sqrt{Q}}{\sqrt{P}}$. By Lemma 4.4.16 and Lemma 4.4.17, we know that if $\rho_{XV} \in [-1, \delta_1]$, then $N_2 \leq N_{low}|_{\rho_{XV}}$; if $\rho_{XV} \in [\delta_1, \delta_2]$, then $N_{low}|_{\rho_{XV}} \leq N_2 \leq N_{high}|_{\rho_{XV}}$; if $\rho_{XV} \in [\delta_2, 1]$, then $N_2 \geq N_{high}|_{\rho_{XV}}$. Therefore, by Theorem 4.4.14 and Lemma 4.4.18, we have

$$R_s = \begin{cases} R_Z(1)|_{\rho_{XV}} \leq R_Z(1)|_{\rho_{XV}=\delta_1} & \text{for } \rho_{XV} \in [-1, \delta_1] \\ R(\alpha_0)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [\delta_1, \delta_2] \\ R(\alpha_{max})|_{\rho_{XV}} \leq R(\alpha_{max})|_{\rho_{XV}=\delta_2} & \text{for } \rho_{XV} \in [\delta_2, 1] \end{cases}$$

In addition, by Lemma 4.4.18, $R(\alpha_0)|_{\rho_{XV}=\delta_1} = R_Z(1)|_{\rho_{XV}=\delta_1}$ and $R(\alpha_0)|_{\rho_{XV}=\delta_2} = R(\alpha_{max})|_{\rho_{XV}=\delta_2}$. Therefore, in this case, we have

$$\max_{\rho_{XV}} R_s = \max_{\rho_{XV} \in [\delta_1, \delta_2]} R(\alpha_0)|_{\rho_{XV}}.$$

Secondly, we consider the case if there are two solutions δ_1^- and δ_1 to $N_2 = N_{low}|_{\rho_{XV}}$ and one solution δ_2 to $N_2 = N_{high}|_{\rho_{XV}}$. It is easy to verify that $\delta_1^- < \delta_1 < \delta_2$. By Lemma 4.4.16, we know that if $\rho_{XV} \in [\delta_1, 1] \cup [-1, \delta_1^-]$, then $N_2 \geq N_{low}|_{\rho_{XV}}$; if $\rho_{XV} \in [\delta_1^-, \delta_1]$, then $N_2 \leq N_{low}|_{\rho_{XV}}$. By Lemma 4.4.17, we know that if $\rho_{XV} \in [\delta_2, 1]$, then $N_2 \geq N_{high}|_{\rho_{XV}}$; if $\rho_{XV} \in [-1, \delta_2]$, then $N_2 \leq N_{high}|_{\rho_{XV}}$. Therefore, by Theorem 4.4.14 and Lemma 4.4.18, we have

$$R_s = \begin{cases} R(\alpha_*)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [-1, \delta_1^-] \\ R_Z(1)|_{\rho_{XV}} \leq R_Z(1)|_{\rho_{XV}=\delta_1} & \text{for } \rho_{XV} \in [\delta_1^-, \delta_1] \\ R(\alpha_0)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [\delta_1, \delta_2] \\ R(\alpha_{max})|_{\rho_{XV}} \leq R(\alpha_{max})|_{\rho_{XV}=\delta_2} & \text{for } \rho_{XV} \in [\delta_2, 1] \end{cases}$$

It is easy to verify that if $P > Q$, then $\delta_1^- < -\frac{\sqrt{Q}}{\sqrt{P}}$. Thus we have for $\rho_{XV} \in [-1, \delta_1^-]$,

$$R_s = R(\alpha_*)|_{\rho_{XV}} = \begin{cases} R(\alpha_{-0})|_{\rho_{XV}} & \text{if } P > Q \\ R(\alpha_0)|_{\rho_{XV}} & \text{else} \end{cases}.$$

Note that when $\rho_{XV} \in [-1, \delta_1^-]$, by Lemma 4.4.18, if $P > Q$, we have $R(\alpha_{-0})|_{\rho_{XV}} \leq R(\alpha_{-0})|_{\rho_{XV}=\delta_1^-} < R(\alpha_0)|_{\rho_{XV}=\delta_1}$; otherwise, $R(\alpha_0)|_{\rho_{XV}} \leq R(\alpha_0)|_{\rho_{XV}=\delta_1}$. In addition, $R(\alpha_0)|_{\rho_{XV}=\delta_1} = R_Z(1)|_{\rho_{XV}=\delta_1}$, $R(\alpha_0)|_{\rho_{XV}=\delta_2} = R(\alpha_{max})|_{\rho_{XV}=\delta_2}$. Therefore, in this case, we have

$$\max_{\rho_{XV}} R_s = \max_{\rho_{XV} \in [\delta_1, \delta_2]} R(\alpha_0)|_{\rho_{XV}}.$$

At last, we consider the case if there are two solutions δ_1^- and δ_1 to $N_2 = N_{low}|_{\rho_{XV}}$ and two solutions δ_2^- and δ_2 to $N_2 = N_{high}|_{\rho_{XV}}$. It is easy to verify that $\delta_2^- < \delta_1^- < \delta_1 < \delta_2$. By Lemma 4.4.16, we know that if $\rho_{XV} \in [\delta_1, 1] \cup [-1, \delta_1^-]$, then $N_2 \geq N_{low}|_{\rho_{XV}}$; if $\rho_{XV} \in [\delta_1^-, \delta_1]$, then $N_2 \leq N_{low}|_{\rho_{XV}}$. By Lemma 4.4.17, we know that if $\rho_{XV} \in [\delta_2, 1] \cup [-1, \delta_2^-]$, then $N_2 \geq N_{high}|_{\rho_{XV}}$; if $\rho_{XV} \in [-1, \delta_2]$, then $N_2 \leq N_{high}|_{\rho_{XV}}$. Therefore, by Theorem 4.4.14 and Lemma 4.4.18, we have

$$R_s = \begin{cases} R(\alpha_*)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [\delta_2^-, \delta_1^-] \\ R_Z(1)|_{\rho_{XV}} \leq R_Z(1)|_{\rho_{XV}=\delta_1} & \text{for } \rho_{XV} \in [\delta_1^-, \delta_1] \\ R(\alpha_0)|_{\rho_{XV}} & \text{for } \rho_{XV} \in [\delta_1, \delta_2] \\ R(\alpha_{max})|_{\rho_{XV}} \leq R(\alpha_{max})|_{\rho_{XV}=\delta_2} & \text{for } \rho_{XV} \in [-1, \delta_2^-] \cup [\delta_2, 1] \end{cases}$$

It is easy to verify that if $P > Q$, then $\delta_1^- < -\frac{\sqrt{Q}}{\sqrt{P}}$. Thus we have for $\rho_{XV} \in [\delta_2^-, \delta_1^-]$,

$$R_s = R(\alpha_*)|_{\rho_{XV}} = \begin{cases} R(\alpha_{-0})|_{\rho_{XV}} & \text{if } P > Q \\ R(\alpha_0)|_{\rho_{XV}} & \text{else} \end{cases}.$$

Note that when $\rho_{XV} \in [\delta_2^-, \delta_1^-]$, by Lemma 4.4.18, if $P > Q$, we have $R(\alpha_{-0})|_{\rho_{XV}} \leq R(\alpha_{-0})|_{\rho_{XV}=\delta_1^-} < R(\alpha_0)|_{\rho_{XV}=\delta_1}$; otherwise, $R(\alpha_0)|_{\rho_{XV}} \leq R(\alpha_0)|_{\rho_{XV}=\delta_1}$. In addition, $R(\alpha_0)|_{\rho_{XV}=\delta_1} = R_Z(1)|_{\rho_{XV}=\delta_1}$, $R(\alpha_0)|_{\rho_{XV}=\delta_2} = R(\alpha_{max})|_{\rho_{XV}=\delta_2}$. Therefore, in this case, we have

$$\max_{\rho_{XV}} R_s = \max_{\rho_{XV} \in [\delta_1, \delta_2]} R(\alpha_0)|_{\rho_{XV}}.$$

■

From the above theorem, it is clear that if $N_2 \geq N_{high}|_{\rho_{XV}=0}$, the optimum correlation coefficient is $\rho_{XV} = 0$. Otherwise, when $N_2 < N_{high}|_{\rho_{XV}=0}$, the optimal choice of ρ_{XV} is the one between δ_* and $\delta^{'}$ which maximizes $R(\alpha_0)$.

In the following we will give an example to show that $\rho_{XV} = 0$ is not always the best choice to obtain high rate at perfect secrecy. Assume that N_2 is relatively small so that $N_2 < N_{low}|_{\rho_{XV}=0}$. If we choose X independent of V, then the maximal rate at perfect secrecy is

$$R_Z(1)|_{\rho_{XV}=0} = \frac{1}{2} \log \frac{(P + Q + N_1)(N_1 + N_2)}{(P + Q + N_1 + N_2)N_1}.$$

However, since $N_2 < N_{low}|_{\rho_{XV}=0}$, there is a $\delta > 0$ such that $N_2 = N_{low}|_{\rho_{XV}=\delta}$. If we choose X dependent on V, say that the correlation coefficient of X and V is δ, then we can achieve $R_Z(1)|_{\rho_{XV}=\delta}$ at perfect secrecy. It is clear that

$$\begin{aligned} R_Z(1)|_{\rho_{XV}=\delta} &= \frac{1}{2} \log \frac{(P + Q + 2\sqrt{PQ}\delta + N_1)(N_1 + N_2)}{(P + Q + 2\sqrt{PQ}\delta + N_1 + N_2)N_1} \\ &> R_Z(1)|_{\rho_{XV}=0}. \end{aligned}$$

Therefore, in this case, it is a better choice to choose X dependent on V.

In Figure 4.22, we illustrate the performance of R_s with respect to ρ_{XV} when $Q = 1, P = N_1 = 10$. As we see, when $N_2 = 10$, the secret rate 0.17 nats can be achieved at $\rho_{XV} = 0.5$. Comparing with the secret rate 0.15 nats achieved at $\rho_{XV} = 0$, we gain more than 10% efficiency.

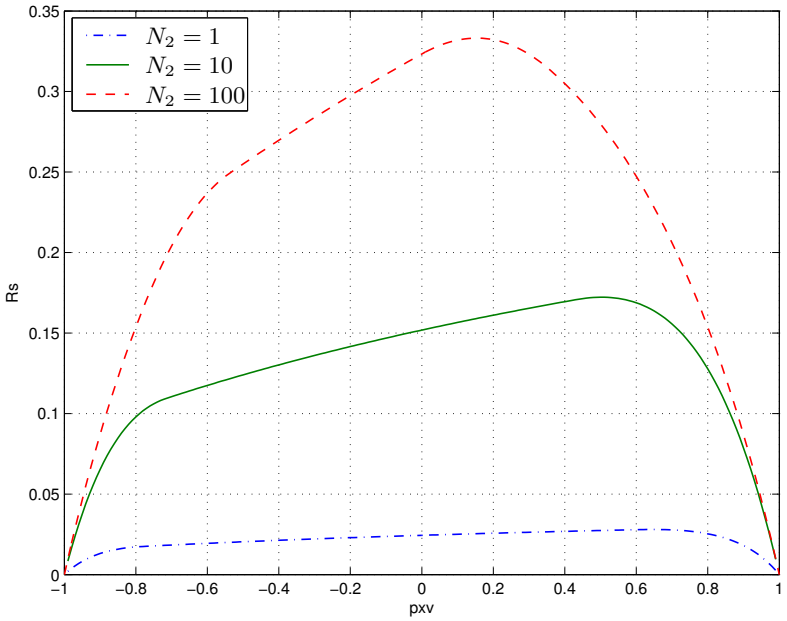


Figure 4.22: R_s w.r.t ρ_{XV} when $Q = 1, P = N_1 = 10$.

4.5 Concluding remarks

In [7], Costa showed that for the dirty paper channel, to choose X independent of the side information V is a best choice to yield the optimal efficiency by dirty paper coding. However, for the Gaussian wiretap channel with side information, as shown in last section, it is not always true. Especially in the case that the noise of wiretap channel is relatively small, to choose X dependent on the side information V can be a better choice, in order to achieve a higher efficiency to the legitimate receiver at a certain security level from the wiretapper. In addition, we give the best choice of the correlation coefficient for the generalized Costa's strategy to achieve the maximal rate at the perfect secrecy.

For the Gaussian wiretap channel with side information, the achievable rate equivocation region is more complicated than that for the Gaussian wiretap channel where the side information is absent. In Section 4.2, we have shown that for the Gaussian wiretap channel, side information helps to achieve a larger secrecy capacity and a larger capacity region. Using the method similar to Costa [7], we derive the region $\mathcal{R}_\perp$ which is better than the one given by Mitrpant in [8, Theorem 4.4] or [9, Theorem 3]. Furthermore, we improve the region $\mathcal{R}_\perp$ by applying the generalized Costa's strategy. However, it still remains an open problem whether $\mathcal{R}$ is the capacity region of the Gaussian wiretap channel with side information.

Chapter 5

Random Linear Code for the Wiretap Channel

5.1 Introduction

The problem of developing forward coding schemes for secure communication over the wiretap channel has not received much attention. Code construction methods and their connection to security have not been explored extensively so far. A basic example introduced by Wyner [1] is only for the wiretap channel with a noiseless main channel and a binary symmetric wiretap channel. The model is shown in Figure 5.1. Another example is given by Thangaraj et al. [22] for the situation when the main channel is noiseless and the wiretap channel is a binary erasure channel.

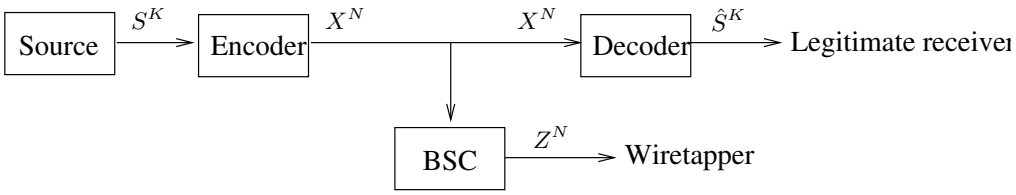


Figure 5.1: Wyner wiretap channel with a noiseless main channel and a binary symmetric wiretap channel.

In this chapter, we focus on the problem of developing coding schemes with linear code for secure communication across the wiretap channel. We consider the specific case that both the main channel and the wiretap channel are binary symmetric. The model is shown in Figure 5.3. It is equivalent to the model shown in Figure 5.2, in the manner that the overall wiretap channel is more noisy than the main channel. This chapter is broadly divided into two parts. In the first part, we provide a proof to show that secrecy capacity could be achieved by using random linear codes. In the second part, we investigate the performance of the coding schemes when linear codes are used in the construction.

5.2 Model description

We consider the situation as given in Figure 5.3. Suppose that all alphabets of the source, the channel input and the channel output are equal to $\{0, 1\}$. Source S satisfies $\Pr\{S =$

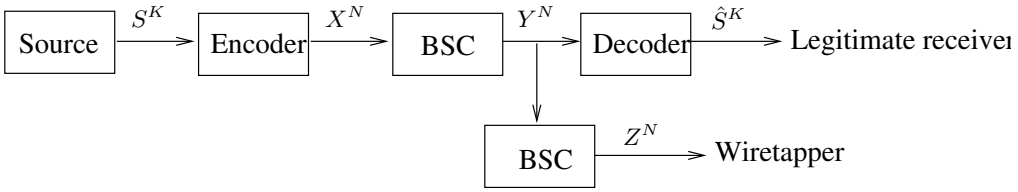


Figure 5.2: Wyner wiretap channel when both main channel and wiretap channel are binary symmetric.

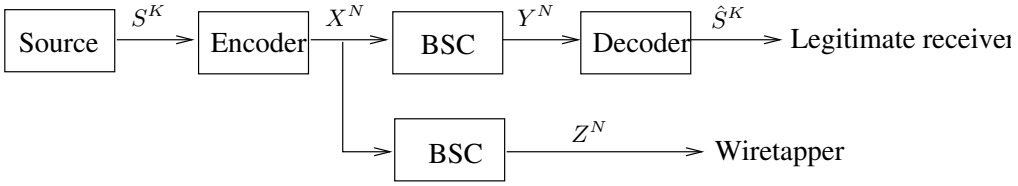


Figure 5.3: Csiszár-Körner wiretap channel when both main channel and the wiretap channel are binary symmetric, and the wiretap channel is more noisy.

$0\} = \Pr\{S = 1\} = \frac{1}{2}$. The main channel is a BSC with crossover probability p ($0 \le p \le \frac{1}{2}$) and the wiretap channel is a BSC with crossover probability p_w ($0 \le p_w \le \frac{1}{2}$ and $p_w \ge p$). The encoder encodes every K source outputs, S^K, into a codeword X^N, which is the input of the main channel. Assume that S^K is uniformly distributed, so we have $H(S^K) = K$. The outputs of the main channel and the wiretap channel are Y^N and Z^N, respectively. Let $E^N = Y^N - X^N$ and $E_w^N = Z^N - X^N$. It is clear that E^N is the noise sequence added into the main channel and E_w^N is the noise sequence added into the wiretap channel. Then, every component of E^N and E_w^N, denoted as E_i and E_{wj}, respectively, where $1 \le i, j \le N$, has the following distribution:

$$\Pr(E_i = 1) = p, \qquad \Pr(E_i = 0) = 1 - p; \tag{5.1a}$$

$$\Pr(E_{wj} = 1) = p_w, \qquad \Pr(E_{wj} = 0) = 1 - p_w. \tag{5.1b}$$

The transmission rate to the legitimate receiver is

$$R = \frac{H(S^K)}{N} = \frac{K}{N}. \tag{5.2}$$

The equivocation of the wiretapper is

$$d = \frac{H(S^K|Z^N)}{H(S^K)} = \frac{H(S^K|Z^N)}{K}. \tag{5.3}$$

At the legitimate receiver, on receipt of Y^N, the decoder makes an estimate $\hat{S}^K$ of the message S^K. Then, corresponding to a given encoder and decoder, the error probability P_e is defined to be

$$P_e = \Pr\{\hat{S}^K \ne S^K\}. \tag{5.4}$$

We refer to the above as an encoder-decoder (K, N, d, P_e).

5.3 Random linear codes to achieve secrecy capacity

The notion of the secrecy capacity has an operational meaning of being the maximum possible rate of the information transmission between the transmitter and the legitimate receiver that still enables the wiretapper to be kept totally ignorant. Thus, the coding problem to achieve the secrecy capacity of the wiretap channel involves adding redundancy for enabling the legitimate receiver to correct errors and adding randomness for keeping the wiretapper ignorant. By [1], for the model shown in Figure 5.3, the secrecy capacity is $C_s = C_M - C_{MW} = h(p_w) - h(p)$. Now we perform a random linear code to establish the achievability of the secrecy capacity. For this aim, we need to construct a random linear code (N, K, d, P_e) such that for arbitrary $\varepsilon, \zeta, \delta > 0$,

$$\begin{aligned} \frac{K}{N} &\geq h(p_w) - h(p) - \varepsilon, && \text{(5.5a)} \\ d &\geq 1 - \zeta, && \text{(5.5b)} \\ P_e &\leq \delta. && \text{(5.5c)} \end{aligned}$$

We now proceed to this task.

5.3.1 Parameter settings

First, we set up the parameters for an encoder-decoder (K, N, d, P_e). Randomly choose a binary matrix H_1 with $N - K_1$ rows and N columns. Independently, randomly choose another binary matrix H with K rows and N columns. Assume that $K \leq K_1$. Let $K_2 = K_1 - K$ and

$$\mathrm{H}_2 = \begin{bmatrix} \mathrm{H}_1 \\ \mathrm{H} \end{bmatrix}. \tag{5.6}$$

Then H_2 is a binary matrix with $N - K_2$ rows and N columns. Later in our proof we will increase N and keep K_1, K proportional to N. In order to ensure that K_1 and K are integers, for arbitrary small $\epsilon > 0$, we take

$$\begin{aligned} K_1 &= \lfloor N[1 - h(p) - 2\epsilon] \rfloor; \\ K_1 - K &= \lfloor N[1 - h(p_w) - 2\epsilon] \rfloor. \end{aligned}$$

Here $\lfloor x \rfloor$ stands for the maximal integer which is not larger than x. Straightforwardly,

$$\begin{aligned} \frac{K}{N} &= \frac{\lfloor N[1 - h(p) - 2\epsilon] \rfloor - \lfloor N[1 - h(p_w) - 2\epsilon] \rfloor}{N} \\ &\geq \frac{N[1 - h(p) - 2\epsilon] - 1 - N[1 - h(p_w) - 2\epsilon]}{N} \\ &= h(p_w) - h(p) - \frac{1}{N}. \end{aligned}$$

It is clear, for given $\varepsilon > 0$, there exists an integer $N_0 > \frac{1}{\varepsilon}$, such that when $N \geq N_0$,

$$\frac{K}{N} \geq h(p_w) - h(p) - \varepsilon.$$

In what follows, we will assume that both H_1 and H are with full rank, i.e., the rank of H_1 is $N - K_1$, and the rank of H is K. The reason is that by Lemma 5.3.1, the rows of the

H_1 and H are linear independent with probability approaching 1 as N goes to infinity. See the proof of Lemma 5.3.1 in Appendix XVI.

Lemma 5.3.1 *A randomly chosen binary matrix* H *with K rows and N columns has rank K with probability approaching 1 as N goes to infinity and $\frac{K}{N} = R$.*

Based on the assumption that H_1 and H are with full rank, H_2, as defined in the equation (5.6), has full rank with probability approaching 1 as N goes to infinity. The proof is the following:

$$\begin{aligned} & \Pr\{\mathrm{H}_2 \text{ has full rank } | \mathrm{H}_1, \mathrm{H} \text{ are with full rank}\} \\ = & \frac{\Pr\{\mathrm{H}_2 \text{ has full rank and } \mathrm{H}_1, \mathrm{H} \text{ are with full rank}\}}{\Pr\{\mathrm{H}_1, \mathrm{H} \text{ are with full rank}\}} \\ \stackrel{(a)}{=} & \frac{\Pr\{\mathrm{H}_2 \text{ has full rank}\}}{\Pr\{\mathrm{H}_1 \text{ has full rank}\} \cdot \Pr\{\mathrm{H} \text{ has full rank}\}}, \end{aligned}$$

where (a) follows from the fact that when H_2 has full rank, then its sub-matrices H_1 and H are surely with full rank; Furthermore, since H_1 and H are chosen independently, $\Pr\{\mathrm{H}_1, \mathrm{H} \text{ are with full rank}\} = \Pr\{\mathrm{H}_1 \text{ has full rank}\} \cdot \Pr\{\mathrm{H} \text{ has full rank}\}$. Now we increase N and keep K_1, K proportional to N. By Lemma 5.3.1, we have

$$\begin{aligned} & \lim_{N\to\infty} \Pr\{\mathrm{H}_2 \text{ has full rank} | \mathrm{H}_1, \mathrm{H} \text{ are with full rank}\} \\ = & \lim_{N\to\infty} \frac{\Pr\{\mathrm{H}_2 \text{ has full rank}\}}{\Pr\{\mathrm{H}_1 \text{ has full rank}\} \cdot \Pr\{\mathrm{H} \text{ has full rank}\}} \\ = & \frac{\lim_{N\to\infty} \Pr\{\mathrm{H}_2 \text{ has full rank}\}}{\lim_{N\to\infty} \Pr\{\mathrm{H}_1 \text{ has full rank}\} \cdot \lim_{N\to\infty} \Pr\{\mathrm{H} \text{ has full rank}\}} \\ = & \frac{1}{1 \cdot 1} = 1. \end{aligned}$$

Therefore, without loss of generality, we also assume that H_2 is with full rank.

Let C_1 be the dual code of the $(N, N-K_1)$ linear code generated by H_1 and C_2 be the dual code of the $(N, N-K_2)$ linear code generated by H_2. In other words, H_1 is a parity check matrix of C_1 and H_2 is a parity check matrix of C_2. To transmit a K-bit secret message s^K, an N-bit codeword x^N is sent to the channel. The corresponding output at the legitimate receiver is y^N, at the wiretapper is z^N. Because of the channel noises, y^N and z^N may be different from x^N. Let $e^N = y^N - x^N$ be the noise added into the main channel and $e_w^N = z^N - x^N$ be the noise added into the wiretap channel. Since the main channel is a BSC with crossover probability p and the wiretap channel is a BSC with crossover probability p_w, we have

$$\begin{aligned} \Pr\{E^N = e^N\} &= p^{w(e^N)}(1-p)^{N-w(e^N)}; \\ \Pr\{E_w^N = e_w^N\} &= p_w^{w(e_w^N)}(1-p_w)^{N-w(e_w^N)}, \end{aligned}$$

where $w(e^N)$ is the number of the nonzero components of e^N, also called the Hamming weight of e^N; and $w(e_w^N)$ is the Hamming weight of e_w^N.

In this chapter and also next chapter, when the dimension of a sequence is clear from the context, we will denote the sequences in boldface letters for simplicity. For example,

$\mathbf{x}$ is the sequence x^N and $\mathbf{s}$ is s^K, etc. A similar convention applies to random variables, which are denoted by upper-case letters. For example, $\mathbf{X}$ is the random variable X^N, etc.

Now let us specify the encoder. To send the secret message $\mathbf{s}$, a sequence $\mathbf{x}$ is chosen at random from the solution set of the following equation

$$\mathbf{x}\mathrm{H}_2{}^{\mathrm{T}} = \mathbf{x}\begin{bmatrix} \mathrm{H}_1 \\ \mathrm{H} \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} \mathbf{x}\mathrm{H}_1{}^{\mathrm{T}} & \mathbf{x}\mathrm{H}^{\mathrm{T}} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \mathbf{s} \end{bmatrix}, \tag{5.7}$$

where $\mathrm{H}_2{}^{\mathrm{T}}$ is the transpose of the matrix H_2; $\mathrm{H}_1{}^{\mathrm{T}}$ and H^{T} are the transposes of the matrices H_1 and H, respectively. Due to the matrix H_2 with rank $N - K_2$, the number of solutions of the above equation is 2^{K_2}. Furthermore, for different secret messages $\mathbf{s}$, the solution sets are disjoint. Note that the number of solutions of the equation $\mathbf{x}\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}$ is 2^{K_1}. So corresponding to different secret messages $\mathbf{s}$, the solutions of the equation $\mathbf{x}\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}$ is equally divided into $\frac{2^{K_1}}{2^{K_2}} = 2^K$ subsets. In other words, C_1 is equally divided into 2^K subsets corresponding to different values of $\mathbf{s}$, and C_2 is the subset of C_1 with $\mathbf{s} = \mathbf{0}$. As for the subset corresponding to a message $\mathbf{s} \neq \mathbf{0}$, we denote as $\mathbf{s} + C_2$.

In the following, we will show that the secrecy capacity can be achieved by a random linear code in two parts, the reliability: $P_e \to 0$ as $N \to \infty$; and the security: $d \to 1$ as $N \to \infty$.

5.3.2 Reliability proof

In this subsection, we will prove that $P_e \to 0$ as $N \to \infty$.

The legitimate receiver uses typical set decoder. The decoder examines the typical set $T_E^N(\epsilon)$, the set of noise sequences $\mathbf{e}$ that satisfy

$$2^{-N[h(p)+\epsilon]} \leq \Pr(\mathbf{E} = \mathbf{e}) \leq 2^{-N[h(p)-\epsilon]}.$$

Check to see if any of those typical noise sequences, $\mathbf{e}$ satisfies

$$\mathbf{e}\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{y}\mathrm{H}_1{}^{\mathrm{T}}.$$

If exactly one typical sequence $\mathbf{e}$ does so, the typical set decoder reports $\mathbf{e}$ as the hypothesized noise sequence. The secret message $\mathbf{s}$ is decoded as $\hat{\mathbf{s}} = (\mathbf{y} - \mathbf{e})\mathrm{H}^{\mathrm{T}}$. However, if no typical sequence in the set $T_E^N(\epsilon)$ matches the observed syndrome $\mathbf{y}\mathrm{H}_1{}^{\mathrm{T}}$, or more than one does, then the typical decoder reports an error.

The error probability of the typical set decoder at the legitimate receiver, can be written as follows,

$$P_e = P_T + P_{\mathrm{H}_1}, \tag{5.8}$$

where P_T is the probability that the true noise sequence is itself not typical, and P_{H_1} is the probability that the true noise sequence is typical and at least one other typical sequence clashes with it.

We first analyze P_T. For given $\epsilon > 0$ and $\delta > 0$, there exists an integer N_1, such that when $N \geq N_1$, $\Pr\{\mathbf{e} \in T_E^N(\epsilon)\} \geq 1 - \delta/2$. Therefore, when $N \geq N_1$, $P_T = 1 - \Pr\{\mathbf{e} \in T_E^N(\epsilon)\} \leq \delta/2$.

The probability P_{H_1}. Let the true noise sequence is $\mathbf{e}$. It belongs to the set $T_E^N(\epsilon)$. If any of the typical noise sequence $\mathbf{e}^*$, different from $\mathbf{e}$, satisfies $(\mathbf{e}^* - \mathbf{e})\mathrm{H}_1{}^{\mathrm{T}} = \mathbf{0}$, then we have

an error. We use the truth function

$$\mathbf{1}[(\mathbf{e}^* - \mathbf{e}){\mathrm{H}_1}^{\mathrm{T}} = \mathbf{0}], \tag{5.9}$$

whose value is one if the statement $(\mathbf{e}^* - \mathbf{e}){\mathrm{H}_1}^{\mathrm{T}} = \mathbf{0}$ is true and zero otherwise. Then when the true noise is $\mathbf{e}$, the number of such errors can be bounded as:

$$[\text{ Number of errors given } \mathbf{e} \text{ and } \mathrm{H}_1] \leq \sum_{\substack{\mathbf{e}^*:\ \mathbf{e}^* \in T_E^N(\epsilon) \\ \mathbf{e}^* \neq \mathbf{e}}} \mathbf{1}[(\mathbf{e}^* - \mathbf{e}){\mathrm{H}_1}^{\mathrm{T}} = \mathbf{0}]. \tag{5.10}$$

The number of errors is either zero or one; the sum on the right-hand side may exceed one, in case where several typical noise sequences have the same syndrome.

Now we can write down the probability P_{H_1} by averaging over $\mathbf{e}$:

$$P_{\mathrm{H}_1} \leq \sum_{\mathbf{e} \in T_E^N(\epsilon)} \Pr(\mathbf{E} = \mathbf{e}) \sum_{\substack{\mathbf{e}^*:\ \mathbf{e}^* \in T_E^N(\epsilon) \\ \mathbf{e}^* \neq \mathbf{e}}} \mathbf{1}[(\mathbf{e}^* - \mathbf{e}){\mathrm{H}_1}^{\mathrm{T}} = \mathbf{0}]. \tag{5.11}$$

We will find the average of P_{H_1}, $\bar{P}_{\mathrm{H}_1}$, by averaging over all possible H_1. By showing that $\bar{P}_{\mathrm{H}_1}$ vanishes as N approaches infinity, we will thus show that there exists a H_1 such that P_{H_1} with vanishing error probability.

We denote averaging over all possible binary matrices H_1 by $\langle \cdots \rangle_{\mathrm{H}_1}$. Then we have

$$\begin{aligned}
\bar{P}_{\mathrm{H}_1} &= \langle P_{\mathrm{H}_1} \rangle_{\mathrm{H}_1} \\
&\leq \langle \sum_{\mathbf{e} \in T_E^N(\epsilon)} \Pr(\mathbf{E} = \mathbf{e}) \sum_{\substack{\mathbf{e}^*:\ \mathbf{e}^* \in T_E^N(\epsilon) \\ \mathbf{e}^* \neq \mathbf{e}}} \mathbf{1}[(\mathbf{e}^* - \mathbf{e}){\mathrm{H}_1}^{\mathrm{T}} = \mathbf{0}] \rangle_{\mathrm{H}_1} \\
&= \sum_{\mathbf{e} \in T_E^N(\epsilon)} \Pr(E^N = \mathbf{e}) \sum_{\substack{\mathbf{e}^*:\ \mathbf{e}^* \in T_E^N(\epsilon) \\ \mathbf{e}^* \neq \mathbf{e}}} \langle \mathbf{1}[(\mathbf{e}^* - \mathbf{e}){\mathrm{H}_1}^{\mathrm{T}} = \mathbf{0}] \rangle_{\mathrm{H}_1}.
\end{aligned}$$

Since for any non-zero binary sequence $\mathbf{v}$, the probability that $\mathbf{v}{\mathrm{H}_1}^{\mathrm{T}} = 0$, averaging over all possible H_1, is $2^{-(N-K_1)}$. So

$$\begin{aligned}
\bar{P}_{\mathrm{H}_1} &\leq (\sum_{\mathbf{e} \in T_E^N(\epsilon)} \Pr(\mathbf{E} = \mathbf{e}))(|T_E^N(\epsilon)| - 1)2^{-(N-K_1)} \\
&< |T_E^N(\epsilon)|2^{-(N-K_1)} \\
&\leq 2^{N[h(p)+\epsilon]}2^{-(N-K_1)} \\
&= 2^{-N(1-h(p)-\epsilon-\frac{K_1}{N})}.
\end{aligned}$$

Note that $\frac{K_1}{N} \leq 1 - h(p) - 2\epsilon < 1 - h(p) - \epsilon$. Therefore, for given $\epsilon > 0$ and $\delta > 0$, there exists an N_2, when $N \geq N_2$, $\bar{P}_{\mathrm{H}_1} \leq \delta/8$. By Markov inequality [1], we have

$$\Pr(P_{\mathrm{H}_1} > \frac{\delta}{2}) < \frac{\bar{P}_{\mathrm{H}_1}}{\delta/2} \leq \frac{\delta/8}{\delta/2} = \frac{1}{4}.$$

[1] Let X be a nonnegative random variable. Markov inequality states that for any $a > 0$, $\Pr(X \geq a) \leq \frac{\mathrm{E}(X)}{a}$.

Thus,

$$\Pr(P_{\mathrm{H}_1} \le \frac{\delta}{2}) = 1 - \Pr(P_{\mathrm{H}_1} \ge \frac{\delta}{2}) > \frac{3}{4}.$$

That is, from all possible H_1, more than 3/4 random choices yield $P_{\mathrm{H}_1} \le \frac{\delta}{2}$.

Thus we have shown that there are H_1 such that, for given $\epsilon > 0$ and $\delta > 0$, when $N \ge \max\{N_1, N_2\}$,

$$P_e = P_T + P_{\mathrm{H}_1} \le \delta/2 + \delta/2 = \delta.$$

This concludes the proof of reliability.

5.3.3 Security proof

In this subsection, we will prove that $d \to 1$ as $N \to \infty$.

Consider the uncertainty of the secret to the wiretapper in three steps:

1. show that $H(\mathbf{S}|\mathbf{Z}) \ge N[h(p) - h(p_w)] - H(\mathbf{X}|\mathbf{S}, \mathbf{Z})$.
2. show that $H(\mathbf{X}|\mathbf{S}, \mathbf{Z}) \le h(P_{ew}) + P_{ew}K_2$. Here P_{ew} means a wiretapper's error probability to decode $\mathbf{x}$ in the case where $\mathbf{s}$ is known to the wiretapper.
3. show that for arbitrary $0 < \lambda < 1/2$, $P_{ew} \le \lambda$.

Combining the above steps, we have

$$\begin{aligned}
d &= \frac{H(\mathbf{S}|\mathbf{Z})}{H(\mathbf{S})} \\
&\ge \frac{N[h(p) - h(p_w)] - h(P_{ew}) - P_{ew}K_2}{K} \\
&\ge \frac{N[h(p) - h(p_w)] - h(\lambda) - \lambda K_2}{K} \\
&\overset{(a)}{\ge} \frac{[h(p) - h(p_w)] - \varepsilon - \lambda K_2/N}{K/N} \\
&\overset{(b)}{\ge} 1 - \frac{\varepsilon + \lambda K_2/N}{h(p) - h(p_w) - \varepsilon} \\
&\overset{(c)}{\ge} 1 - \frac{\varepsilon + \lambda(1 - h(p_w))}{h(p) - h(p_w) - \varepsilon} \\
&\overset{(d)}{\ge} 1 - \zeta.
\end{aligned}$$

where

(a) follows from the fact that $h(\lambda) \le 1$ and when $N \ge N_0$, $\varepsilon \ge \frac{1}{N}$.

(b) follows from the fact that $h(p) - h(p_w) - \varepsilon \le \frac{K}{N} \le h(p) - h(p_w)$.

(c) follows from the fact that $\frac{K_2}{N} = \frac{K_1 - K}{N} < 1 - h(p_w)$.

(d) follows from the fact that there exists $0 < \lambda < 1/2$ such that for given arbitrary small ε and ζ, $\zeta \ge \frac{\varepsilon + \lambda(1 - h(p_w))}{h(p) - h(p_w) - \varepsilon}$.

We now proceed to step 1 by considering

$$\begin{aligned}
H(\mathbf{S}|\mathbf{Z}) &= H(\mathbf{S},\mathbf{Z}) - H(\mathbf{Z}) \\
&= H(\mathbf{S},\mathbf{X},\mathbf{Z}) - H(\mathbf{X}|\mathbf{S},\mathbf{Z}) - H(\mathbf{Z}) \\
&= H(\mathbf{S},\mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{S},\mathbf{Z}) \\
&= H(\mathbf{X}|\mathbf{Z}) + H(\mathbf{S}|\mathbf{X},\mathbf{Z}) - H(\mathbf{X}|\mathbf{S},\mathbf{Z}) \\
&\overset{(a)}{=} H(\mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{S},\mathbf{Z}) \\
&\overset{(b)}{\geq} H(\mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{Y}) - H(\mathbf{X}|\mathbf{S},\mathbf{Z}) \\
&= I(\mathbf{X};\mathbf{Y}) - I(\mathbf{X};\mathbf{Z}) - H(\mathbf{X}|\mathbf{S},\mathbf{Z}) \\
&\overset{(c)}{=} N[I(X;Y) - I(X;Z)] - H(\mathbf{X}|\mathbf{S},\mathbf{Z}) \\
&= N[h(p) - h(p_w)] - H(\mathbf{X}|\mathbf{S},\mathbf{Z}),
\end{aligned}$$

where

(a) follows from the fact that $H(\mathbf{S}|\mathbf{X},\mathbf{Z}) = 0$ since $\mathbf{S} = \mathbf{X}\mathrm{H}^{\mathrm{T}}$.

(b) follows from the fact that $H(\mathbf{X}|\mathbf{Y}) \geq 0$.

(c) follows from the fact that $I(\mathbf{X};\mathbf{Y}) = I(X^N;Y^N) = NI(X;Y)$ and $I(\mathbf{X};\mathbf{Z}) = I(X^N;Z^N) = NI(X;Z)$.

Thus the proof of step 1 is completed.

To prove step 2, we need to bound the entropy of the codeword $\mathbf{X}$ conditioned on the message $\mathbf{S}$ and wiretapper's observation $\mathbf{Z}$. When $\mathbf{S}$ takes value $\mathbf{s}$, we consider the subset of C_1, $\mathbf{s}+C_2$ as a codebook, $\mathbf{X}$ in the codebook as the input codeword, $\mathbf{Z}$ as the corresponding output of passing $\mathbf{X}$ through the wiretap channel. From $\mathbf{Z}$, the decoder estimates $\mathbf{X}$ as $\hat{\mathbf{X}} = g(\mathbf{Z})$. Define the probability of error

$$P_{ew} = \Pr(\hat{\mathbf{X}} \neq \mathbf{X}). \tag{5.12}$$

From Fano's inequality, we have

$$H(\mathbf{X}|\mathbf{s},\mathbf{Z}) \overset{(a)}{\leq} h(P_{ew}) + P_{ew}K_2,$$

where (a) follows from the fact that, there are 2^{K_2} codewords in the codebook $\mathbf{s} + C_2$. Furthermore, we have

$$\begin{aligned}
H(\mathbf{X}|\mathbf{S},\mathbf{Z}) &= \sum_{\mathbf{s}} \Pr(\mathbf{S}=\mathbf{s}) H(\mathbf{X}|\mathbf{s},\mathbf{Z}) \\
&\leq \{h(P_{ew}) + P_{ew}K_2\} \sum_{\mathbf{s}} \Pr(\mathbf{S}=\mathbf{s}). \\
&= h(P_{ew}) + P_{ew}K_2.
\end{aligned}$$

Thus we complete the proof of step 2.

Now we proceed to step 3. Note that the estimate $g(\mathbf{Z})$ of the decoder can be arbitrary. Here we use the typical set decoder. With the knowledge of $\mathbf{s}$ and $\mathbf{z}$, the decoder tries to find the codeword $\mathbf{x}$ sent to the channel. The decoder examines the typical set $T_{E_w}^N(\epsilon)$, the set of noise sequences $\mathbf{e_w}$ that satisfy

$$2^{-N[h(p_w)+\epsilon]} \leq \Pr(\mathbf{E_w} = \mathbf{e_w}) \leq 2^{-N[h(p_w)-\epsilon]}.$$

Check to see if any of those typical noise sequences, $\mathbf{e_w}$ satisfies

$$\mathbf{e_w}{\mathrm{H}_2}^{\mathrm{T}} = \mathbf{z}{\mathrm{H}_2}^{\mathrm{T}}.$$

If exactly one typical sequence $\mathbf{e_w}$ does, the typical set decoder reports $\mathbf{e_w}$ as the hypothesized noise sequence. The codeword $\mathbf{x}$ is decoded as $\hat{\mathbf{x}} = \mathbf{z} - \mathbf{e_w}$. However, if no typical sequence in the set $T_{E_w}^N(\epsilon)$ matches the observed syndrome $\mathbf{z}{\mathrm{H}_2}^{\mathrm{T}}$, or more than one does, then the typical decoder reports an error.

The error probability of the typical set decoder at the legitimate receiver, can be written as follows,

$$P_{ew} = P_{T_w} + P_{\mathrm{H}_2}, \tag{5.13}$$

where P_{T_w} is the probability that the true noise sequence is itself not typical, and P_{H_2} is the probability that the true noise sequence is typical and at least one other typical sequence clashes with it.

We first analyze P_{T_w}. For given $\epsilon > 0$ and $\lambda > 0$, there exists an integer N_3, such that when $N \geq N_3$, $\Pr\{\mathbf{e_w} \in T_{E_w}^N(\epsilon)\} \geq 1 - \lambda/2$. Therefore, when $N \geq N_3$, $P_{T_w} = 1 - \Pr\{\mathbf{e_w} \in T_{E_w}^N(\epsilon)\} \leq \lambda/2$.

The probability P_{H_2}. Let the true noise sequence is $\mathbf{e_w}$. It belongs to the set $T_{E_w}^N(\epsilon)$. If any of the typical noise sequence $\mathbf{e}_\mathbf{w}^*$, different from $\mathbf{e_w}$, satisfies $(\mathbf{e}_\mathbf{w}^* - \mathbf{e_w}){\mathrm{H}_2}^{\mathrm{T}} = \mathbf{0}$, then we have an error. We use the truth function

$$\mathbf{1}[(\mathbf{e}_\mathbf{w}^* - \mathbf{e_w}){\mathrm{H}_2}^{\mathrm{T}} = \mathbf{0}], \tag{5.14}$$

whose value is one if the statement $(\mathbf{e}_\mathbf{w}^* - \mathbf{e_w}){\mathrm{H}_2}^{\mathrm{T}} = \mathbf{0}$ is true and zero otherwise. Then when the true noise is $\mathbf{e_w}$, the number of such errors can be bounded as:

$$[\text{ Number of errors given } \mathbf{e} \text{ and } \mathrm{H}_2] \leq \sum_{\substack{\mathbf{e}_\mathbf{w}^*\colon \ \mathbf{e}_\mathbf{w}^* \in T_{E_w}^N(\epsilon) \\ \mathbf{e}_\mathbf{w}^* \neq \mathbf{e_w}}} \mathbf{1}[(\mathbf{e}_\mathbf{w}^* - \mathbf{e_w}){\mathrm{H}_2}^{\mathrm{T}} = \mathbf{0}]. \tag{5.15}$$

The number of errors is either zero or one; the sum on the right-hand side may exceed one, in case where several typical noise sequences have the same syndrome. Here, note that

$$\mathbf{1}[(\mathbf{e}_\mathbf{w}^* - \mathbf{e_w}){\mathrm{H}_2}^{\mathrm{T}} = \mathbf{0}] = \mathbf{1}[(\mathbf{e}_\mathbf{w}^* - \mathbf{e_w}){\mathrm{H}_1}^{\mathrm{T}} = \mathbf{0}] \cdot \mathbf{1}[(\mathbf{e}_\mathbf{w}^* - \mathbf{e_w})\mathrm{H}^{\mathrm{T}} = \mathbf{0}].$$

We can write down the probability P_{H_2} by averaging over $\mathbf{e_w}$:

$$P_{\mathrm{H}_2} \leq \sum_{\mathbf{e_w} \in T_E^N(\epsilon)} \Pr(\mathbf{E_w} = \mathbf{e_w}) \sum_{\substack{\mathbf{e}_\mathbf{w}^*\colon \ \mathbf{e}_\mathbf{w}^* \in T_E^N(\epsilon) \\ \mathbf{e}_\mathbf{w}^* \neq \mathbf{e_w}}} \mathbf{1}[(\mathbf{e}_\mathbf{w}^* - \mathbf{e_w}){\mathrm{H}_2}^{\mathrm{T}} = \mathbf{0}]. \tag{5.16}$$

Now we will find the average of P_{H_2}, $\bar{P}_{\mathrm{H}_2}$, by averaging over all possible H_2 with $N - K_1 + K$ rows and N columns. Note that H_2 can be randomly generated in the way that H_1 and H are randomly generated independently.

We denote averaging over all possible binary matrices H_2 by $\langle \cdots \rangle_{\mathrm{H}_2}$. Then we have

$\bar{P}_{\mathrm{H}_2} = \langle P_{\mathrm{H}_2} \rangle_{\mathrm{H}_2}$

$$
\begin{aligned}
&\leq \langle \sum_{\mathbf{e_w}\in T_{E_w}^N(\epsilon)} \Pr(\mathbf{E_w}=\mathbf{e_w}) \sum_{\substack{\mathbf{e_w^*}:\ \mathbf{e_w^*}\in T_{E_w}^N(\epsilon)\\ \mathbf{e_w^*}\neq \mathbf{e_w}}} \mathbf{1}[(\mathbf{e_w^*}-\mathbf{e_w}){H_2}^{\mathrm{T}}=\mathbf{0}]\rangle_{\mathrm{H_2}}\\
&= \sum_{\mathbf{e_w}\in T_{E_w}^N(\epsilon)} \Pr(\mathbf{E_w}=\mathbf{e_w}) \sum_{\substack{\mathbf{e_w^*}:\ \mathbf{e_w^*}\in T_{E_w}^N(\epsilon)\\ \mathbf{e_w^*}\neq \mathbf{e_w}}} \langle\mathbf{1}[(\mathbf{e_w^*}-\mathbf{e_w}){H_2}^{\mathrm{T}}=\mathbf{0}]\rangle_{\mathrm{H_2}}\\
&= \sum_{\mathbf{e_w}\in T_{E_w}^N(\epsilon)} \Pr(\mathbf{E_w}=\mathbf{e_w}) \sum_{\substack{\mathbf{e_w^*}:\ \mathbf{e_w^*}\in T_{E_w}^N(\epsilon)\\ \mathbf{e_w^*}\neq \mathbf{e_w}}} \langle\langle\mathbf{1}[(\mathbf{e_w^*}-\mathbf{e_w}){H_1}^{\mathrm{T}}=\mathbf{0}]\cdot\mathbf{1}[(\mathbf{e_w^*}-\mathbf{e_w})\mathrm{H}^{\mathrm{T}}=\mathbf{0}]\rangle_{\mathrm{H_1}}\rangle_{\mathrm{H}}\\
&= \sum_{\mathbf{e_w}\in T_{E_w}^N(\epsilon)} \Pr(\mathbf{E_w}=\mathbf{e_w}) \sum_{\substack{\mathbf{e_w^*}:\ \mathbf{e_w^*}\in T_{E_w}^N(\epsilon)\\ \mathbf{e_w^*}\neq \mathbf{e_w}}} \langle\mathbf{1}[(\mathbf{e_w^*}-\mathbf{e_w}){H_1}^{\mathrm{T}}=\mathbf{0}]\rangle_{\mathrm{H_1}}\cdot\langle\mathbf{1}[(\mathbf{e_w^*}-\mathbf{e_w})\mathrm{H}^{\mathrm{T}}=\mathbf{0}]\rangle_{\mathrm{H}}.
\end{aligned}
$$

Since for any non-zero binary sequence $\mathbf{v}$, the probability that $\mathbf{v}{H_1}^{\mathrm{T}}=\mathbf{0}$, averaging over all possible $\mathrm{H_1}$, is $2^{-(N-K_1)}$ and the probability that $\mathbf{v}\mathrm{H}^{\mathrm{T}}=\mathbf{0}$ averaging over all possible H, is 2^{-K}. So

$$
\begin{aligned}
\bar{P}_{\mathrm{H_2}} &\leq (\sum_{\mathbf{e_w}\in T_{E_w}^N(\epsilon)} \Pr(\mathbf{E_w}=\mathbf{e_w}))(|T_{E_w}^N(\epsilon)|-1)2^{-(N-K_1)}\cdot 2^{-K}\\
&< |T_{E_w}^N(\epsilon)|2^{-(N-K_1+K)}\\
&\leq 2^{N[h(p_w)+\epsilon]}2^{-(N-K_1+K)}\\
&= 2^{-N(1-h(p_w)-\epsilon-\frac{K_1-K}{N})}.
\end{aligned}
$$

Note that $\frac{K_1-K}{N}\leq 1-h(p_w)-2\epsilon<1-h(p_w)-\epsilon$. Therefore, for given $\epsilon>0$ and $\lambda>0$, there exists an N_4, when $N\geq N_4$, $\bar{P}_{\mathrm{H_2}}\leq\lambda/8$. By Markov inequality, we have

$$\Pr(P_{\mathrm{H_2}}>\frac{\lambda}{2})<\frac{\bar{P}_{\mathrm{H_2}}}{\lambda/2}\leq\frac{\lambda/8}{\lambda/2}=\frac{1}{4}.$$

Thus,

$$\Pr(P_{\mathrm{H_2}}\leq\frac{\lambda}{2})=1-\Pr(P_{\mathrm{H_2}}\geq\frac{\lambda}{2})>\frac{3}{4}.$$

That is, from all possible $\mathrm{H_2}$, more than 3/4 random choices yield $P_{\mathrm{H_2}}\leq\lambda/2$. Due to the structure of $\mathrm{H_2}$, this implies that, there are more than 3/4 random choices from all possible $\mathrm{H_1}$, independently more than 3/4 random choices from all possible H such that $\mathrm{H_2}$ satisfies $P_{\mathrm{H_2}}\leq\lambda/2$.

Thus we have shown that there exists $\mathrm{H_1}$ and H such that, for given $\epsilon>0$ and $\lambda>0$, when $N\geq\max\{N_3,N_4\}$,

$$P_{ew}=P_{T_w}+P_{\mathrm{H_2}}\leq\lambda/2+\lambda/2=\lambda.$$

This completes the proof of step 3.

Note that we have shown that for given $\varepsilon,\delta,\zeta,\epsilon>0$, when $N\geq\max\{N_0,N_1,N_2,N_3,N_4\}$, there are more than 3/4 random choices from all possible $\mathrm{H_1}$ such that $P_e\leq\delta$; Furthermore, there are more than 3/4 random choices from all possible $\mathrm{H_1}$, more than 3/4 random choices from all possible H, such that $P_{ew}\leq\lambda$. Therefore, there are at least 1/2 random choices of all possible $\mathrm{H_1}$ and more than 3/4 random choices from all possible H such that $P_e\leq\delta$ and

$P_{ew} \leq \lambda$ are both satisfied at the same time. Thus we have shown that there exist H_1 and H that lead to a random linear code such that

$$\frac{K}{N} \geq h(p_w) - h(p) - \varepsilon, \quad d \geq 1 - \zeta, \quad P_e \leq \delta.$$

5.4 Performance of linear codes in wiretap channel

We have proved that the secrecy capacity of the wiretap channel as shown in Figure 5.3, can be achieved by using random linear codes. However, the typical set decoder used in the proof is not easy to implement. Thus, the method is existent but not effective in practice. Until now it is still an unsolved problem to write down an explicit and practical encoder and decoder to achieve the reliable and secure communication over the wiretap channel at rates close to the secrecy capacity.

The motivation of this section is the need of constructive and applicable codes for the wiretap channel. We restrict our attention to the binary linear codes for ease of implementation. The performance of the codes is evaluated from three perspectives: the efficiency measured by the rate from the source to the legitimate receiver, the reliability measured by the error probability of decoding at the legitimate receiver and the security measured by the equivocation of the wiretapper about the information transmitted.

Consider the situation as given in Figure 5.3. The main channel is a BSC with crossover probability p ($0 \leq p \leq \frac{1}{2}$) and the wiretap channel is a BSC with crossover probability p_w ($0 \leq p_w \leq \frac{1}{2}$ and $p_w \geq p$). We use the encoding strategy similar to the one for the random linear code given in Section 5.3. Let H_1 be an $N - K_1$ by N binary matrix and H be a K by N binary matrix. From (5.6), we construct H_2 as

$$\mathrm{H}_2 = \begin{bmatrix} \mathrm{H}_1 \\ \mathrm{H} \end{bmatrix}.$$

Assume that H_1, H and H_2 are with full rank. Let C_1 be the dual code of the $(N, N - K_1)$ linear code generated by H_1 and C_2 be the dual code of the $(N, N-K_2)$ linear code generated by H_2. That is, H_1 is a parity check matrix of C_1 and H_2 is a parity check matrix of C_2.

5.4.1 Efficiency

By the encoding strategy, to transmit a K-bit secret message $\mathbf{s}$, an N-bit codeword $\mathbf{x}$ is sent to the channel. So the rate of the transmission is

$$R = \frac{K}{N}. \tag{5.17}$$

Furthermore, $\mathbf{x}$ is chosen at random from the solution set of the equation (5.7)

$$\mathbf{x}{\mathrm{H}_2}^{\mathrm{T}} = \mathbf{x} \begin{bmatrix} \mathrm{H}_1 \\ \mathrm{H} \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} \mathbf{x}{\mathrm{H}_1}^{\mathrm{T}} & \mathbf{x}\mathrm{H}^{\mathrm{T}} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \mathbf{s} \end{bmatrix}.$$

Due to the 2^K different secret messages, the solution set of the equation $\mathbf{x}{\mathrm{H}_1}^{\mathrm{T}} = \mathbf{0}$, i.e., C_1, is equally divided into 2^K subsets. Every subset is a coset of C_2 by Lemma 5.4.1. In particular, C_2 is the subset of C_1 corresponding to $\mathbf{s} = \mathbf{0}$. Let $\mathbf{x}(\mathbf{s}(\mathbf{i}))$ be the coset leader of

the coset corresponding to the secret message $\mathbf{s}(\mathbf{i})$, $0 \leq i \leq 2^K - 1$. Then, the codebook in the encoding scheme can be shown as follows:

Table 5.1: The codebook in the encoding scheme

Space of input $\mathbf{x}$	Secret $\mathbf{s}$	Set of codewords corresponding to secret $\mathbf{s}$
C_1	$\mathbf{s}(\mathbf{0})$	$\mathbf{x}(\mathbf{s}(\mathbf{0})) + C_2$
	$\mathbf{s}(\mathbf{1})$	$\mathbf{x}(\mathbf{s}(\mathbf{1})) + C_2$
	$\vdots$	$\vdots$
	$\mathbf{s}(\mathbf{2^K - 1})$	$\mathbf{x}(\mathbf{s}(\mathbf{2^K - 1})) + C_2$

Lemma 5.4.1 *The solution set of the equation (5.7) is a coset of C_2. Here C_2 is the dual code of the code generated by the matrix* H_2.

Proof: See the proof in Appendix XVII. ■

Using the above codebook, in order to transmit the secret $\mathbf{s}$, we randomly choose a sequence $\mathbf{x}$ from the set $\mathbf{x}(\mathbf{s}) + C_2$. Let $\mathbf{y}, \mathbf{z}$ be the outputs of the main channel and the wiretap channel, respectively, corresponding to the input $\mathbf{x}$. Note that $\mathbf{x}$ is chosen from C_1, which is a subspace of $\{0,1\}^N$, while $\mathbf{y}, \mathbf{z}$ can be any sequence from the whole space $\{0,1\}^N$.

5.4.2 Reliability

At the legitimate receiver, the decoder uses syndrome decoding [20, Chapter 3]. The reason is that the true error sequence $\mathbf{e}$ has the same syndrome as $\mathbf{y}$, i.e.,

$$\mathbf{e}{\mathrm{H}_1}^{\mathrm{T}} = \mathbf{y}{\mathrm{H}_1}^{\mathrm{T}}.$$

However, there are 2^{K_1} error patterns that result in the same syndrome, and the true error sequence $\mathbf{e}$ is just one of them. Note that for a BSC, the error patterns with smaller Hamming weight are more probable. In order to minimize the probability of a decoding error, the decoder chooses the one with the minimum Hamming weight from the 2^{K_1} candidates to be the error sequence $\mathbf{e}$. Then, the secret $\mathbf{s}$ is decoded as

$$\hat{\mathbf{s}} = (\mathbf{y} - \mathbf{e})\mathrm{H}^{\mathrm{T}}.$$

It is clear that the set of 2^{K_1} candidates is a coset of code C_1. Furthermore, there are 2^{N-K_1} disjoint cosets of C_1 in $\{0,1\}^N$ and they together span the whole space $\{0,1\}^N$. We denote the 2^{N-K_1} coset leaders as $\mathbf{e}(\mathbf{i})$, where $0 \leq i \leq 2^{N-K_1} - 1$ and $\mathbf{e}(\mathbf{0}) = \mathbf{0}$.

The error probability of decoding. If the true error sequence $\mathbf{e}$ is one of 2^{N-K_1} coset leaders, $\mathbf{x} = \mathbf{y} - \mathbf{e}$ will be correctly decoded. So does $\mathbf{s} = \mathbf{x}\mathrm{H}^{\mathrm{T}}$. Furthermore, if the true error sequence $\mathbf{e}$ belongs to any coset $\mathbf{e}(\mathbf{i}) + C_2$, $\mathbf{s}$ will also be decoded correctly. The reason is that in this case, since $\mathbf{e} \in \mathbf{e}(\mathbf{i}) + C_2$, we have

$$\mathbf{e}{\mathrm{H}_2}^{\mathrm{T}} = \mathbf{e}(\mathbf{i}){\mathrm{H}_2}^{\mathrm{T}} \quad \Rightarrow \quad \mathbf{e}\mathrm{H}^{\mathrm{T}} = \mathbf{e}(\mathbf{i})\mathrm{H}^{\mathrm{T}}.$$

The codeword $\mathbf{x}$ is decoded as $\hat{\mathbf{x}} = \mathbf{y} - \mathbf{e}(\mathbf{i})$. However,

$$\begin{aligned}\hat{\mathbf{x}}\mathrm{H}^{\mathrm{T}} &= (\mathbf{y} - \mathbf{e}(\mathbf{i}))\mathrm{H}^{\mathrm{T}} = \mathbf{y}\mathrm{H}^{\mathrm{T}} - \mathbf{e}(\mathbf{i})\mathrm{H}^{\mathrm{T}} \\ &= \mathbf{y}\mathrm{H}^{\mathrm{T}} - \mathbf{e}\mathrm{H}^{\mathrm{T}} = (\mathbf{y} - \mathbf{e})\mathrm{H}^{\mathrm{T}} \\ &= \mathbf{x}\mathrm{H}^{\mathrm{T}} = \mathbf{s}.\end{aligned}$$

Thus, when the true error sequence is from the 2^{N-K_1} cosets $\mathbf{e}(\mathbf{i}) + C_2$, where $0 \leq i \leq 2^{N-K_1} - 1$, the secret $\mathbf{s}$ can be decoded correctly by the legitimate receiver. The total number of such error patterns is $2^{N-K_1} \cdot 2^{K_2} = 2^{N-K}$. The probability of correct decoding is

$$\Pr\{\hat{\mathbf{s}} = \mathbf{s}\} = \sum_{i=0}^{2^{N-K_1}-1} \sum_{\mathbf{e} \in \mathbf{e}(\mathbf{i}) + C_2} p^{w(\mathbf{e})}(1-p)^{N-w(\mathbf{e})}.$$

By the theorem for the weight distribution of a coset of a linear code given in [13], we have

$$\sum_{\mathbf{e} \in \mathbf{e}(\mathbf{i}) + C_2} x^{N-w(\mathbf{e})} y^{w(\mathbf{e})} = \frac{1}{2^{N-K_2}} \sum_{j=0}^{N} (2b_j(\mathbf{e}(\mathbf{i})) - B_j)(x+y)^{N-j}(x-y)^j,$$

where $b_j(\mathbf{e}(\mathbf{i}))$ is equal to the number of codewords of weight j in the dual code $C_2^{\perp}$ orthogonal to $\mathbf{e}(\mathbf{i})$, and B_j is equal to the number of codewords of weight j in the dual code $C_2^{\perp}$. Taking $x = 1 - p$ and $y = p$, we have

$$\sum_{\mathbf{e} \in \mathbf{e}(\mathbf{i}) + C_2} p^{w(\mathbf{e})}(1-p)^{N-w(\mathbf{e})} = \frac{1}{2^{N-K_2}} \sum_{j=0}^{N} (2b_j(\mathbf{e}(\mathbf{i})) - B_j)(1-2p)^j.$$

Therefore,

$$\begin{aligned}\Pr\{\hat{\mathbf{s}} = \mathbf{s}\} &= \frac{1}{2^{N-K_2}} \sum_{i=0}^{2^{N-K_1}-1} \sum_{j=0}^{N} (2b_j(\mathbf{e}(\mathbf{i})) - B_j)(1-2p)^j \\ &= \frac{1}{2^{N-K_2}} \sum_{i=0}^{2^{N-K_1}-1} \sum_{j=0}^{N} 2b_j(\mathbf{e}(\mathbf{i}))(1-2p)^j - \frac{1}{2^K} \sum_{j=0}^{N} B_j(1-2p)^j \\ &= \frac{1}{2^{N-K_2}} \sum_{j=0}^{N} (2 \sum_{i=0}^{2^{N-K_1}-1} b_j(\mathbf{e}(\mathbf{i})))(1-2p)^j - \frac{1}{2^K} \sum_{j=0}^{N} B_j(1-2p)^j.\end{aligned}$$

The error probability of decoding P_e is

$$\begin{aligned}P_e &= \Pr\{\hat{\mathbf{s}} \neq \mathbf{s}\} = 1 - \Pr\{\hat{\mathbf{s}} = \mathbf{s}\} \\ &= 1 + \frac{1}{2^K} \sum_{j=0}^{N} B_j(1-2p)^j - \frac{1}{2^{N-K_2}} \sum_{j=0}^{N} (2 \sum_{i=0}^{2^{N-K_1}-1} b_j(\mathbf{e}(\mathbf{i})))(1-2p)^j. \quad (5.18)\end{aligned}$$

Clearly, when $i = 0$, $\mathbf{e}(\mathbf{0}) = \mathbf{0}$. We have

$$b_j(\mathbf{e}(\mathbf{0})) = B_j. \quad (5.19)$$

Now let us try to simplify (5.18) for the special cases when C_1 spans the whole space $\{0,1\}^N$ and when C_1 is a binary Hamming code.

C_1 spans the whole space $\{0,1\}^N$.

Note that when C_1 spans the whole space $\{0,1\}^N$, then $K_1 = N$ and there is only one coset in $\{0,1\}^N$: $\mathbf{e} + C_1$ with $\mathbf{e} = \mathbf{0}$. In this case, (5.18) can be simplified as follows:

$$P_e = 1 - \frac{1}{2^{N-K_2}} \sum_{j=0}^{N} B_j (1-2p)^j. \tag{5.20}$$

C_1 is a binary Hamming code.

Note that when C_1 is a binary Hamming code, then C_1 has 1 error correcting capability and its parameters N, K_1 satisfy that $N = 2^{N-K_1} - 1$. In this case, the coset leader $\mathbf{e}(\mathbf{i})$ of the coset $\mathbf{e}(\mathbf{i}) + C_1$, $1 \le i \le N$ is of weight 1. Since $\mathbf{e}(\mathbf{i}')$ is different from $\mathbf{e}(\mathbf{i})$ when $i' \neq i$, so these N coset leaders are all possible N-bit sequences of weight 1.

Consider $\sum_{i=1}^{N} b_j(\mathbf{e}(\mathbf{i}))$. Let $\mathbf{v}$ be a codeword of weight j. Since $\{\mathbf{e}(\mathbf{i}), 1 \le i \le N\}$ are all possible sequences of weight 1, it is clear that there are j sequences from them not orthogonal to $\mathbf{v}$. In other words, for fixed $\mathbf{v}$ of weight j, there are $N - j$ coset leaders orthogonal to $\mathbf{v}$. Furthermore, there are B_j such $\mathbf{v}$ of weight j in the code $C_2^{\perp}$. Therefore, we have

$$\sum_{i=1}^{N} b_j(\mathbf{e}(\mathbf{i})) = (N-j)B_j. \tag{5.21}$$

Taking account of (5.19), we have

$$\sum_{i=0}^{N} b_j(\mathbf{e}(\mathbf{i})) = (N+1-j)B_j. \tag{5.22}$$

The probability of correct decoding in this case can be calculated as follows:

$$\begin{aligned}
\Pr\{\hat{\mathbf{s}} = \mathbf{s}\} &= \frac{1}{2^{N-K_2}} \sum_{j=0}^{N} (2 \sum_{i=0}^{N} b_j(\mathbf{e}(\mathbf{i})))(1-2p)^j - \frac{1}{2^K} \sum_{j=0}^{N} B_j (1-2p)^j \\
&= \frac{1}{2^{N-K_2}} \sum_{j=0}^{N} 2(N+1-j)B_j (1-2p)^j - \frac{1}{2^K} \sum_{j=0}^{N} B_j (1-2p)^j \\
&\overset{(a)}{=} \frac{1}{2^K} \sum_{j=0}^{N} B_j (1-2p)^j - \frac{2}{2^{N-K_2}} \sum_{j=0}^{N} j B_j (1-2p)^j \\
&\overset{(a)}{=} \frac{1}{2^K} \sum_{j=0}^{N} (1 - \frac{2j}{N+1}) B_j (1-2p)^j,
\end{aligned}$$

where (a) follows from the fact that $N = 2^{N-K_1} - 1$, since C_1 is a binary Hamming code. Thus, the error probability of decoding has the following form

$$P_e = 1 - \Pr\{\hat{\mathbf{s}} = \mathbf{s}\}$$

$$= \quad 1 - \frac{1}{2^K}\sum_{j=0}^{N}(1 - \frac{2j}{N+1})B_j(1-2p)^j, \tag{5.23}$$

where $\{B_j, 0 \le j \le N\}$ is the weight distribution of the code $C_2^{\perp}$, the code generated by the matrix H_2.

So far, we have given a way to calculate P_e with the knowledge of the weight distribution of $C_2^{\perp}$, for the case that C_1 is a binary Hamming code. By the Macwilliams identity [20, Chapter 3], it is easy to show that P_e can also be calculated with the knowledge of the weight distribution of C_2.

Using the Macwilliams identity [20, Chapter 3] for a (n, k) linear code C, we have

$$\sum_{\mathbf{v}\in C} x^{n-w(v)}y^{w(v)} = \frac{1}{2^{n-k}}\sum_{j=0}^{n} W_j(x+y)^{n-j}(x-y)^j,$$

where W_i is the number of codewords of weight j in the dual code $C_{\perp}$. Let $\{D_j, 0 \le j \le N\}$ and $\{B_j, 0 \le j \le N\}$ be the weight distribution of C_2 and it dual code $C_2^{\perp}$, respectively. Taking $x = 1-p, y = p$ and applying the Macwilliams identity for C_2, we have the following

$$\begin{aligned}
\sum_{j=0}^{N} D_j p^j (1-p)^{N-j} &= \frac{1}{2^{N-K_2}}\sum_{j=0}^{N} B_j(1-2p)^j \\
2^{N-K_2}\sum_{j=0}^{N} D_j p^j (1-p)^{N-j} &= \sum_{j=0}^{N} B_j(1-2p)^j.
\end{aligned}$$

Consider the first derivative of the above equation with respect to p.

$$\sum_{j=0}^{N} -2jB_j(1-2p)^{j-1} = 2^{N-K_2}\sum_{j=0}^{N}[jD_j p^{j-1}(1-p)^{N-j} - (N-j)D_j p^j (1-p)^{N-j-1}]$$

$$\begin{aligned}
\sum_{j=0}^{N} 2jB_j(1-2p)^j &= -2^{N-K_2}\sum_{j=0}^{N}(1-2p)[jD_j p^{j-1}(1-p)^{N-j} - (N-j)D_j p^j (1-p)^{N-j-1}] \\
&= 2^{N-K_2}\sum_{j=0}^{N}(N - \frac{j(1-p)}{p} - \frac{(N-j)p}{1-p})D_j p^j (1-p)^{N-j}.
\end{aligned}$$

From (5.23), we have

$$\begin{aligned}
P_e &= 1 - \frac{1}{2^K}\sum_{j=0}^{N}(1 - \frac{2j}{N+1})B_j(1-2p)^j \\
&= 1 - \frac{1}{2^K}\sum_{j=0}^{N} B_j(1-2p)^j + \frac{1}{2^K}\frac{1}{N+1}\sum_{j=0}^{N} 2jB_j(1-2p)^j \\
&= 1 - 2^{N-K_1}\sum_{j=0}^{N} D_j p^j (1-p)^{N-j} + \frac{2^{N-K_1}}{N+1}\sum_{j=0}^{N}(N - \frac{j(1-p)}{p} - \frac{(N-j)p}{1-p})D_j p^j (1-p)^{N-j}
\end{aligned}$$

$$\stackrel{(a)}{=} 1 - \sum_{j=0}^{N} (1 + \frac{j(1-p)}{p} + \frac{(N-j)p}{1-p}) D_j p^j (1-p)^{N-j}, \tag{5.24}$$

where (a) follows from the fact that $2^{N-K_1} = N+1$ since C_1 is a binary Hamming code.

5.4.3 Security

Consider the wiretapper' s equivocation about the secret message. We have

$$\begin{aligned} d &= \frac{H(\mathbf{S}|\mathbf{Z})}{H(\mathbf{S})} \\ &= \frac{H(\mathbf{S}) + H(\mathbf{Z}|\mathbf{S}) - H(\mathbf{Z})}{H(\mathbf{S})} \\ &= \frac{K + H(\mathbf{Z}|\mathbf{S}) - H(\mathbf{Z})}{K} \\ &= 1 - \frac{H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S})}{K}. \end{aligned} \tag{5.25}$$

To calculate d, we need to know the entropy of $\mathbf{Z}$ and the conditional entropy of $\mathbf{Z}$ given the secret message $\mathbf{S}$.

First let us consider the conditional probability of $\mathbf{z}$ given $\mathbf{s(i)}$, $0 \le i \le 2^K - 1$.

$$\begin{aligned} p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s(i)}) &= \sum_{\mathbf{x} \in \mathbf{x(s(i))} + C_2} p_{\mathbf{X}|\mathbf{S}}(\mathbf{x}|\mathbf{s(i)}) p_{\mathbf{Z}|\mathbf{X},\mathbf{S}}(\mathbf{z}|\mathbf{x}, \mathbf{s(i)}) \\ &\stackrel{(a)}{=} \frac{1}{2^{K_2}} \sum_{\mathbf{x} \in \mathbf{x(s(i))} + C_2} p_{\mathbf{Z}|\mathbf{X}}(\mathbf{z}|\mathbf{x}) \\ &\stackrel{(b)}{=} \frac{1}{2^{K_2}} \sum_{\mathbf{x} \in \mathbf{x(s(i))} + C_2} p_w^{w(\mathbf{x}+\mathbf{z})} (1-p_w)^{N - w(\mathbf{x}+\mathbf{z})} \\ &= \frac{1}{2^{K_2}} \sum_{\mathbf{v} \in \mathbf{x(s(i))} + \mathbf{z} + C_2} p_w^{w(\mathbf{v})} (1-p_w)^{N - w(\mathbf{v})}, \end{aligned}$$

where

(a) follows the fact that $p_{\mathbf{X}|\mathbf{S}}(\mathbf{x}|\mathbf{s}) = \frac{1}{2^{K_2}}$ and $p(\mathbf{z}|\mathbf{x}, \mathbf{s(i)}) = p(\mathbf{z}|\mathbf{x})$. The reason is that to send $\mathbf{s(i)}$, $\mathbf{x}$ is chosen randomly from the coset $\mathbf{x(s(i))} + C_2$. Furthermore, $\mathbf{S} \to \mathbf{X} \to \mathbf{Z}$ forms a Markov chain;

(b) follows the fact that the wiretap channel is a BSC with crossover probability p_w.

Applying the theorem for the weight distribution of a coset of a linear code given in [13], we have

$$\sum_{\mathbf{v} \in \mathbf{x(s(i))} + \mathbf{z} + C_2} p_w^{w(\mathbf{v})} (1-p_w)^{N - w(\mathbf{v})} = \frac{1}{2^{N-K_2}} \sum_{j=0}^{N} (2b_{ij} - B_j)(1-2p_w)^j,$$

where b_{ij} is equal to the number of codewords of weight j in the dual code $C_2^{\perp}$ orthogonal to $\mathbf{x(s(i))} + \mathbf{z}$, and B_j is equal to the number of codewords of weight j in the dual code $C_2^{\perp}$.

Therefore, $p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{i}))$ can be calculated as follows:

$$p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{i})) = \frac{1}{2^{K_2}} \sum_{\mathbf{v}\in\mathbf{x}(\mathbf{s}(\mathbf{i}))+\mathbf{z}+C_2} p_w^{w(\mathbf{v})}(1-p_w)^{N-w(\mathbf{v})} \tag{5.26}$$

$$= \frac{1}{2^N}\sum_{j=0}^{N}(2b_{ij}-B_j)(1-2p_w)^j. \tag{5.27}$$

From (5.26), we see that the probability of $\mathbf{z}$ given $\mathbf{s}(\mathbf{i})$ is decided by the weight distribution of the coset $\mathbf{x}(\mathbf{s}(\mathbf{i}))+\mathbf{z}+C_2$. Note that given $\mathbf{s}(\mathbf{i})$, $\mathbf{x}(\mathbf{s}(\mathbf{i}))$ is a fixed sequence. Thus for given $\mathbf{s}(\mathbf{i})$, $\{\mathbf{x}(\mathbf{s}(\mathbf{i}))+\mathbf{z}, \mathbf{z}\in\{0,1\}^N\}$ is a permutation of $\{\mathbf{z}, \mathbf{z}\in\{0,1\}^N\}$. As a straightforward consequence, $\{\mathbf{x}(\mathbf{s}(\mathbf{i}))+\mathbf{z}+C_2, \mathbf{z}\in\{0,1\}^N\}$ is a permutation of $\{\mathbf{z}+C_2, \mathbf{z}\in\{0,1\}^N\}$. If we consider the distribution of $\mathbf{Z}$ given $\mathbf{S}=\mathbf{s}$, it is clear that for $\mathbf{s}(\mathbf{0})=\mathbf{0}$ and any $1\le i\le 2^K-1$, $\{p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{i})), \mathbf{z}\in\{0,1\}^N\}$ is a permutation of $\{p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0})), \mathbf{z}\in\{0,1\}^N\}$. As a result, we have the following lemma.

Lemma 5.4.2 $H(\mathbf{Z}|\mathbf{S}) = H(\mathbf{Z}|\mathbf{S}=\mathbf{0})$.

Proof:

$$\begin{aligned}
H(\mathbf{Z}|\mathbf{S}) &= \sum_{i=0}^{2^K-1}\Pr(\mathbf{S}=\mathbf{s}(\mathbf{i}))H(\mathbf{Z}|\mathbf{S}=\mathbf{s}(\mathbf{i})) \\
&= \sum_{i=0}^{2^K-1}\Pr(\mathbf{S}=\mathbf{s}(\mathbf{i}))\sum_{\mathbf{z}\in\{0,1\}^N} p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{i}))\log\frac{1}{p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{i}))} \\
&= H(\mathbf{Z}|\mathbf{S}=\mathbf{0})\sum_{i=0}^{2^K-1}\Pr(\mathbf{S}=\mathbf{s}(\mathbf{i})) \\
&= H(\mathbf{Z}|\mathbf{S}=\mathbf{0}).
\end{aligned}$$

■

Easily, from (5.26) and (5.27), given $\mathbf{s}(\mathbf{0})=\mathbf{0}$, we have

$$p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0})) = \frac{1}{2^{K_2}} \sum_{\mathbf{v}\in\mathbf{z}+C_2} p_w^{w(\mathbf{v})}(1-p_w)^{N-w(\mathbf{v})} \tag{5.28}$$

$$= \frac{1}{2^N}\sum_{j=0}^{N}(2b_j(\mathbf{z})-B_j)(1-2p_w)^j, \tag{5.29}$$

where $b_j(\mathbf{z})$ is equal to the number of codewords of weight j in the dual code $C_2^{\perp}$ orthogonal to $\mathbf{z}$. By Lemma 5.4.2, the conditional entropy of $\mathbf{Z}$ given $\mathbf{S}$ can be calculated as follows:

$$H(\mathbf{Z}|\mathbf{S}) = \sum_{\mathbf{z}\in\{0,1\}^N} -\frac{1}{2^N}\sum_{j=0}^{N}(2b_j(\mathbf{z})-B_j)(1-2p_w)^j \log(\frac{1}{2^N}\sum_{j=0}^{N}(2b_j(\mathbf{z})-B_j)(1-2p_w)^j). \tag{5.30}$$

Now let us consider the probability of $\mathbf{z}$.

$$\begin{aligned} p_{\mathbf{Z}}(\mathbf{z}) &= \sum_{\mathbf{s}} p_S(\mathbf{s}) \sum_{\mathbf{x}\in\mathbf{x}(\mathbf{s})+C_2} p_{\mathbf{X}|\mathbf{S}}(\mathbf{x}|\mathbf{s}) p_{\mathbf{Z}|\mathbf{X},\mathbf{S}}(\mathbf{z}|\mathbf{x},\mathbf{s}(\mathbf{i})) \\ &\overset{(a)}{=} \sum_{\mathbf{s}} \frac{1}{2^K} \sum_{\mathbf{x}\in\mathbf{x}(\mathbf{s})+C_2} \frac{1}{2^{K_2}} p_{\mathbf{Z}|\mathbf{X}}(\mathbf{z}|\mathbf{x}) \\ &\overset{(b)}{=} \frac{1}{2^{K_1}} \sum_{\mathbf{x}\in C_1} p_w^{w(\mathbf{x}+\mathbf{z})}(1-p_w)^{N-w(\mathbf{x}+\mathbf{z})} \\ &= \frac{1}{2^{K_1}} \sum_{\mathbf{v}\in\mathbf{z}+C_1} p_w^{w(\mathbf{v})}(1-p_w)^{N-w(\mathbf{v})} \qquad (5.31) \\ &\overset{(c)}{=} \frac{1}{2^N} \sum_{j=0}^{N} (2a_j(\mathbf{z}) - A_j)(1-2p_w)^j, \qquad (5.32) \end{aligned}$$

where

(a) follows the fact that $P_S(\mathbf{s}) = \frac{1}{2^K}$, $p_{\mathbf{X}|\mathbf{S}}(\mathbf{x}|\mathbf{s}) = \frac{1}{2^{K_2}}$ and $p(\mathbf{z}|\mathbf{x},\mathbf{s}(\mathbf{i})) = p(\mathbf{z}|\mathbf{x})$. The reason is that $\mathbf{S}$ is uniformly distributed. In order to send $\mathbf{s}(\mathbf{i})$, $\mathbf{x}$ is chosen randomly from the coset $\mathbf{x}(\mathbf{s}(\mathbf{i})) + C_2$. Furthermore, $\mathbf{S} \to \mathbf{X} \to \mathbf{Z}$ forms a Markov chain;

(b) follows the fact that $K_1 = K + K_2$ and the wiretap channel is a BSC with crossover probability p_w.

(c) follows from the theorem for the weight distribution of a coset of a linear code given in [13]. Here $a_j(\mathbf{z})$ is equal to the number of codewords of weight j in the dual code $C_1^\perp$ orthogonal to $\mathbf{z}$, and A_j is equal to the number of codewords of weight j in the dual code $C_1^\perp$.

Therefore, the entropy of $\mathbf{Z}$ is

$$H(\mathbf{Z}) = \sum_{\mathbf{z}\in\{0,1\}^N} -\frac{1}{2^N} \sum_{j=0}^{N} (2a_j(\mathbf{z}) - A_j)(1-2p_w)^j \log \frac{1}{2^N} \sum_{j=0}^{N} (2a_j(\mathbf{z}) - A_j)(1-2p_w)^j. \quad (5.33)$$

5.5 Two special cases

As we have discussed, when linear codes C_1, C_2 are used for the wiretap channel, theoretically, the rate R, the error probability P_e and the equivocation d can be calculated to evaluate the performance from the perspectives of the efficiency, reliability and security. However, in general, the computation of P_e and d becomes practically impossible for large N, K_1 and K_2. In this section, we show the calculation for two special cases. The first is the case when C_1 is a Hamming code and C_2 is a repetition code. The second is the degraded case when $p = 0$, C_1 spans the whole space $\{0,1\}^N$, and C_2 is a special kind of linear code, for example, the binary Hamming code or the repetition code.

5.5.1 C_1 is a Hamming code and C_2 is a repetition code

When C_1 is a Hamming code and C_2 is a repetition code, the parameters satisfy the following equations:

$$K_1 = N - \log(N+1);$$

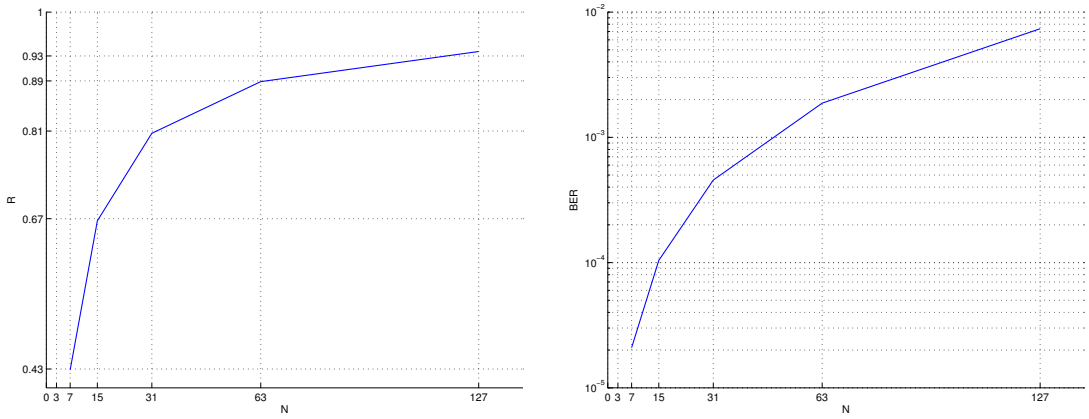
$$\begin{aligned} K_2 &= 1; \\ K &= K_1 - K_2 = N - \log(N+1) - 1. \end{aligned}$$

First, let us consider the efficiency R.

Recalling the expression of R from (5.17), we have:

$$R = \frac{K}{N} = \frac{N - \log(N+1) - 1}{N}.$$

As shown in Figure 5.4 (a), R is closer to 1 as N increases.



(a) R w.r.t N.

(b) P_e w.r.t N, when $p = 0.001$.

Figure 5.4: Rate R and error probability of decoding P_e with respect to N, when C_1 is a Hamming code of length N, C_2 is a repetition code.

The reliability.

Recall the expression of P_e for the case that C_1 is a Hamming code from (5.23) and (5.24). We have

$$\begin{aligned} P_e &= 1 - \frac{1}{2^K} \sum_{j=0}^{N} (1 - \frac{2j}{N+1}) B_j (1-2p)^j \\ &= 1 - \sum_{j=0}^{N} [D_j p^j (1-p)^{N-j} + j D_j p^{j-1} (1-p)^{N-j+1} + (N-j) D_j p^{j+1} (1-p)^{N-j-1}], \end{aligned}$$

where $\{B_j, 0 \le j \le N\}$ is the weight distribution of $C_2^{\perp}$ and $\{D_j, 0 \le j \le N\}$ is the weight distribution of C_2. If C_2 is the $(N, 1)$ repetition code, then we have

$$\begin{aligned} D_0 &= 1; \\ D_N &= 1; \\ D_j &= 0, \quad j \neq 0, N. \end{aligned}$$

It is easy to calculate P_e with the knowledge of the weight distribution of C_2. Therefore, when C_1 is a Hamming code and C_2 is a repetition code, we have P_e in the following

form:

$$P_e = 1 - [(1-p)^N + Np(1-p)^{N-1} + p^N + N(1-p)p^{N-1}]. \tag{5.34}$$

It is easy to verify that for fixed p, P_e is increasing with respect to N as shown in Figure 5.4 (b).

The security.

From (5.25) and Lemma 5.4.2, we can calculate the equivocation as follows:

$$d = 1 - \frac{H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S})}{K} = 1 - \frac{H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S}=\mathbf{0})}{N - \log(N+1) - 1}. \tag{5.35}$$

Consider the probability of $\mathbf{z}$ given $\mathbf{s}(\mathbf{0}) = \mathbf{0}$. From (5.28), since C_2 is a binary repetition code, we have

$$\begin{aligned} p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0})) &= \frac{1}{2^{K_2}} \sum_{\mathbf{v}\in\mathbf{z}+C_2} p_w^{w(\mathbf{v})}(1-p_w)^{N-w(\mathbf{v})} \\ &= \frac{1}{2}(p_w^{w(\mathbf{z})}(1-p_w)^{N-w(\mathbf{z})} + p_w^{N-w(\mathbf{z})}(1-p_w)^{w(\mathbf{z})}). \end{aligned}$$

The conditional entropy of $\mathbf{Z}$ given that $\mathbf{S} = \mathbf{0}$ can be calculated as follows:

$$\begin{aligned} H(\mathbf{Z}|\mathbf{S}=\mathbf{0}) &= -\sum_{\mathbf{z}\in\{0,1\}^N} p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0})) \log p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0})) \\ &= -\sum_{i=0}^{N} \binom{N}{i} \frac{1}{2}(p_w^i(1-p_w)^{N-i} + p_w^{N-i}(1-p_w)^i) \log[\frac{1}{2}(p_w^i(1-p_w)^{N-i} + p_w^{N-i}(1-p_w)^i)] \\ &= 1 - \frac{1}{2}\sum_{i=0}^{N} \binom{N}{i} (p_w^i(1-p_w)^{N-i} + p_w^{N-i}(1-p_w)^i) \log(p_w^i(1-p_w)^{N-i} + p_w^{N-i}(1-p_w)^i). \end{aligned}$$

Since $p_w \le \frac{1}{2}$, then for any $0 \le i \le N$,

$$p_w^i(1-p_w)^{N-i} + p_w^{N-i}(1-p_w)^i \le p_w^N + (1-p_w)^N.$$

Thus we have

$$\begin{aligned} H(\mathbf{Z}|\mathbf{S}=\mathbf{0}) &\ge 1 - \frac{1}{2}\sum_{i=0}^{N} \binom{N}{i} (p_w^i(1-p_w)^{N-i} + p_w^{N-i}(1-p_w)^i) \log(p_w^N + (1-p_w)^N) \\ &= 1 - \log(p_w^N + (1-p_w)^N) \\ &= 1 - N\log(1-p_w) - \log(1 + (\frac{p_w}{1-p_w})^N) \\ &\ge -N\log(1-p_w). \end{aligned}$$

In addition, we have

$$H(\mathbf{Z}|\mathbf{S}=\mathbf{0}) \overset{(a)}{\le} 1 - \frac{1}{2}\sum_{i=0}^{N} \binom{N}{i} p_w^i(1-p_w)^{N-i} \log p_w^i(1-p_w)^{N-i}$$

$$
\begin{aligned}
& -\frac{1}{2}\sum_{i=0}^{N}\binom{N}{i}p_w^{N-i}(1-p_w)^i\log p_w^{N-i}(1-p_w)^i \\
= \;& 1-\sum_{i=0}^{N}\binom{N}{i}p_w^{i}(1-p_w)^{N-i}\log p_w^{i}(1-p_w)^{N-i} \\
= \;& 1-\sum_{i=0}^{N}\binom{N}{i}p_w^{i}(1-p_w)^{N-i}\log (1-p_w)^{N}(\frac{p_w}{1-p_w})^i \\
= \;& 1-N\log(1-p_w)-\sum_{i=0}^{N} i\binom{N}{i}p_w^{i}(1-p_w)^{N-i}\log\frac{p_w}{1-p_w} \\
\overset{(b)}{=} \;& 1-N\log(1-p_w)-Np_w\log\frac{p_w}{1-p_w} \\
= \;& 1+Nh(p_w), \qquad (5.36)
\end{aligned}
$$

where

(a) follows from the inequality $(x+y)\log(x+y) \geq x\log x + y\log y$ for $x, y > 0$.

(b) follows from the fact that, since $\sum_{i=0}^{N}\binom{N}{i}x^i = (1+x)^N$ and $\sum_{i=0}^{N} i\binom{N}{i}x^i = x(\sum_{i=0}^{N}\binom{N}{i}x^i)'$, we have $\sum_{i=0}^{N} i\binom{N}{i}x^i = Nx(1+x)^{N-1}$.

So far, due to (5.36) and (5.36), we can bound $H(\mathbf{Z}|\mathbf{S}=\mathbf{0})$ as follows:

$$
-N\log(1-p_w) \leq H(\mathbf{Z}|\mathbf{S}=\mathbf{0}) \leq 1+Nh(p_w). \qquad (5.37)
$$

Now let us consider the probability of $\mathbf{z}$. From (5.31) and (5.32), we have

$$
\begin{aligned}
p_{\mathbf{Z}}(\mathbf{z}) &= \frac{1}{2^{K_1}}\sum_{\mathbf{v}\in\mathbf{z}+C_1} p_w^{w(\mathbf{v})}(1-p_w)^{N-w(\mathbf{v})} \\
&= \frac{1}{2^N}\sum_{j=0}^{N}(2a_j(\mathbf{z})-A_j)(1-2p_w)^j.
\end{aligned}
$$

Here $a_j(\mathbf{z})$ is equal to the number of codewords of weight j in the dual code $C_1^{\perp}$ orthogonal to $\mathbf{z}$, and A_j is equal to the number of codewords of weight j in the dual code $C_1^{\perp}$. Note that when C_1 is a binary Hamming code, its dual code $C_1^{\perp}$ has only one all zero codeword $\mathbf{0}$ and N codewords of weight $\frac{N+1}{2}$. Then we have

$$
\begin{aligned}
A_0 &= 1; \\
A_{\frac{N+1}{2}} &= N; \\
A_j &= 0, \quad j \neq 0, \frac{N+1}{2}.
\end{aligned}
$$

If $\mathbf{z} \in C_1$, the coset $\mathbf{z}+C_1$ is C_1 itself. We have

$$
\begin{aligned}
p_{\mathbf{Z}}(\mathbf{z}) &= \frac{1}{2^{K_1}}\sum_{\mathbf{v}\in\mathbf{z}+C_1} p_w^{w(\mathbf{v})}(1-p_w)^{N-w(\mathbf{v})} \\
&= \frac{1}{2^{K_1}}\sum_{\mathbf{v}\in C_1} p_w^{w(\mathbf{v})}(1-p_w)^{N-w(\mathbf{v})}
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{1}{2^N}\sum_{j=0}^{N} A_j(1-2p_w)^j \\
&= \frac{1}{2^N}(1+N(1-2p_w)^{\frac{N+1}{2}}).
\end{aligned}
$$

If $\mathbf{z} \notin C_1$, then $\mathbf{z}$ must be belong to one of cosets of C_1. Suppose $\mathbf{z} \in \mathbf{e}(\mathbf{i}) + C_1$, where $\mathbf{e}(\mathbf{i})$ is the coset leader of $\mathbf{e}(\mathbf{i}) + C_1$. Thus the coset $\mathbf{z} + C_1$ in fact is the same as $\mathbf{e}(\mathbf{i}) + C_1$. It is easy to verify that $a_j(\mathbf{e}(\mathbf{i})) = a_j(\mathbf{z})$, where $a_j(\mathbf{e}(\mathbf{i}))$ is equal to the number of codewords of weight j in the dual code $C_1^{\perp}$ orthogonal to $\mathbf{e}(\mathbf{i})$. Let $m = N - K_1$ and the syndrome of $\mathbf{e}(\mathbf{i})$ be $\mathbf{e}(\mathbf{i}){\mathrm{H}_1}^{\mathrm{T}}$. Assume this syndrome contains k zeros and $m-k$ ones. We have $m - k \geq 1$, since $\mathbf{e}(\mathbf{i}) \notin C_1$. Note that $C_1^{\perp}$ has only N codewords of weight $\frac{N+1}{2}$ except for the sequence $\mathbf{0}$, the number of codewords of weight $\frac{N+1}{2}$ in the code $C_1^{\perp}$ orthogonal to $\mathbf{e}(\mathbf{i})$ can be counted as follows:

$$
\begin{aligned}
a_{\frac{N+1}{2}}(\mathbf{e}(\mathbf{i})) &\overset{(a)}{=} (2^k-1) + [\binom{m-k}{2} + \binom{m-k}{4} + \ldots] \\
&\quad +(2^k-1)[\binom{m-k}{2} + \binom{m-k}{4} + \ldots] \\
&= 2^k[1 + \binom{m-k}{2} + \binom{m-k}{4} + \ldots] - 1 \\
&\overset{(b)}{=} 2^k 2^{m-k-1} - 1 \\
&= 2^{m-1} - 1 \\
&\overset{(c)}{=} \frac{N-1}{2},
\end{aligned}
$$

where

(a) Note that H_1 is the generator matrix of the code $C_1^{\perp}$. The first item $(2^k - 1)$ is the number of possible combinations to yield codewords of weight $\frac{N+1}{2}$ orthogonal to $\mathbf{e}(\mathbf{i})$ from the k codewords orthogonal to $\mathbf{e}(\mathbf{i})$ in H_1. The second item $[\binom{m-k}{2} + \binom{m-k}{4} + \ldots]$ is the number of possible combinations to yield codewords of weight $\frac{N+1}{2}$ orthogonal to $\mathbf{e}(\mathbf{i})$ from the $m-k$ codewords not orthogonal to $\mathbf{e}(\mathbf{i})$ in H_1. The third item is the number of possible choices to yield codewords of weight $\frac{N+1}{2}$ orthogonal to $\mathbf{e}(\mathbf{i})$ from the combinations of the k codewords orthogonal to $\mathbf{e}(\mathbf{i})$ in H_1 and $n-k$ codewords not orthogonal to $\mathbf{e}(\mathbf{i})$ in H_1.

(b) follows the fact that $1 + \binom{m-k}{2} + \binom{m-k}{4} + \ldots = 2^{m-k-1}$, here $m - k \geq 1$ and $\binom{m-k}{i} = 0$, if $m - k < i$.

(c) follows the fact that $N = 2^m - 1$, since C_1 is a binary Hamming code.

Thus, when $\mathbf{z} \notin C_1$, we have

$$
\begin{aligned}
a_0(\mathbf{z}) &= 1; \\
a_{\frac{N+1}{2}}(\mathbf{z}) &= \frac{N-1}{2}; \\
a_j(\mathbf{z}) &= 0, \quad \text{where } j \neq 0, \frac{N+1}{2}.
\end{aligned}
$$

The probability of $\mathbf{z}$, when $\mathbf{z} \notin C_1$, can be calculated as follows:

$$\begin{aligned} p_{\mathbf{Z}}(\mathbf{z}) &= \frac{1}{2^{K_1}} \sum_{\mathbf{v} \in \mathbf{z}+C_1} p_w^{w(\mathbf{v})} (1-p_w)^{N-w(\mathbf{v})} \\ &= \frac{1}{2^{K_1}} \sum_{\mathbf{v} \in \mathbf{e}(\mathbf{i})+C_1} p_w^{w(\mathbf{v})} (1-p_w)^{N-w(\mathbf{v})} \\ &= \frac{1}{2^N} \sum_{j=0}^{N} (2a_j(\mathbf{e}(\mathbf{i})) - A_j)(1-2p_w)^j \\ &= \frac{1}{2^N}(1-(1-2p_w)^{\frac{N+1}{2}}). \end{aligned}$$

Now we can draw a conclusion that when C_1 is a binary Hamming code, $\mathbf{Z}$ has the following distribution:

$$p_{\mathbf{Z}}(\mathbf{z}) = \begin{cases} \frac{1}{2^N}(1+N(1-2p_w)^{\frac{N+1}{2}}) & \text{when } \mathbf{z} \in C_1 \\ \frac{1}{2^N}(1-(1-2p_w)^{\frac{N+1}{2}}) & \text{when } \mathbf{z} \notin C_1 \end{cases}. \tag{5.38}$$

Therefore,

$$\begin{aligned} H(\mathbf{Z}) &= -\sum_{\mathbf{z} \in \{0,1\}^N} p_{\mathbf{Z}}(\mathbf{z}) \log p_{\mathbf{Z}}(\mathbf{z}) \\ &= -\sum_{\mathbf{z} \in C_1} p_{\mathbf{Z}}(\mathbf{z}) \log p_{\mathbf{Z}}(\mathbf{z}) - \sum_{\mathbf{z} \notin C_1} p_{\mathbf{Z}}(\mathbf{z}) \log p_{\mathbf{Z}}(\mathbf{z}) \\ &= \frac{2^{K_1}}{2^N}(1+N(1-2p_w)^{\frac{N+1}{2}}) \log \frac{2^N}{1+N(1-2p_w)^{\frac{N+1}{2}}} \\ &\quad + \frac{2^N - 2^{K_1}}{2^N}(1-(1-2p_w)^{\frac{N+1}{2}}) \log \frac{2^N}{1-(1-2p_w)^{\frac{N+1}{2}}} \\ &= N - \frac{2^{K_1}}{2^N}(1+N(1-2p_w)^{\frac{N+1}{2}}) \log(1+N(1-2p_w)^{\frac{N+1}{2}}) \\ &\quad - \frac{2^N - 2^{K_1}}{2^N}(1-(1-2p_w)^{\frac{N+1}{2}}) \log(1-(1-2p_w)^{\frac{N+1}{2}}) \\ &= N - \frac{1}{N+1}(1+N(1-2p_w)^{\frac{N+1}{2}}) \log(1+N(1-2p_w)^{\frac{N+1}{2}}) \\ &\quad - \frac{N}{N+1}(1-(1-2p_w)^{\frac{N+1}{2}}) \log(1-(1-2p_w)^{\frac{N+1}{2}}). \end{aligned}$$

Clearly, $H(\mathbf{Z}) \leq N$ and

$$\begin{aligned} H(\mathbf{Z}) &\overset{(a)}{\geq} N - \frac{N}{N+1}(1-2p_w)^{\frac{N+1}{2}}(1+N(1-2p_w)^{\frac{N+1}{2}}) \\ &\quad + \frac{N}{N+1}(1-2p_w)^{\frac{N+1}{2}}(1-(1-2p_w)^{\frac{N+1}{2}}) \\ &= N(1-(1-2p_w)^{N+1}), \end{aligned} \tag{5.39}$$

where (a) follows from the inequality $\log x \leq x-1$ for $x \geq 0$.

So far, we can calculate the equivocation d from (5.35) by knowing $H(\mathbf{Z}|\mathbf{S}=\mathbf{0})$ and $H(\mathbf{Z})$. In particular, for fixed p_w, as N approaching infinity, the equivocation d can be bounded as follows.

$$-\log(1-p_w) \leq \lim_{N\to\infty} d \leq h(p_w). \tag{5.40}$$

The proof is the following. From (5.35), (5.37) and (5.39),

$$\begin{aligned} d &= 1 - \frac{H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S}=\mathbf{0})}{N - \log(N+1) - 1} \\ &\geq 1 - \frac{N(1+\log(1-p_w))}{N - \log(N+1) - 1} \\ &\to -\log(1-p_w) \quad \text{as} \quad N \to \infty; \end{aligned}$$

$$\begin{aligned} d &\leq 1 - \frac{N - N(1-2p_w)^{N+1} - 1 - Nh(p_w)}{N - \log(N+1) - 1} \\ &= 1 - \frac{N-1}{N - \log(N+1) - 1} + \frac{N(h(p_w) + (1-2p_w)^{N+1})}{N - \log(N+1) - 1} \\ &\to h(p_w) \quad \text{as} \quad N \to \infty. \end{aligned}$$

As we see in Figure 5.5, when we use a Hamming code C_1 and a repetition code C_2 for the wiretap channel, as N increases, the equivocation d could behave quite differently with respect to different values of p_w. However, as N becomes larger, d changes slower and seems to converge. Besides, for fixed N, we can always gain more equivocation d as p_w increases.

5.5.2 C_1 spans the whole space $\{0,1\}^N$

Consider the degraded case when the main channel is noiseless, i.e., $p = 0$. Let C_1 span the whole space $\{0,1\}^N$. It is clear that $K_1 = N$ and $P_e = 0$. In this case, the coding strategy is the same as the one given by Wyner [1]. Here, we will show the performance of the coding scheme when C_2 is a binary Hamming code or a repetition code.

C_2 is a Hamming code.

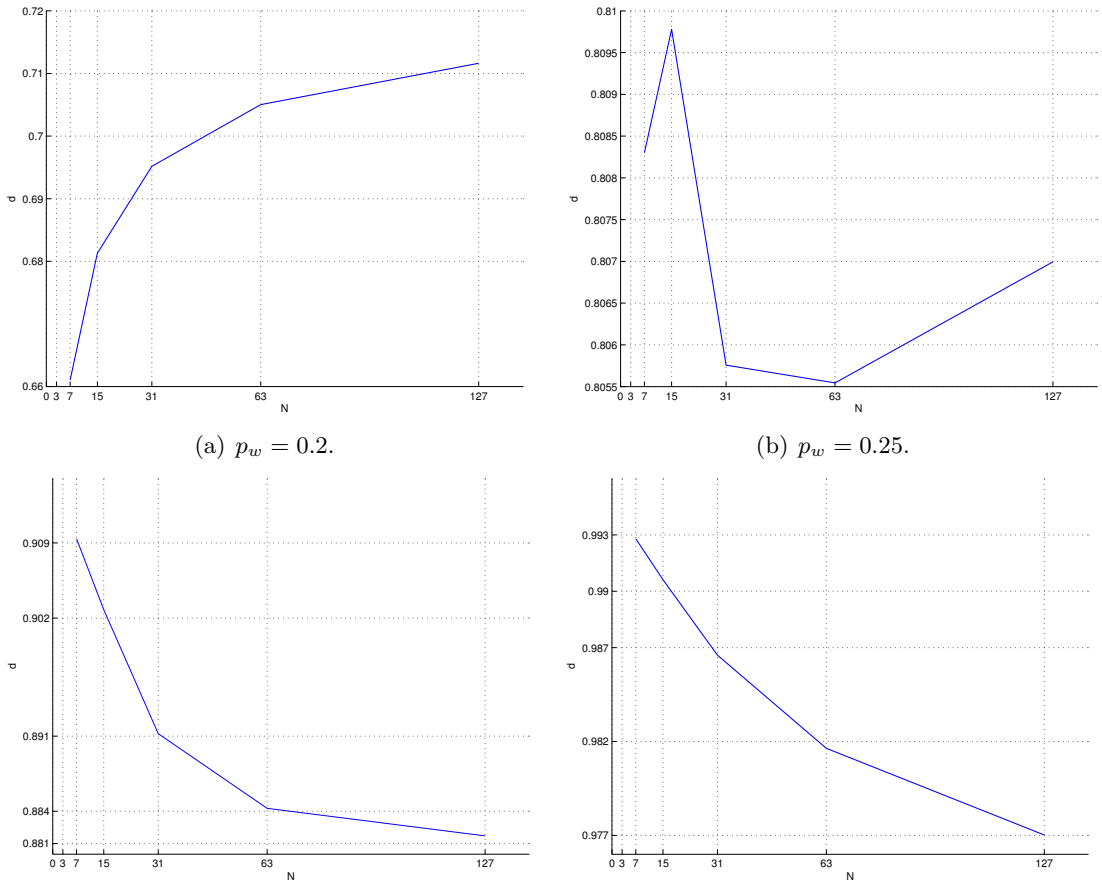
First we consider the efficiency. Since C_2 is a Hamming code, then $N = 2^{N-K_2} - 1$, i.e., $K_2 = N - \log(N+1)$. Thus we have $K = K_1 - K_2 = \log(N+1)$. The rate

$$R = \frac{K}{N} = \frac{\log(N+1)}{N}.$$

It is clear that R is decreasing with respect to N.

Now let us consider the security. From (5.25) and Lemma 5.4.2, we can calculate the equivocation as follows:

$$d = 1 - \frac{H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S})}{K} = 1 - \frac{H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S}=\mathbf{0})}{\log(N+1)}. \tag{5.41}$$



(a) $p_w = 0.2$.

(b) $p_w = 0.25$.

(c) $p_w = 0.3$.

(d) $p_w = 0.4$.

Figure 5.5: Equivocation d with respect to N, when C_1 is a Hamming code of length N, C_2 is a repetition code.

Since C_1 spans the whole space $\{0,1\}^N$ and the wiretap channel is a BSC, $\mathbf{Z}$ is uniformly distributed in the space $\{0,1\}^N$ due to the encoding strategy. Thus we have $H(\mathbf{Z}) = N$.

Since C_2 is a binary Hamming code, we have

$$\begin{aligned} p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0})) &= \frac{1}{2^{K_2}} \sum_{\mathbf{v}\in\mathbf{z}+C_2} p_w^{w(\mathbf{v})}(1-p_w)^{N-w(\mathbf{v})} \\ &= \begin{cases} \frac{1}{2^N}(1+N(1-2p_w)^{\frac{N+1}{2}}) & \text{when } \mathbf{z}\in C_2 \\ \frac{1}{2^N}(1-(1-2p_w)^{\frac{N+1}{2}}) & \text{when } \mathbf{z}\notin C_2 \end{cases}. \end{aligned}$$

Therefore,

$$\begin{aligned} H(\mathbf{Z}|\mathbf{S}=\mathbf{0}) &= -\sum_{\mathbf{z}\in\{0,1\}^N} p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0}))\log p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0})) \\ &= -\sum_{\mathbf{z}\in C_2} p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0}))\log p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0})) - \sum_{\mathbf{z}\notin C_2} p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0}))\log p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0})) \\ &= \frac{2^{K_2}}{2^N}(1+N(1-2p_w)^{\frac{N+1}{2}})\log\frac{2^N}{1+N(1-2p_w)^{\frac{N+1}{2}}} \\ &\quad +\frac{2^N-2^{K_2}}{2^N}(1-(1-2p_w)^{\frac{N+1}{2}})\log\frac{2^N}{1-(1-2p_w)^{\frac{N+1}{2}}} \\ &= N-\frac{1}{N+1}(1+N(1-2p_w)^{\frac{N+1}{2}})\log(1+N(1-2p_w)^{\frac{N+1}{2}}) \\ &\quad -\frac{N}{N+1}(1-(1-2p_w)^{\frac{N+1}{2}})\log(1-(1-2p_w)^{\frac{N+1}{2}}). \end{aligned}$$

The last equation follows from the fact that $N = 2^{N-K_2}-1$, since C_2 is a binary Hamming code. Similarly to the proof of (5.39), we have

$$N(1-(1-2p_w)^{N+1}) \le H(\mathbf{Z}|\mathbf{S}=\mathbf{0}) \le N. \tag{5.42}$$

So far, we can calculate the equivocation d.

$$\begin{aligned} d &= 1-\frac{H(\mathbf{Z})-H(\mathbf{Z}|\mathbf{S}=\mathbf{0})}{\log(N+1)} \\ &= 1+\frac{(1+N(1-2p_w)^{\frac{N+1}{2}})\log(1+N(1-2p_w)^{\frac{N+1}{2}})}{(N+1)\log(N+1)} \\ &\quad +\frac{N(1-(1-2p_w)^{\frac{N+1}{2}})\log(1-(1-2p_w)^{\frac{N+1}{2}})}{(N+1)\log(N+1)}. \end{aligned}$$

Furthermore, we can bound d as follows:

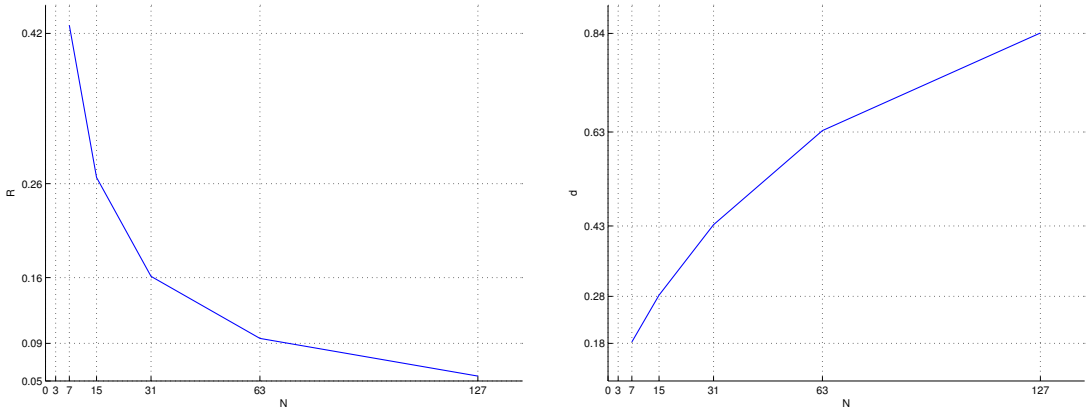
$$\begin{aligned} d &= 1-\frac{H(\mathbf{Z})-H(\mathbf{Z}|\mathbf{S}=\mathbf{0})}{\log(N+1)} \\ &\ge 1-\frac{N-N+N(1-2p_w)^{N+1}}{\log(N+1)} \end{aligned}$$

$$
\begin{aligned}
&= 1 - \frac{N}{\log(N+1)}(1-2p_w)^{N+1} \\
&\to 1 \quad \text{as} \quad N \to \infty.
\end{aligned}
$$

Therefore, when C_2 is a Hamming code, we have

$$\lim_{N\to\infty} d = 1. \tag{5.43}$$

As we see in Figure 5.6, as N becomes larger, the rate R decreases while the equivocation d increases. The family of codes offers good security, in the manner that the perfect secrecy can be asymptotically achieved by increasing the code length N. However, low efficiency is its disadvantage.



(a) R w.r.t N.

(b) d w.r.t N when $p_w = 0.01$.

Figure 5.6: Rate R and equivocation d with respect to N, when C_1 spans the whole space, C_2 is a Hamming code of length N.

C_2 is a repetition code.

First we consider the efficiency. Since C_2 is a repetition code, then $K_2 = 1$. Thus we have $K = K_1 - K_2 = N - 1$. The rate

$$R = \frac{K}{N} = \frac{N-1}{N} = 1 - \frac{1}{N}.$$

It is clear that R is closer to 1 as N increases.

Now let us consider the security. From (5.25) and Lemma 5.4.2, we can calculate the equivocation as follows:

$$d = 1 - \frac{H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S})}{K} = 1 - \frac{H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S}=\mathbf{0})}{N-1}. \tag{5.44}$$

Since C_1 spans the whole space $\{0,1\}^N$ and the wiretap channel is a BSC, $\mathbf{Z}$ is uniformly distributed in the space $\{0,1\}^N$ due to the encoding strategy. Thus we have $H(\mathbf{Z}) = N$.

Since C_2 is a repetition code, we have

$$\begin{aligned} p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0})) &= \frac{1}{2^{K_2}} \sum_{\mathbf{v}\in\mathbf{z}+C_2} p_w^{w(\mathbf{v})}(1-p_w)^{N-w(\mathbf{v})} \\ &= \frac{1}{2^{K_2}}(p_w^{w(\mathbf{z})}(1-p_w)^{N-w(\mathbf{z})} + p_w^{N-w(\mathbf{z})}(1-p_w)^{w(\mathbf{z})}). \end{aligned}$$

Therefore,

$$H(\mathbf{Z}|\mathbf{S}=\mathbf{0}) = -\sum_{\mathbf{z}\in\{0,1\}^N} p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0})) \log p_{\mathbf{Z}|\mathbf{S}}(\mathbf{z}|\mathbf{s}(\mathbf{0}))$$

$$= 1 - \frac{1}{2}\sum_{i=0}^{N} \binom{N}{i} (p_w^i(1-p_w)^{N-i} + p_w^{N-i}(1-p_w)^i) \log(p_w^i(1-p_w)^{N-i} + p_w^{N-i}(1-p_w)^i).$$

Similarly to the proof of (5.36) and (5.36), we have

$$-N\log(1-p_w) \le H(\mathbf{Z}|\mathbf{S}=\mathbf{0}) \le 1 + Nh(p_w). \tag{5.45}$$

So far, we can calculate the equivocation d.

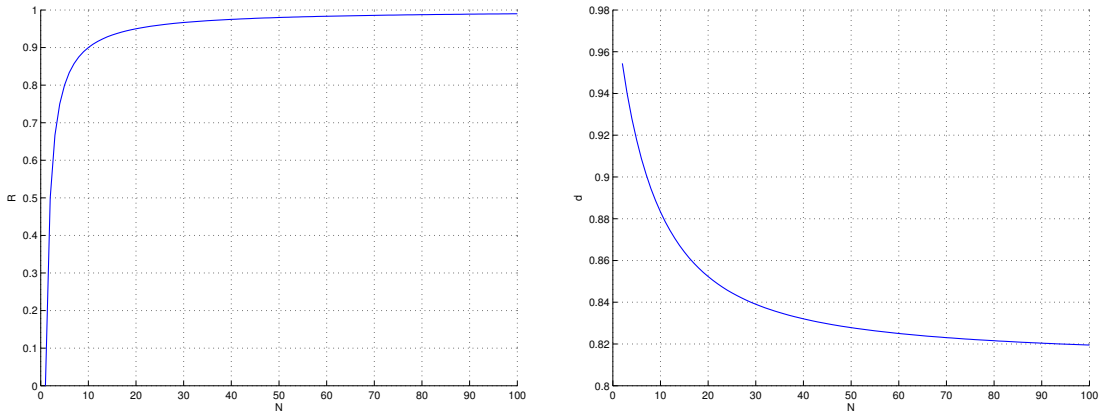
$$\begin{aligned} d &= 1 - \frac{H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S}=\mathbf{0})}{N-1} \\ &= \frac{\sum_{i=0}^{N}\binom{N}{i}(p_w^i(1-p_w)^{N-i} + p_w^{N-i}(1-p_w)^i)\log(p_w^i(1-p_w)^{N-i} + p_w^{N-i}(1-p_w)^i)}{2(N-1)}. \end{aligned}$$

Furthermore, we can bound d as follows:

$$\begin{aligned} d &= 1 - \frac{H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S}=\mathbf{0})}{N-1} \\ &\ge 1 - \frac{N + N\log(1-p_w)}{N-1} \\ &= -\frac{N\log(1-p_w)+1}{N-1} \\ &\to -\log(1-p_w) \quad \text{as} \quad N\to\infty; \end{aligned}$$

$$\begin{aligned} d &\le 1 - \frac{N-1-Nh(p_w)}{N-1} \\ &= \frac{Nh(p_w)}{N-1} \\ &\to h(p_w) \quad \text{as} \quad N\to\infty. \end{aligned}$$

As we see in Figure 5.7, as N becomes larger, the rate R increases while the equivocation d decreases. The family of codes offers good efficiency, in the manner that the rate approaches to the capacity of the main channel by increasing the code length N. Note that in this case, perfect secrecy can not be achieved. However, as we have shown above, the equivocation up to $-\log(1-p_w)$ can be always guaranteed.



(a) R w.r.t N.

(b) d w.r.t N when $p_w = 0.25$.

Figure 5.7: Rate R and equivocation d with respect to N, when C_1 spans the whole space, C_2 is a repetition code.

5.5.3 Example

Choose

$$\mathrm{H}_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}; \quad \mathrm{H} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

We construct H_2 as follows:

$$\mathrm{H}_2 = \begin{bmatrix} \mathrm{H}_1 \\ \mathrm{H} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Let C_1 be the $(7, 4)$ Hamming code and C_2 be the $(7, 1)$ repetition code. It is clear that H_1 is a parity check matrix of C_1. The code generated by H_2 is the $(7, 6)$ even weight code, whose dual code is C_2. The codebook in the encoding scheme is shown in Table 5.2.

The efficiency. Since $N = 7$, $K_1 = 4$, $K_2 = 1$ and $K = K_1 - K_2 = 3$, the rate of the transmission is

$$R = \frac{K}{N} = \frac{3}{7}.$$

The reliability. Since C_1 is a binary Hamming code and C_2 is a repetition code, from (5.34), the error probability of decoding can be calculated as

$$P_e = 1 - [(1-p)^7 + 7p(1-p)^6 + p^7 + 7(1-p)p^6].$$

Table 5.2: The codebook in the encoding scheme with $N = 7, K = 3$

Space of input $\mathbf{x}$	Secret $\mathbf{s}$	Set of codewords corresponding to secret $\mathbf{s}$
C_1	000	{0000000, 1111111}
	001	{0101101, 1010010}
	010	{0001011, 1110100}
	011	{0110001, 1001110}
	100	{0010111, 1101000}
	101	{0111010, 1000101}
	110	{0011100, 1100011}
	111	{0100110, 1011001}

The security. From (5.35), the equivocation

$$d = 1 - \frac{H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{S} = \mathbf{0})}{3},$$

where

$$H(\mathbf{Z}|\mathbf{S} = \mathbf{0}) = 1 - \frac{1}{2}\sum_{i=0}^{7} \binom{7}{i} (p_w^i(1-p_w)^{7-i} + p_w^{7-i}(1-p_w)^i) \log(p_w^i(1-p_w)^{7-i} + p_w^{7-i}(1-p_w)^i);$$

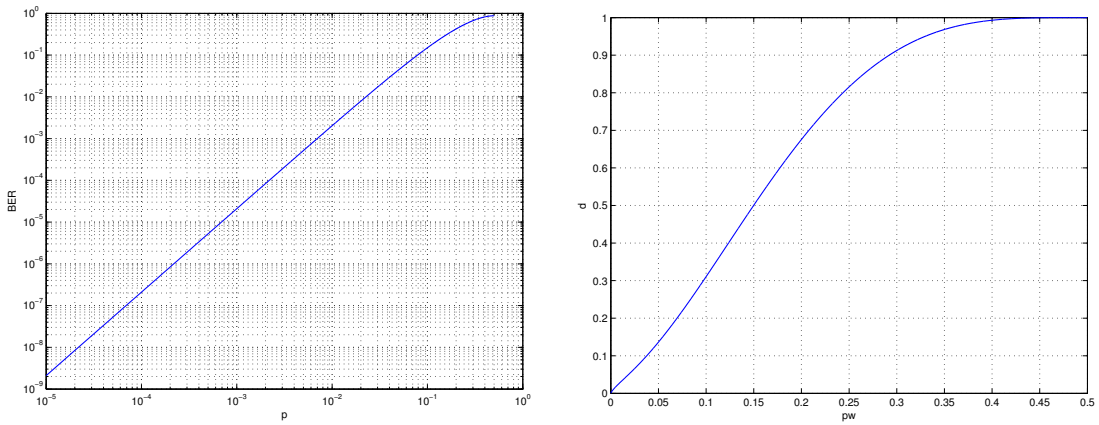
$$H(\mathbf{Z}) = 7 - \frac{1}{8}(1+7(1-2p_w)^4)\log(1+7(1-2p_w)^4) - \frac{7}{8}(1-(1-2p_w)^4)\log(1-(1-2p_w)^4).$$

The performance of this coding scheme is shown in Figure 5.8 for different main channel and wiretap channels.

5.6 Concluding remarks

In this chapter, we focus on the problem of developing coding schemes for secure communication across the wiretap channel. We investigate the specific case when both the main channel and the wiretap channel are BSCs. We show that the secrecy capacity can be achieved by using random linear codes. The coding method used in our proof is not strictly new. It is contained in the proof as given by Wyner [1] for the special case when the main channel is noiseless and the wiretap channel is a BSC. Note that for the case investigated by Wyner [1], the transmitter need not to think of the reliability of the transmission to the legitimate receiver since the main channel is noiseless. However, in our case, we need a secrecy capacity achieving coding scheme which guarantees both the reliability and the security of the wiretap channel at the same time.

Theoretically, the secrecy capacity is shown to be achievable by using random linear codes. However, the decoder used in the proof is not easy to implement. For practical purpose, we use linear codes of short code length for the wiretap channel. Their performance is evaluated from the perspectives of the efficiency, reliability and security, which are measured by the rate, the error probability of decoding and the equivocation of the wiretapper, respectively. In particular, we show the performance evaluation when Hamming codes and repetition codes are used in our construction.



(a) P_e w.r.t p.

(b) d w.r.t p_w.

Figure 5.8: Error probability P_e and equivocation d with respect to p and p_w, respectively, when C_1 is $(7, 4)$ Hamming code and C_2 is a $(7, 1)$ repetition code.

Chapter 6

Application to Biometrics

Biometric data are said to identify a person based on "who he is", rather than on "what he has" (such as a smartcard) or "what he knows" (such as a password). Since biometric properties can not be lost or forgotten in contrast to tokens and passwords, they offer an attractive and convenient alternative to identify and authenticate people. In this chapter, a fuzzy commitment scheme proposed by Juels and Wattenberg [15] and a modified version by Cohen and Zémor [16] are reviewed. In particular, for practical purpose, we consider the case when linear codes of short code length are used in the scheme of Cohen and Zémor. As noted in [16], the security problem in biometrics can be reformulated as a communication problem for the wiretap channel. Using the terminologies for the wiretap channel, we give an information theoretic security analysis for both schemes.

6.1 Introduction

In biometrics, a human being needs to be identified by measuring a set of parameters of the body, such as DNA, fingerprints, face and iris features. At enrollment, the biometric of a person is measured and a derived template is encoded in reference information and stored in a database. At the authentication phase, a server measures a biometric, retrieves the corresponding reference information from the database and performs a match. We assume that the database is publicly accessible. Then, it is desirable that no information on the biometric template is leaked to a third party.

Note that changes occur naturally in biological characteristics over time. Additionally, successive biometrical measures of the same person always tend to differ slightly. Therefore, protecting the biometrical data through a straightforward means of commitment like hashing is not possible. The reason is that small changes in input values to a hash function will yield large and unpredictable changes in output values and thus results in a rejection. So at the authentication phase, not only the original biometric template but also the slightly modified version should be accepted.

To solve this problem, Juels and Wattenberg [15] introduced a fuzzy commitment scheme, whose construction is based on the error-correcting codes and tolerates small errors in biometric templates. Their scheme enjoys rigorous provable information-theoretic security for uniformly distributed biometric templates. However, in practice, the distribution of the biometric templates may be far from uniform. For that case, Cohen and Zémor [16] proposed a generalized coset scheme, where they remodelled the problem in biometrics as a communication problem over the wiretap channel. Their scheme involves random codes

with an unacceptable decoding complexity and thus is impractical. In [60], a concrete system based on the scheme of Juels and Wattenberg [15] is proposed for iris scans. Their work is reported to generate up to 140-bit biometric key with 0.47% false rejection rate.

However, the scheme of Juels and Wattenberg [15] does not tolerate translation and rotation errors. Any elements missing or adding will also result in the failure of matching. To overcome these problems, Juels and Sudan [58] proposed a new architecture. In contrast to the scheme of Juels and Wattenberg [15] which is based on the Hamming metric, their construction is based on the set difference metric and hence possesses the advantage of order invariance. The security of this scheme is based on the infeasibility of the polynomial reconstruction problem. In [59], Dodis et al. modified the scheme of Juels and Sudan [58] and provided a strict security analysis for both, the original scheme and the modified version. The modified scheme has the advantages of lower storage and being easier to analyze. Since the scheme of Juels and Sudan [58] enjoys the property of order invariance, it is a promising candidate for biometric cryptosystems. In [62], Clancy et al. proposed an application using fingerprints based on the scheme of Juels and Sudan [58]. Their work is reported to derive a 69-bit biometric key but unfortunately with 30% false rejection rate. Furthermore, their scheme inherently assumes that fingerprints are pre-aligned. This is not a realistic assumption due to different types of distortion that can occur in biometric data acquisition.

A different approach has been taken by Linnartz and Tuyls in [61], where they focused on the continuous space and assumes a particular continuous distribution (typically a Gaussian distribution) on the biometric template. Their work was later generalized by Dodis et al. in [59], where the authors focused on discrete metric spaces.

In this chapter, we will focus our attention on the scheme of Juels and Wattenberg [15] and a modified version by Cohen and Zémor [16]. Review the security problem in biometrics as a communication problem for the wiretap channel. We provide an information theoretic sense security analysis by using the terminologies for the wiretap channel.

6.2 Juels-Wattenberg scheme

Let C be a binary linear code. The Juels-Wattenberg scheme is as follows.

- At enrollment, randomly choose a k-bit secret vector $\mathbf{s}$ and encode it as an n-bit codeword $\mathbf{c}$, where $\mathbf{c} \in C$.
- Store the vector $\mathbf{w} = \mathbf{c} + \mathbf{b}$ and the Hash value of $\mathbf{c}$. Here $\mathbf{b}$ is the submitted biometric template.
- At the authentication phase, when $\mathbf{b}' = \mathbf{b} + \mathbf{e}$ is submitted, add it to $\mathbf{w}$ and yield a noisy version $\mathbf{c} + \mathbf{e}$ of $\mathbf{c}$. Decode $\mathbf{c} + \mathbf{e}$ as $\mathbf{c}'$. Clearly, correct decoding delivers $\mathbf{c}' = \mathbf{c}$.
- Validity is checked by calculating the Hash value of $\mathbf{c}'$ and comparing it to the stored Hash value of $\mathbf{c}$.

Note that in the Juels-Wattenberg scheme [15], $\mathbf{c}, \mathbf{b}$ and $\mathbf{b}'$ are all binary vectors.

Consider $\mathbf{w} = \mathbf{c} + \mathbf{b}$ as a very noisy version of the secret codeword $\mathbf{c}$. Since $\mathbf{w}$ is stored in the database, a third party, i.e., a wiretapper may have access to $\mathbf{w}$. Furthermore, for the legitimate user who has submitted $\mathbf{b}$ at enrollment, when he submits $\mathbf{b}'$ at the authentication phase, we consider him to have access to a less noisy version $\mathbf{c} + \mathbf{e}$ of the secret codeword $\mathbf{c}$. Here $\mathbf{e}$ is the noise due to the biometric instability and $\mathbf{e} = \mathbf{b} + \mathbf{b}'$. Our main concern is to

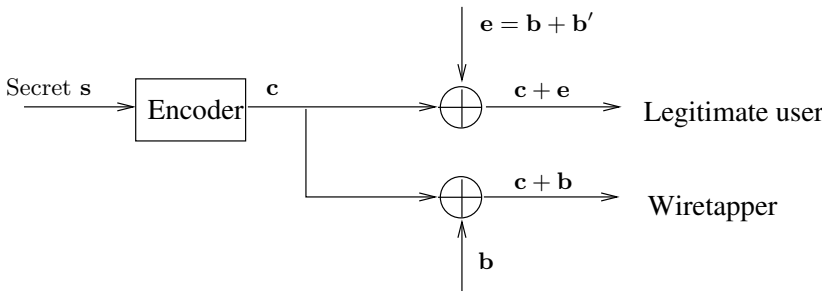


Figure 6.1: The reformulation of the Juels-Wattenberg scheme as a wiretap channel.

insure no leakage of the secret information to the wiretapper. As noted in [16], this problem can be remodelled as that of maximizing the amount of information that can be reliably transmitted through the less noisy "channel" with maximum "equivocation", i.e., insuring that the wiretapper gets essentially no information on the secret data. Thus, as shown in Figure 6.1, the security problem in biometrics can be reformulated as a communication problem for the wiretap channel. From the results given by Wyner [1], the secrecy capacity of this wiretap channel $\max_{p(\mathbf{c})}[I(\mathbf{c}; \mathbf{c}+\mathbf{e}) - I(\mathbf{c}; \mathbf{c}+\mathbf{b})]$.

6.3 Security analysis of Juels-Wattenberg scheme

One of the important properties of the Juels-Wattenberg Scheme is "fuzziness", which means that the scheme is resilient to small corruptions in the biometric templates. More precisely, in their scheme, the corruption is measured by Hamming distance and the "fuzziness" property is achieved by using an error-correcting code C. In fact, the resilience of a fuzzy commitment scheme is bounded by the error-correcting capability of code C used in its construction.

Now we consider the information leakage problem as a wiretap problem and characterize the performance of the Juels-Wattenberg scheme with the terminologies for the wiretap channel. Referring to Figure 6.1, we calculate the rate R to the legitimate user and the equivocation d of the wiretapper as follows:

$$\begin{aligned} R &= \frac{k}{n}; \\ d &= \frac{H(\mathbf{c}|\mathbf{c}+\mathbf{b})}{H(\mathbf{c})} = 1 - \frac{I(\mathbf{c}; \mathbf{c}+\mathbf{b})}{H(\mathbf{c})}. \end{aligned}$$

Note that in the idealized setting of [15], the biometric vector $\mathbf{b}$ is assumed to be uniformly distributed among vectors of a given length n. It is easy to verify that $\mathbf{c}+\mathbf{b}$ is also uniformly distributed in $\{0,1\}^n$. So we have

$$H(\mathbf{b}+\mathbf{c}) = H(\mathbf{b}) = n.$$

Therefore,

$$\begin{aligned} I(\mathbf{c}; \mathbf{c}+\mathbf{b}) &= H(\mathbf{c}+\mathbf{b}) - H(\mathbf{c}+\mathbf{b}|\mathbf{c}) \\ &= H(\mathbf{c}+\mathbf{b}) - H(\mathbf{b}|\mathbf{c}) \end{aligned}$$

$$
\begin{aligned}
&= H(\mathbf{c}+\mathbf{b}) - H(\mathbf{b}) \\
&= n - n \\
&= 0.
\end{aligned}
$$

Thus we have

$$d = 1 - \frac{I(\mathbf{c}; \mathbf{c}+\mathbf{b})}{H(\mathbf{c})} = 1.$$

In this case, the vector $\mathbf{c}+\mathbf{b}$ yields no information on the secret codeword $\mathbf{c}$ or the original secret $\mathbf{s}$. Note that there is no assumption on the distribution of $\mathbf{c}$. If $\mathbf{b}$ is uniformly distributed, then from $\mathbf{c}+\mathbf{b}$ there is no information leakage on $\mathbf{c}$, regardless of whatever distribution $\mathbf{c}$ has. However, in practice, the distribution of $\mathbf{b}$ may be far from uniform and in that case, $\mathbf{c}+\mathbf{b}$ is liable to leak undesirable partial knowledge of $\mathbf{c}$, and hence of $\mathbf{s}$, to an unauthorized third party.

As we have discussed above, we consider the information leakage problem in biometrics as a wiretap problem and give a security proof in the information theoretic sense. Note that the rate of the wiretap channel is corresponding to the storage of the commitment scheme. In order to save the storage of the database at a certain security level, it is equivalent to design a code to achieve the higher rate to the legitimate user with the same equivocation of the wiretapper. Besides, the equivocation of the wiretapper shows how much information on the secret is accessible to a third party. Higher equivocation corresponds to less information leakage and offers better security. Especially, the equivocation $d = 1$ implies the perfect secrecy. It is clear that for the general case when $\mathbf{b}$ is not uniformly distributed, the perfect secrecy can not be guaranteed by the scheme.

6.4 A modified fuzzy commitment scheme

A modified fuzzy commitment scheme is proposed by Cohen and Zémor [16] for the general case when $\mathbf{b}$ is not uniformly distributed. It is a secrecy capacity achieving fuzzy commitment scheme, whose security is based on the random coding argument for the wiretap channel. However, it requires a decoder with unacceptable decoding complexity. Furthermore, it is based on the hypothesis that there exists a typical set T of typical biometric templates $\mathbf{b}$ such that the probability $\Pr(\mathbf{b} \notin T)$ decreases exponentially with the code length n. And the distribution of $\mathbf{b}$ conditional to $\mathbf{b} \in T$ is very close to uniform. Here we mention that as n increases, the storage of the data will increase exponentially and thus the scheme will become impractical. So we need to find the trade-off between the ideality and the reality.

Although the random coding technique is rather impractical, it provides a limit of how far one can go and, often enough, a clue of how a practical scheme may be implemented. Here, instead of random codes, we use linear codes with reasonable length n and analyze its security. Similarly to the parameter settings in last chapter for the wiretap channel when the main channel and the wiretap channel are both noisy, let H_1 be an $n-k_1$ by n binary matrix and H be a k by n binary matrix. Let $k_2 = k_1 - k$. Both H_1 and H are with full rank. Let C_1 be the dual code of the $(n, n-k_1)$ linear code generated by H_1. The modified fuzzy commitment scheme is as follows.

- At enrollment, randomly choose a k-bit secret $\mathbf{s}$. Encode $\mathbf{s}$ as the codeword $\mathbf{c} \in C_1$ such that $\mathbf{c}\mathrm{H}^{\mathrm{T}} = \mathbf{s}$.

- Store the vector $\mathbf{w} = \mathbf{c} + \mathbf{b}$ and the Hash value of $\mathbf{s}$.
- At the authentication phase, when $\mathbf{b}' = \mathbf{b} + \mathbf{e}$ is submitted, add it to $\mathbf{w}$ and yield a noisy version $\mathbf{c} + \mathbf{e}$ of $\mathbf{c}$. Decode $\mathbf{c} + \mathbf{e}$ as $\mathbf{c}'$. Clearly, correct decoding delivers $\mathbf{c}' = \mathbf{c}$ and then $\mathbf{c}'\mathrm{H}^{\mathrm{T}} = \mathbf{s}$.
- Validity is checked by calculating the Hash value of $\mathbf{c}'\mathrm{H}^{\mathrm{T}}$ and comparing it to the stored Hash value of $\mathbf{s}$.

Compare the above scheme with the one given in [16]. The only difference is the setting of H. In [16], H is randomly chosen and here we require that it is of full rank. In fact, by Lemma 5.3.1, as n goes to infinity, a randomly chosen H is of full rank with probability approaching 1. So we can regard the above scheme as the one in [16] in the case that the code length is limited. In particular, we assume that every component of $\mathbf{e}$ and $\mathbf{b}$, denoted as $\mathbf{e_i}$ and $\mathbf{b_j}$, respectively, where $1 \leq i, j \leq N$, has the following distribution:

$$\begin{aligned} \Pr(\mathbf{e_i} = 1) = p, \qquad & \Pr(\mathbf{e_i} = 0) = 1 - p; \\ \Pr(\mathbf{b_j} = 1) = p_b, \qquad & \Pr(\mathbf{b_j} = 0) = 1 - p_b. \end{aligned}$$

Then, the maximal rate without information leakage on the secret data is the secrecy capacity of the wiretap channel: $h(p_b) - h(p)$.

6.5 Security analysis of the modified scheme

Now let us consider the performance of the above scheme. Similarly to the Juels-Wattenberg scheme, the resilience of the modified fuzzy commitment scheme is bounded by the error-correcting capability of code C_1. Furthermore, it is clear that the rate is

$$R = \frac{k}{n}.$$

The equivocation is

$$d = \frac{H(\mathbf{s}|\mathbf{c} + \mathbf{b})}{H(\mathbf{s})}.$$

As analyzed in [17], we have the following lemma.

Lemma 6.5.1 $H(\mathbf{s}|\mathbf{c} + \mathbf{b}) = H(\mathbf{s}|\mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}})$.

Proof: First, since $\mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}$ is a function of $\mathbf{c} + \mathbf{b}$, we have

$$H(\mathbf{s}|\mathbf{c} + \mathbf{b}) \leq H(\mathbf{s}|\mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}).$$

Now let us prove the reverse inequality. Consider

$$\begin{aligned} H(\mathbf{s}|\mathbf{c} + \mathbf{b}) - H(\mathbf{s}|\mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}) &= H(\mathbf{s}, \mathbf{c} + \mathbf{b}) - H(\mathbf{c} + \mathbf{b}) - H(\mathbf{s}, \mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}) + H(\mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}) \\ &= H(\mathbf{s}, \mathbf{c} + \mathbf{b}, \mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}) - H(\mathbf{s}, \mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}) \\ &\quad -H(\mathbf{c} + \mathbf{b}, \mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}) + H(\mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}) \\ &= H(\mathbf{c} + \mathbf{b}|\mathbf{s}, \mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}) - H(\mathbf{c} + \mathbf{b}|\mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}) \\ &\geq H(\mathbf{c} + \mathbf{b}|\mathbf{s}, \mathbf{b}) - H(\mathbf{c} + \mathbf{b}|\mathbf{s} + \mathbf{b}\mathrm{H}^{\mathrm{T}}) \end{aligned}$$

$$
\begin{aligned}
&= H(\mathbf{c}|\mathbf{s},\mathbf{b}) - H(\mathbf{c}+\mathbf{b}|\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}}) \\
&= H(\mathbf{c}|\mathbf{s}) - H(\mathbf{c}+\mathbf{b}|\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}}) \\
&\geq 0.
\end{aligned}
$$

The last inequality is due to $\mathbf{c}$ being chosen randomly from the codewords such that $\mathbf{c} \in C_1$ and $\mathbf{c}\mathrm{H}^{\mathrm{T}} = \mathbf{s}$.

Thus we have proved that $H(\mathbf{s}|\mathbf{c}+\mathbf{b}) = H(\mathbf{s}|\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}})$. In other words, there is no advantage for the wiretapper in possessing $\mathbf{c}+\mathbf{b}$ on top of its syndrome. ■

By Lemma 6.5.1, the equivocation can be calculated as follows.

$$
d = \frac{H(\mathbf{s}|\mathbf{c}+\mathbf{b})}{H(\mathbf{s})} = \frac{H(\mathbf{s}|\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}})}{H(\mathbf{s})} = 1 - \frac{I(\mathbf{s};\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}})}{H(\mathbf{s})}.
$$

Note that

$$
\begin{aligned}
I(\mathbf{s};\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}}) &= H(\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}}) - H(\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}}|\mathbf{s}) \\
&= H(\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}}) - H(\mathbf{b}\mathrm{H}^{\mathrm{T}}|\mathbf{s}) \\
&= H(\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}}) - H(\mathbf{b}\mathrm{H}^{\mathrm{T}}) \\
&= k - H(\mathbf{b}\mathrm{H}^{\mathrm{T}}).
\end{aligned}
$$

The last equation follows from the fact that since $\mathbf{s}$ is uniformly distributed, $H(\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}}) = H(\mathbf{s}) = k$. Now, we could simplify the calculation of the equivocation as follows.

$$
d = 1 - \frac{I(\mathbf{s};\mathbf{s}+\mathbf{b}\mathrm{H}^{\mathrm{T}})}{H(\mathbf{s})} = 1 - \frac{k - H(\mathbf{b}\mathrm{H}^{\mathrm{T}})}{k} = \frac{H(\mathbf{b}\mathrm{H}^{\mathrm{T}})}{k}.
$$

Clearly, in order to guarantee perfect secrecy on the secret $\mathbf{s}$, we need

$$
d = 1 \quad \Leftrightarrow \quad H(\mathbf{b}\mathrm{H}^{\mathrm{T}}) = k.
$$

This give us some insight into the choice H so as to yield as high as possible security. That is, the best choice of H for this scheme is the one so that $\mathbf{b}\mathrm{H}^{\mathrm{T}}$ is uniformly distributed, or as close as possible to be uniformly distributed.

6.6 Concluding remarks

In this chapter, a fuzzy commitment scheme by Juels and Wattenberg [15] and a modified version by Cohen and Zémor [16] are reviewed. Note that we use binary codes in both schemes. We point out that both schemes are easy to extend by using linear codes over arbitrary finite fields. Furthermore, the information leakage problem in biometrics is modelled as a wiretap problem. For the Juels-Wattenberg scheme, an information theoretic security proof is provided. For the modified version given by Cohen and Zémor [16], we consider the practical case when linear codes of reasonable length are used in the scheme. At last but not least, we give some insight into the choice of the parameters C_1 and H so that the scheme has good performance in resilience, storage and security.

Chapter 7

Conclusions

7.1 Summary of the thesis

In this thesis, we explore the security capacity and the capacity region for the wiretap channel with side information. For the discrete memoryless case, we give a bound for the secrecy capacity and an achievable rate equivocation region. In particular, the secrecy capacity in some special cases is determined.

We extend our result for the discrete memoryless case to the Gaussian case. Our contribution to the Gaussian wiretap channel with side information is twofold. First, we derive an achievable rate equivocation region $\mathcal{R}_\perp$ by using Costa's strategy. We compare it with the region $\mathcal{R}_L$ for the Gaussian wiretap channel given by Leung-Yan-Cheong and Hellman [4, Theorem 1]. We draw a conclusion that for the Gaussian wiretap channel, side information helps to get a larger secrecy capacity and achieve a larger rate equivocation region. Furthermore, we generalize Costa's strategy by taking the correlation coefficient of the codeword and side information as another parameter into our consideration. The region $\mathcal{R}_\perp$ is improved by using the generalized Costa's strategy. That is, for the Gaussian wiretap channel, it is a better choice in some cases to send a codeword dependent on side information, in order to yield higher secret rate with the same equivocation. In addition, we give the best choice of the correlation coefficient for the generalized Costa's strategy to achieve the maximal rate at the perfect secrecy.

In this thesis, we also investigate the problem of developing forward coding schemes for secure communication over the wiretap channel. A code construction is considered for the specific case when both the main channel and the wiretap channel are binary symmetric. Theoretically, we show that the secrecy capacity can be achieved by using random linear codes. For practical purpose, we evaluate the performance of the coding schemes when linear codes especially Hamming codes and repetition codes are used in the construction. The performance is characterized from the perspectives of the efficiency, reliability and security which are measured by the rate, the error probability of decoding and the equivocation of the wiretap, respectively.

As an application, we reformulate the security problem in biometrics as a communication problem for the wiretap channel. A fuzzy commitment scheme by Juels and Wattenberg [15] and a modified version by Cohen and Zémor [16] are reviewed. Both schemes are based on error correcting codes and promise a secure biometric template storage. The performance of the schemes is characterized with the terminologies for the wiretap channel, where high rate corresponds to efficient storage of the protected biometric data and high equivocation

corresponds to low information leakage to a third party. For the Juels-Wattenberg scheme, under the assumption that the biometric template is uniformly distributed, we give a security proof in the information theoretic sense. For the Cohen-Zémor scheme, we focus on the case when linear codes of reasonable length are used in its construction. In particular, we also give some insight into the choice of the parameters so that the scheme has good performance in resilience, storage and security.

7.2 Possible directions for future work

There are still many problems left to solve. For example, for the discrete memoryless wiretap channel with side information, the secrecy capacity is not totally determined and the capacity region remains unknown. Even for the Gaussian wiretap channel with side information, both the secrecy capacity and capacity region problems are not totally solved yet. A theoretical challenge is to enlarge the achievable region or show the converse of the coding theorem.

Note that the secrecy capacity achieving codes are mostly random codes and difficult to implement. For practical purpose, more attention should be paid to the code construction methods which offer high efficiency and high security for reliable communication over the wiretap channel. In this thesis, we explore the wiretap channel in the specific case when both the main channel and the wiretap channel are binary symmetric. In particular, we show the performance when linear codes are used in the construction. Further work is to allow other types of codes to be used in our coding strategy or to design secrecy capacity approaching codes for other special wiretap channels.

Another possible direction for future research is the application to biometrics. Considering the biometric scheme as a communication scheme for the wiretap channel, one can provide a precise evaluation of the performance of the biometric scheme. Furthermore, lighted by our results for the wiretap channel with side information, in order to better design a biometric scheme with efficient storage and high security, it might be helpful to introduce side information noncausally known to the encoder in the scheme.

Bibliography

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

[2] P. P. Bergmans, "Random coding theorem for broadcast channels with degraded components," *IEEE Trans. Info. Theory*, vol. IT-19(2), pp. 197-207, March 1973.

[3] S. K. Leung-Yan-Cheong, "On a special class of wiretap channels," *IEEE Trans. Info. Theory*, vol. IT-23(5), pp. 625-627, September 1977.

[4] S. K. Leung-Yan-Cheong and Martin E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Info. Theory*, vol. IT-24(4), pp. 451-456, July 1978.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. IT-24(3), pp. 339-348, May 1978.

[6] M. van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. IT-43(2), pp. 712-714, March 1997.

[7] Max H. M. Costa, "Writing on dirty paper," *IEEE Trans. Info. Theory*, vol. IT-29(3), pp. 439-441, May 1983.

[8] Chaichana Mitrpant, "Information hiding: an application of wiretap channels with side information," dissertation, University of Essen, Germany, 2004.

[9] Chaichana Mitrpant, A. J. Han Vinck and Yuan Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Info. Theory*, vol. IT-52(5), pp. 2181-2190, May 2006.

[10] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Problems of control and Information Theory*, vol. 9, no. 1, pp. 19-31, 1980.

[11] C. Heegard and A. El Gamal, "On the capacity of computer memory with defects," *IEEE Trans. Info. Theory*, vol. IT-29(5), pp. 731-739, September 1983.

[12] R. Ahlswede and J. Körner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Info. Theory*, vol. IT-21(6), pp. 629-637, November 1975.

[13] E. F. Assmus, Jr., and H. F. Mattson, Jr., "The weight-distribution of a coset of a linear code," *IEEE Trans. Info. Theory*, vol. IT-24(4), pp. 497, July 1978.

[14] Fan Shengjin, "A new extracting formula and a new distinguishing means on the one variable cubic equation," *Natural Science Journal of Hainan Teacher's College*, vol. 2, no. 2, pp. 91-98, December 1989.

[15] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," *Proc. 6th ACM Conf. Computer and Comm. Security*, pp. 28-36, Kent Ridge Digital Labs, Singapore, November 01-04, 1999.

[16] Gérard Cohen and Gilles Zémor, "Generalized coset schemes for the wire-tap channel: application to biometrics," *Proc. IEEE Int. Symp. Inf. Theory*, Chicago, IL, June 27-July 2, 2004.

[17] Gérard Cohen and Gilles Zémor, "Syndrome-coding for the wiretap channel revisited," *Proc. IEEE Inf. Theory Workshop*, Chengdu, China, October 22-26, 2006.

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

[19] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[20] Shu Lin and Daniel J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, New Jersey 07632: Prentice Hall, Inc., 1983.

[21] David MacKay, *Information Theory, Inference and Learning Algorithms*. Cambridge University Press, 2003.

[22] Andrew Thangaraj, Souvik Dihidar, A. R. Calderbank, Steven W. McLaughlin and Jean-Marc Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Info. Theory*, vol. IT-53(8), pp. 2933-2945, August 2007.

[23] T. M. Cover, "Broadcast channels," *IEEE Trans. Info. Theory*, vol. IT-18(1), pp. 2-14, January 1972.

[24] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. Info. Theory*, vol. IT-23(1), pp. 60-64, January 1977.

[25] T. M. Cover, "An achievable rate region for the broadcast channel," *IEEE Trans. Info. Theory*, vol. IT-21(4), pp. 399-404, July 1975.

[26] A. D. Wyner, "A theorem on the entropy of certain binary sequences and applications: Part II," *IEEE Trans. Info. Theory*, vol. IT-19(6), pp. 772-777, November 1973.

[27] P. P. Bergmans, "A simple converse for broadcast channels with additive white Gaussian noise," *IEEE Trans. Info. Theory*, vol. IT-20(2), pp. 279-280, March 1974.

[28] E. C. van der Meulen, "Random coding theorems for the general discrete memoryless broadcast channels," *IEEE Trans. Info. Theory*, vol. IT-21(2), pp. 180-190, March 1975.

[29] T. M. Cover, "Comments on broadcast channels," *IEEE Trans. Info. Theory*, vol. IT-44(6), pp. 2524-2530, October 1998.

[30] E. C. van der Meulen, "A survey of multi-way channels in information theory: 1961-1976," *IEEE Trans. Info. Theory*, vol. IT-23(1), pp. 1-37, January 1977.

[31] J. Körner and K. Marton, "Comparison of two noisy channels," in *Topics in Information Theory*, I. Csiszár and P. Elias, Eds. Amsterdam, The Netherlands: North-Holland, pp. 411-423, 1977.

[32] Kensuke Yasui, Tota Suko and Toshiyasu Matsushima, "An algorithm for computing the secrecy capacity of broadcast channels with confidential messages," *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, June 24-29, 2007.

[33] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Trans. Info. Theory*, vol. IT-49(3), pp. 563-593, March 2003.

[34] A. S. Cohen and A. Lapidoth, "The Gaussian watermarking game," *IEEE Trans. Info. Theory*, vol. IT-48(6), pp. 1639-1667, June 2002.

[35] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Info. Theory*, vol. IT-25(3), pp. 306-311, May 1979.

[36] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna Gaussian broadcast channel," *IEEE Trans. Info. Theory*, vol. IT-49(7), pp. 1691-1706, July 2003.

[37] W. Yu and J. Cioffi, "Sum capacity of Gaussian vector broadcast channels," *IEEE Trans. Info. Theory*, vol. IT-50(9), pp. 1875-1892, September 2004.

[38] P. Viswanath and D. Tse, "Sum capacity of the multiple antenna Gaussian broadcast channel and uplink-downlink duality," *IEEE Trans. Info. Theory*, vol. IT-49(8), pp. 1912-1921, August 2003.

[39] S. Vishwanath, N. Jindal and A. Goldsmith, "Duality, achievable rates, and sum-rate capacity of Gaussian MIMO broadcast channels," *IEEE Trans. Info. Theory*, vol. IT-49(10), pp. 2658-2668, October 2003.

[40] W. Yu, A. Sutivong, D. Julian, T. M. Cover and M. Chiang, "Writing on colored paper," in *Proc. IEEE Int. Symp. Inf. Theory*, Washington D.C., June 24-29, 2001.

[41] R. Zamir, S. Shamai and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Info. Theory*, vol. IT-48(6), pp. 1250-1276, June 2002.

[42] Y. -H. Kim, A. Sutivong and S. Sigurjónsson "Multiple user writing on dirty paper," in *Proc. IEEE Int. Symp. Inf. Theory*, Chicago, IL, June 27-July 2, 2004.

[43] A. B. Carleial and M. E. Hellman, "A note on Wyner's wiretap channel," *IEEE Trans. Info. Theory*, vol. IT-23(3), pp. 387-390, May 1977.

[44] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. Eurocrypt 2000*, International Conference on Advances in Cryptology: Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000.

[45] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Proc. Eurocrypt 84*, A workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques, Paris, France, April 9-11, 1984.

[46] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Info. Theory*, vol. IT-39(3), pp. 733-742, May 1993.

[47] U. Maurer and S. Wolf, "Secret key agreement over unauthenticated public channels - Part I: Definitions and bounds," *IEEE Trans. Info. Theory*, vol. IT-49(4), pp. 822-831, April 2003.

[48] U. Maurer and S. Wolf, "Secret key agreement over unauthenticated public channels - Part II: The simulatability condition," *IEEE Trans. Info. Theory*, vol. IT-49(4), pp. 832-838, April 2003.

[49] U. Maurer and S. Wolf, "Secret key agreement over unauthenticated public channels - Part III: Privacy amplification," *IEEE Trans. Info. Theory*, vol. IT-49(4), pp. 839-851, April 2003.

[50] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Info. Theory*, vol. IT-46(2), pp. 344-366, March 2000.

[51] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Info. Theory*, vol. IT-50(12), pp. 3047-3061, December 2004.

[52] H. Yamamoto, "Coding theorems for secret sharing communication systems with two noisy channels," *IEEE Trans. Info. Theory*, vol. IT-35(3), pp. 572-578, May 1989.

[53] H. Yamamoto, "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels," *IEEE Trans. Info. Theory*, vol. IT-37(3), pp. 634-638, May 1991.

[54] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Info. Theory*, vol. IT-43(3), pp. 827-835, May 1997.

[55] Neri Merhav, "Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels," *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, June 24-29, 2007.

[56] E. Tekin and A. Yener, "The Gaussian multiple-access wire-tap channel with collective secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, July 9-14, 2006.

[57] E. Tekin and A. Yener, "Achievable rates for two-way wire-tap channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, June 24-29, 2007.

[58] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symp. Inf. Theory*, Lausanne, Switzerland, June 30-July 5, 2002.

[59] Y. Dodis, L. Reyzin and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Eurocrypt 2004*, International Conference on Advances in Cryptology: Theory and Application of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004.

[60] F. Hao, R. Anderson and J. Daugman, "Combining cryptography with biometrics effectively," *Technical Report UCAM-CL-TR-640*, University of Cambridge, 2005.

[61] J.-P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *Proc. 4th Int'l Conf. Audio- and Vidio-based Biometric Preson Authentication*, Guildford, UK, June 9-11, 2003.

[62] T. C. Clancy, N. Kiyavash and D. J. Lin, "Secure smartcard-based fingerprint authentication," *Proc. 2003 ACM SIGMM workshop on Biometrics methods and applications*, Berkley, California, November 08, 2003.

Appendices

Appendix I

Calculation of $I(U;Y), I(U;Z)$ and $I(U;V)$:

Referring to Figure 4.10, we have the followings:

$$\begin{aligned}
|\overrightarrow{X}| &= \sqrt{P}, \\
|\overrightarrow{V}| &= \sqrt{Q}, \\
|\overrightarrow{\eta_1}| &= \sqrt{N_1}, \\
|\overrightarrow{\eta_{12}}| &= \sqrt{N_1+N_2}, \\
|\overrightarrow{\eta_1'}| &= \sqrt{(1-\alpha)^2Q+N_1}, \\
|\overrightarrow{\eta_{12}'}| &= \sqrt{(1-\alpha)^2Q+N_1+N_2}, \\
|\overrightarrow{U'}| &= \sqrt{P+Q+2\sqrt{PQ}\cos\theta_{XV}}, \\
|\overrightarrow{U}| &= \sqrt{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}}, \\
|\overrightarrow{Y}| &= \sqrt{P+Q+N_1+2\sqrt{PQ}\cos\theta_{XV}}, \\
|\overrightarrow{Z}| &= \sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\cos\theta_{XV}}.
\end{aligned}$$

By the law of cosines, it is easy to get that

$$\begin{aligned}
\cos\theta_{UY} &= \frac{|\overrightarrow{U}|^2+|\overrightarrow{Y}|^2-|\overrightarrow{\eta_1'}|^2}{2|\overrightarrow{U}|\cdot|\overrightarrow{Y}|} \\
&= \frac{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}+P+Q+N_1+2\sqrt{PQ}\cos\theta_{XV}-(1-\alpha)^2Q-N_1}{2\sqrt{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}}\cdot\sqrt{P+Q+N_1+2\sqrt{PQ}\cos\theta_{XV}}} \\
&= \frac{P+\alpha Q+(1+\alpha)\sqrt{PQ}\cos\theta_{XV}}{\sqrt{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}}\cdot\sqrt{P+Q+N_1+2\sqrt{PQ}\cos\theta_{XV}}}; \\
\cos\theta_{UZ} &= \frac{|\overrightarrow{U}|^2+|\overrightarrow{Z}|^2-|\overrightarrow{\eta_{12}'}|^2}{2|\overrightarrow{U}|\cdot|\overrightarrow{Z}|} \\
&= \frac{P+\alpha Q+(1+\alpha)\sqrt{PQ}\cos\theta_{XV}}{\sqrt{P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV}}\cdot\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\cos\theta_{XV}}}; \\
\cos\theta_{UV} &= \frac{|\overrightarrow{U}|^2+|\alpha\overrightarrow{V}|^2-|\overrightarrow{X}|^2}{2|\overrightarrow{U}|\cdot|\alpha\overrightarrow{V}|}
\end{aligned}$$

$$= \frac{P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV} + \alpha^2 Q - P}{2\sqrt{P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV}} \cdot \alpha\sqrt{Q}}$$
$$= \frac{\alpha\sqrt{Q} + \sqrt{P}\cos\theta_{XV}}{\sqrt{P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV}}}.$$

By Pythagorean identity, for any θ, $\sin^2\theta + \cos^2\theta = 1$. So we have

$$\begin{aligned}
\sin^2\theta_{UY} &= 1 - \cos^2\theta_{UY} \\
&= 1 - \left(\frac{P + \alpha Q + (1+\alpha)\sqrt{PQ}\cos\theta_{XV}}{\sqrt{P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV}} \cdot \sqrt{P + Q + N_1 + 2\sqrt{PQ}\cos\theta_{XV}}}\right)^2 \\
&= \frac{(1-\alpha)^2 PQ(1-\cos^2\theta_{XV}) + N_1(P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV})}{(P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV})(P + Q + N_1 + 2\sqrt{PQ}\cos\theta_{XV})}; \\
\sin^2\theta_{UZ} &= 1 - \cos^2\theta_{UZ} \\
&= 1 - \left(\frac{P + \alpha Q + (1+\alpha)\sqrt{PQ}\cos\theta_{XV}}{\sqrt{P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV}} \cdot \sqrt{P + Q + N_1 + N_2 + 2\sqrt{PQ}\cos\theta_{XV}}}\right)^2 \\
&= \frac{(1-\alpha)^2 PQ(1-\cos^2\theta_{XV}) + (N_1+N_2)(P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV})}{(P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV})(P + Q + N_1 + N_2 + 2\sqrt{PQ}\cos\theta_{XV})}; \\
\sin^2\theta_{UV} &= 1 - \cos^2\theta_{UV} \\
&= 1 - \left(\frac{\alpha\sqrt{Q} + \sqrt{P}\cos\theta_{XV}}{\sqrt{P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV}}}\right)^2 \\
&= \frac{P(1-\cos^2\theta_{XV})}{P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV}}.
\end{aligned}$$

Recalling that $I(X;V) = \frac{1}{2}\log\frac{1}{1-\rho_{XV}^2} = \frac{1}{2}\log\frac{1}{1-\cos^2\theta_{XV}} = \frac{1}{2}\log\frac{1}{\sin^2\theta_{XV}}$, we have

$$\begin{aligned}
I(U;Y) &= \frac{1}{2}\log\frac{1}{\sin^2\theta_{UY}} \\
&= \frac{1}{2}\log\frac{(P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV})(P + Q + N_1 + 2\sqrt{PQ}\cos\theta_{XV})}{(1-\alpha)^2 PQ(1-\cos^2\theta_{XV}) + N_1(P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV})}; \\
I(U;Z) &= \frac{1}{2}\log\frac{1}{\sin^2\theta_{UZ}} \\
&= \frac{1}{2}\log\frac{(P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV})(P + Q + N_1 + N_2 + 2\sqrt{PQ}\cos\theta_{XV})}{(1-\alpha)^2 PQ(1-\cos^2\theta_{XV}) + (N_1+N_2)(P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV})}; \\
I(U;V) &= \frac{1}{2}\log\frac{1}{\sin^2\theta_{UV}} \\
&= \frac{1}{2}\log\frac{P + \alpha^2 Q + 2\alpha\sqrt{PQ}\cos\theta_{XV}}{P(1-\cos^2\theta_{XV})}.
\end{aligned}$$

The difference of mutual information can be calculated to yield

$$\begin{aligned}
I(U;Y) - I(U;V) &= \frac{1}{2}\log\frac{1}{\sin^2\theta_{UY}} - \frac{1}{2}\log\frac{1}{\sin^2\theta_{UV}} \\
&= \frac{1}{2}\log\frac{\sin^2\theta_{UV}}{\sin^2\theta_{UY}}
\end{aligned}$$

$$= \frac{1}{2}\log\frac{P(1-\cos^2\theta_{XV})(P+Q+N_1+2\sqrt{PQ}\cos\theta_{XV})}{(1-\alpha)^2PQ(1-\cos^2\theta_{XV})+N_1(P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV})};$$

$$I(U;Z)-I(U;V) = \frac{1}{2}\log\frac{1}{\sin^2\theta_{UZ}}-\frac{1}{2}\log\frac{1}{\sin^2\theta_{UV}}$$
$$= \frac{1}{2}\log\frac{\sin^2\theta_{UV}}{\sin^2\theta_{UZ}}$$
$$= \frac{1}{2}\log\frac{P(1-\cos^2\theta_{XV})(P+Q+N_1+N_2+2\sqrt{PQ}\cos\theta_{XV})}{(1-\alpha)^2PQ(1-\cos^2\theta_{XV})+(N_1+N_2)(P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV})};$$

$$I(U;Y)-I(U;Z) = \frac{1}{2}\log\frac{1}{\sin^2\theta_{UY}}-\frac{1}{2}\log\frac{1}{\sin^2\theta_{UZ}}$$
$$= \frac{1}{2}\log\frac{\sin^2\theta_{UZ}}{\sin^2\theta_{UY}}$$
$$= \frac{1}{2}\log(\frac{(P+Q+N_1+2\sqrt{PQ}\cos\theta_{XV})}{(P+Q+N_1+N_2+2\sqrt{PQ}\cos\theta_{XV})}\cdot$$
$$\frac{\{(1-\alpha)^2PQ(1-\cos^2\theta_{XV})+(N_1+N_2)(P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV})\}}{\{(1-\alpha)^2PQ(1-\cos^2\theta_{XV})+N_1(P+\alpha^2Q+2\alpha\sqrt{PQ}\cos\theta_{XV})\}}).$$

Note that $\rho_{XV}=\cos\theta_{XV}$. Replacing $\cos\theta_{XV}$ with ρ_{XV}, we easily get the expressions of $I(U;Y), I(U;Z), I(U;V)$ and the differences of the mutual information with respect to ρ_{XV}.

Appendix II

Lemma 3 in [12]: Let $\mathcal{P}_n$ be the set of all probability n-vectors $\mathbf{p}=(p_1,\cdots,p_n)$ and let $f_j(\mathbf{p})$, $j=1,\cdots,k$, be continuous functions on $\mathcal{P}_n$. Then, to any probability measure u on (the Borel subsets of) $\mathcal{P}_n$ there exists $(k+1)$ elements $\mathbf{p}_i$ of $\mathcal{P}_n$ and constants $\alpha_i\geq 0$, $i=1,\cdots,k+1$ with $\sum_{i=1}^{k+1}\alpha_i=1$ such that

$$\int f_j(\mathbf{p})du=\sum_{i=1}^{k+1}\alpha_i f_j(\mathbf{p}_i),\quad j=1,\cdots,k.$$

Proof of $|\mathcal{U}|\leq|\mathcal{X}||\mathcal{V}|+3$.

Proof: By applying Lemma 3 in [12] to the present situation, we show that the cardinality of the range of U can be bounded by $|\mathcal{X}||\mathcal{V}|+3$. Let us denote the product set $\mathcal{X}\times\mathcal{V}=\{1,2,\cdots,n\}$, $n=|\mathcal{X}||\mathcal{V}|$. Choose $\mathcal{P}_n$ as the set of all probability distributions on $\mathcal{X}\times\mathcal{V}$. We can interpret $\{\Pr((X,V)=(x,v)|U=u)\}_{(x,v)\in\mathcal{X}\times\mathcal{V}}$ as an element of $\mathcal{P}_n$ and $\{\Pr(U=u)\}_{u\in\mathcal{U}}$ as a Borel measure on $\mathcal{P}_n$. Consider the following continuous functions on $\mathcal{P}_n$:

a) For $\mathbf{p}=(p(1),\cdots,p(n))\in\mathcal{P}_n$, set

$$f_j(\mathbf{p})=p(j),\quad j=1,2,\cdots,n;$$

b)

$$f_{n+1}(\mathbf{p}) \;=\; H(Y)+\sum_y\sum_{x,v}p(x,v)p(y|x,v)\cdot$$

$$\log(\sum_{x,v} p(x,v)p(y|x,v));$$

c)

$$\begin{aligned} f_{n+2}(\mathbf{p}) &= H(Z) + \sum_z \sum_y \sum_{x,v} p(x,v)p(y|x,v)p(z|y) \cdot \\ &\quad \log(\sum_y \sum_{x,v} p(x,v)p(y|x,v)p(z|y)); \end{aligned}$$

d) $f_{n+3}(\mathbf{p}) = H(V) + \sum_v \sum_x p(x,v) \log(\sum_x p(x,v))$.

Observe that

$$\begin{aligned} &\sum_{u\in\mathcal{U}} \Pr(U=u) f_j(\Pr(\cdot|U=u)) = p(j), \\ &\qquad\qquad \text{for} \quad j = 1, 2, \cdots, n-1; \\ &\sum_{u\in\mathcal{U}} \Pr(U=u) f_{n+1}(\Pr(\cdot|U=u)) = I(U;Y); \\ &\sum_{u\in\mathcal{U}} \Pr(U=u) f_{n+2}(\Pr(\cdot|U=u)) = I(U;Z); \\ &\sum_{u\in\mathcal{U}} \Pr(U=u) f_{n+3}(\Pr(\cdot|U=u)) = I(U;V). \end{aligned}$$

Lemma 3 in [12] implies that the alphabet of the random variable U can be restricted as $|\mathcal{U}| \leq n+3$, i.e. $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{V}| + 3$. ■

Appendix III

Proof of $I(U;Y) \geq I(U;Z)$.

Proof: Let $f(N) = \frac{(P+\alpha^2 Q)(P+Q+N)}{PQ(1-\alpha)^2+(P+\alpha^2 Q)N}$.

First, we prove that $f(N)$ is a non-increasing function with respect to N as follows:

$$\begin{aligned} f'(N) &= \frac{(P+\alpha^2Q)(PQ(1-\alpha)^2 + (P+\alpha^2Q)N) - (P+\alpha^2Q)^2(P+Q+N)}{(PQ(1-\alpha)^2 + (P+\alpha^2Q)N)^2} \\ &= \frac{(P+\alpha^2Q)(PQ(1-\alpha)^2 + (P+\alpha^2Q)N - (P+\alpha^2Q)(P+Q+N))}{(PQ(1-\alpha)^2 + (P+\alpha^2Q)N)^2} \\ &= \frac{(P+\alpha^2Q)(PQ(1-\alpha)^2 - (P+\alpha^2Q)(P+Q))}{(PQ(1-\alpha)^2 + (P+\alpha^2Q)N)^2} \\ &= \frac{-(P+\alpha^2Q)(P+\alpha Q)^2}{(PQ(1-\alpha)^2 + (P+\alpha^2Q)N)^2} \\ &\leq 0. \end{aligned}$$

Note that $I(U;Y) = \frac{1}{2}\log f(N_1)$ and $I(U;Z) = \frac{1}{2}\log f(N_1+N_2)$. Since $f(N)$ is a non-increasing function with respect to N, we have $f(N_1) \geq f(N_1+N_2)$, which means that $I(U;Y) \geq I(U;Z)$. This completes the proof of $I(U;Y) \geq I(U;Z)$. ■

Appendix IV

Lemma 4.2.5: R_Z, which is defined in (4.8), is a increasing function with respect to α as $-\frac{P}{Q} < \alpha < 1$; a decreasing function as $\alpha < -\frac{P}{Q}$ or $\alpha > 1$; minimized at $\alpha = -\frac{P}{Q}$ and maximized at $\alpha = 1$.

Proof: Let

$$g(\alpha) = \frac{PQ(1-\alpha)^2 + (P+\alpha^2 Q)(N_1+N_2)}{PQ(1-\alpha)^2 + (P+\alpha^2 Q)N_1}.$$

First, we consider $g'(\alpha)$,

$$\begin{aligned}
g'(\alpha) &= \left(\frac{PQ(1-\alpha)^2 + (P+\alpha^2 Q)(N_1+N_2)}{PQ(1-\alpha)^2 + (P+\alpha^2 Q)N_1}\right)' \\
&= \frac{(-2PQ(1-\alpha) + 2\alpha Q(N_1+N_2))(PQ(1-\alpha)^2 + (P+\alpha^2 Q)N_1)}{(PQ(1-\alpha)^2 + (P+\alpha^2 Q)N_1)^2} \\
&- \frac{(-2PQ(1-\alpha) + 2\alpha Q N_1)(PQ(1-\alpha)^2 + (P+\alpha^2 Q)(N_1+N_2))}{(PQ(1-\alpha)^2 + (P+\alpha^2 Q)N_1)^2} \\
&= \frac{2PQN_2(1-\alpha)(P+\alpha^2 Q) - 2QN_1N_2\alpha(P+\alpha^2 Q) + 2QN_2\alpha(PQ(1-\alpha)^2 + N_1(P+\alpha^2 Q))}{(PQ(1-\alpha)^2 + (P+\alpha^2 Q)N_1)^2} \\
&= \frac{2PQN_2(1-\alpha)(P+\alpha^2 Q) + 2PQN_2\alpha(1-\alpha)^2 Q}{(PQ(1-\alpha)^2 + (P+\alpha^2 Q)N_1)^2} \\
&= \frac{2PQN_2(1-\alpha)(P+\alpha^2 Q + \alpha(1-\alpha)Q)}{(PQ(1-\alpha)^2 + (P+\alpha^2 Q)N_1)^2} \\
&= \frac{2PQN_2(1-\alpha)(P+\alpha Q)}{(PQ(1-\alpha)^2 + (P+\alpha^2 Q)N_1)^2}.
\end{aligned}$$

Clearly, if $\alpha > 1$ or $\alpha < -\frac{P}{Q}$, $g'(\alpha) < 0$; and if $-\frac{P}{Q} < \alpha < 1$, we have $g'(\alpha) > 0$. Thus, we have proved that: $g(\alpha)$ is an increasing function with respect to α when $\alpha \in (-\frac{P}{Q}, 1)$; $g(\alpha)$ is a decreasing function with respect to α when $\alpha \in (-\infty, -\frac{P}{Q}) \cup (1, \infty)$; $g(\alpha)$ is locally maximized at $\alpha = 1$ and locally minimized at $\alpha = -\frac{P}{Q}$. Note that

$$\begin{aligned}
g(1) &= \frac{N_1+N_2}{N_1}; \\
g(-\frac{P}{Q}) &= \frac{P+Q+N_1+N_2}{P+Q+N_1}.
\end{aligned}$$

Now let us consider $\lim_{\alpha\to\infty} g(\alpha)$.

$$\lim_{\alpha\to\infty} g(\alpha) = \frac{P+N_1+N_2}{P+N_1}.$$

It is clear that $g(1) \geq \lim_{\alpha\to\infty} g(\alpha)$ and $g(-\frac{P}{Q}) \leq \lim_{\alpha\to\infty} g(\alpha)$, so we have shown that $g(\alpha)$ is globally maximized at $\alpha = 1$ and globally minimized at $\alpha = -\frac{P}{Q}$. In addition,

$$R_Z = \frac{1}{2}\log\frac{P+Q+N_1}{P+Q+N_1+N_2} + \frac{1}{2}\log g(\alpha).$$

Then the function R_Z has the same property as $g(\alpha)$. Thus we completed the proof of this lemma. ■

Appendix V

Proof of $I(U;Y) \geq I(U;Z)$.

Proof: Let

$$f(N) = \frac{(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})(P+Q+N+2\sqrt{PQ}\rho_{XV})}{(1-\alpha)^2 PQ(1-\rho_{XV}^2)+N(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})}.$$

First, we prove that $f(N)$ is a non-increasing function with respect to N as follows:

$$\begin{aligned}
f'(N) &= [(1-\alpha)^2 PQ(1-\rho_{XV}^2)+N(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})- \\
&\quad (P+Q+N+2\sqrt{PQ}\rho_{XV})(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})] \\
&\quad \cdot\frac{(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})}{[(1-\alpha)^2 PQ(1-\rho_{XV}^2)+N(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})]^2} \\
&= [(1-\alpha)^2 PQ(1-\rho_{XV}^2)-(P+Q+2\sqrt{PQ}\rho_{XV})(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})] \\
&\quad \cdot\frac{(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})}{[(1-\alpha)^2 PQ(1-\rho_{XV}^2)+N(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})]^2} \\
&= -\frac{(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})[(P+\alpha Q)+(1+\alpha)\sqrt{PQ}\rho_{XV}]^2}{[(1-\alpha)^2 PQ(1-\rho_{XV}^2)+N(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})]^2} \\
&\leq 0.
\end{aligned}$$

Note that $I(U;Y) = \frac{1}{2}\log f(N_1)$ and $I(U;Z) = \frac{1}{2}\log f(N_1+N_2)$. Since $f(N)$ is a non-increasing function with respect to N, we have $f(N_1) \geq f(N_1+N_2)$, which means that $I(U;Y) \geq I(U;Z)$. This completes the proof of $I(U;Y) \geq I(U;Z)$. ■

Appendix VI

Proof of (4.50) and (4.51).

From (4.47), we have

$$\begin{aligned}
I(U;V) &> I(U;Y) \\
0 &> I(U;Y)-I(U;V) \\
0 &> \frac{1}{2}\log\frac{P(1-\rho_{XV}^2)(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{(1-\alpha)^2 PQ(1-\rho_{XV}^2)+N_1(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV})}
\end{aligned}$$

$$(1-\alpha)^2 PQ(1-\rho_{XV}^2)+N_1(P+\alpha^2 Q+2\alpha\sqrt{PQ}\rho_{XV}) > P(1-\rho_{XV}^2)(P+Q+N_1+2\sqrt{PQ}\rho_{XV})$$

$$[P(1-\rho_{XV}^2)+N_1]Q\alpha^2-2[PQ(1-\rho_{XV}^2)-N_1\sqrt{PQ}\rho_{XV}]\alpha > P(1-\rho_{XV}^2)(P+2\sqrt{PQ}\rho_{XV})-PN_1\rho_{XV}^2.$$

Let us consider the equality

$$[P(1-\rho_{XV}^2)+N_1]Q\alpha^2-2[PQ(1-\rho_{XV}^2)-N_1\sqrt{PQ}\rho_{XV}]\alpha+PN_1\rho_{XV}^2-P(1-\rho_{XV}^2)(P+2\sqrt{PQ}\rho_{XV}) = 0.$$

The discriminant of the above quadratic equation is:

$$\begin{aligned}\Delta &= 4[PQ(1-\rho_{XV}^2) - N_1\sqrt{PQ}\rho_{XV}]^2 \\ &\quad -4Q[P(1-\rho_{XV}^2)+N_1][PN_1\rho_{XV}^2 - P(1-\rho_{XV}^2)(P+2\sqrt{PQ}\rho_{XV})] \\ &= 4P^2Q(1-\rho_{XV}^2)^2(P+Q+2\sqrt{PQ}\rho_{XV}+N_1).\end{aligned}$$

Let

$$\begin{aligned}\alpha_{00} &= \frac{2[PQ(1-\rho_{XV}^2) - N_1\sqrt{PQ}\rho_{XV}] + \sqrt{\Delta}}{2Q[P(1-\rho_{XV}^2)+N_1]} \\ &= \frac{2[PQ(1-\rho_{XV}^2) - N_1\sqrt{PQ}\rho_{XV}] + 2P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1)}}{2Q[P(1-\rho_{XV}^2)+N_1]} \\ &= \frac{PQ(1-\rho_{XV}^2) - N_1\sqrt{PQ}\rho_{XV} + P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1)}}{Q[P(1-\rho_{XV}^2)+N_1]}; \\ \alpha_{-00} &= \frac{2[PQ(1-\rho_{XV}^2) - N_1\sqrt{PQ}\rho_{XV}] - \sqrt{\Delta}}{2Q[P(1-\rho_{XV}^2)+N_1]} \\ &= \frac{2[PQ(1-\rho_{XV}^2) - N_1\sqrt{PQ}\rho_{XV}] - 2P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1)}}{2Q[P(1-\rho_{XV}^2)+N_1]} \\ &= \frac{PQ(1-\rho_{XV}^2) - N_1\sqrt{PQ}\rho_{XV} - P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1)}}{Q[P(1-\rho_{XV}^2)+N_1]}.\end{aligned}$$

Therefore, under the assumption that $P, Q, N_1, N_2 > 0$, we have

$$\begin{aligned}I(U;V) > I(U;Y) &\iff \alpha > \alpha_{00} \quad \text{or} \quad \alpha < \alpha_{-00}; \\ I(U;Y) \geq I(U;V) &\iff \alpha_{-00} \leq \alpha \leq \alpha_{00}.\end{aligned}$$

Appendix VII

Lemma 4.4.5: R_Z, which is defined in (4.49), is maximized at $\alpha = 1$ and minimized at $\alpha = \alpha_{min}$. Furthermore,

(a) when $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$, R_Z is
a non-increasing function with respect to α as $\alpha \leq \alpha_{min}$;
a non-decreasing function as $\alpha_{min} \leq \alpha \leq 1$;
a non-increasing function as $\alpha \geq 1$.

(b) when $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$, R_Z is
a non-decreasing function with respect to α as $\alpha \leq 1$;
a non-increasing function as $1 \leq \alpha \leq \alpha_{min}$;
a non-decreasing function as $\alpha \geq \alpha_{min}$.

(c) when $\sqrt{P}\rho_{XV} + \sqrt{Q} = 0$, R_Z is
a non-decreasing function with respect to α as $\alpha \leq 1$ and a non-increasing function as $\alpha > 1$.

Proof: Let

$$f(\alpha) = \frac{(1-\alpha)^2 PQ(1-\rho_{XV}^2) + (N_1+N_2)(P+\alpha^2 Q + 2\alpha\sqrt{PQ}\rho_{XV})}{(1-\alpha)^2 PQ(1-\rho_{XV}^2) + N_1(P+\alpha^2 Q + 2\alpha\sqrt{PQ}\rho_{XV})}.$$

Consider

$$f'(\alpha) = \frac{g(\alpha)}{\{(1-\alpha)^2 PQ(1-\rho_{XV}^2) + N_1(P+\alpha^2 Q + 2\alpha\sqrt{PQ}\rho_{XV})\}^2},$$

where

$$\begin{aligned}
g(\alpha) &= [-2(1-\alpha)PQ(1-\rho_{XV}^2) + 2(N_1+N_2)(\alpha Q + \rho_{XV}\sqrt{PQ})] \\
&\quad \cdot[(1-\alpha)^2 PQ(1-\rho_{XV}^2) + N_1(P+\alpha^2 Q + 2\alpha\sqrt{PQ}\rho_{XV})] \\
&\quad -[-2(1-\alpha)PQ(1-\rho_{XV}^2) + 2N_1(\alpha Q + \rho_{XV}\sqrt{PQ})] \\
&\quad \cdot[(1-\alpha)^2 PQ(1-\rho_{XV}^2) + (N_1+N_2)(P+\alpha^2 Q + 2\alpha\sqrt{PQ}\rho_{XV})] \\
&= -2(1-\alpha)PQ(1-\rho_{XV}^2)(1-\alpha)^2 PQ(1-\rho_{XV}^2) \\
&\quad -2(1-\alpha)PQ(1-\rho_{XV}^2)N_1(P+\alpha^2 Q + 2\alpha\sqrt{PQ}\rho_{XV}) \\
&\quad +2(N_1+N_2)(\alpha Q + \rho_{XV}\sqrt{PQ})(1-\alpha)^2 PQ(1-\rho_{XV}^2) \\
&\quad +2(N_1+N_2)N_1(\alpha Q + \rho_{XV}\sqrt{PQ})(P+\alpha^2 Q + 2\alpha\sqrt{PQ}\rho_{XV}) \\
&\quad +2(1-\alpha)PQ(1-\rho_{XV}^2)(1-\alpha)^2 PQ(1-\rho_{XV}^2) \\
&\quad +2(1-\alpha)PQ(1-\rho_{XV}^2)(N_1+N_2)(P+\alpha^2 Q + 2\alpha\sqrt{PQ}\rho_{XV}) \\
&\quad -2N_1(\alpha Q + \rho_{XV}\sqrt{PQ})(1-\alpha)^2 PQ(1-\rho_{XV}^2) \\
&\quad -2N_1(N_1+N_2)(\alpha Q + \rho_{XV}\sqrt{PQ})(P+\alpha^2 Q + 2\alpha\sqrt{PQ}\rho_{XV}) \\
&= 2(1-\alpha)(1-\rho_{XV}^2)PQN_2(P+\alpha^2 Q + 2\alpha\sqrt{PQ}\rho_{XV}) \\
&\quad +2(1-\alpha)^2 PQN_2(1-\rho_{XV}^2)(\alpha Q + \sqrt{PQ}\rho_{XV}) \\
&= 2(1-\alpha)(1-\rho_{XV}^2)PQN_2(P+\alpha^2 Q + 2\alpha\sqrt{PQ}\rho_{XV} + (1-\alpha)(\alpha Q + \sqrt{PQ}\rho_{XV})) \\
&= 2(1-\alpha)(1-\rho_{XV}^2)PQN_2(P+\sqrt{PQ}\rho_{XV} + (Q+\sqrt{PQ}\rho_{XV})\alpha) \\
&= 2(1-\alpha)(\alpha + \frac{P+\sqrt{PQ}\rho_{XV}}{Q+\sqrt{PQ}\rho_{XV}})(1-\rho_{XV}^2)(Q+\sqrt{PQ}\rho_{XV})PQN_2 \\
&= -2(\alpha-1)(\alpha-\alpha_{min})(1-\rho_{XV}^2)(\sqrt{Q}+\sqrt{P}\rho_{XV})PQ\sqrt{Q}N_2.
\end{aligned}$$

Here

$$\alpha_{min} = -\frac{\sqrt{P}(\sqrt{P}+\sqrt{Q}\rho_{XV})}{\sqrt{Q}(\sqrt{P}\rho_{XV}+\sqrt{Q})}.$$

Note that when $|\rho_{XV}| = 1$, $g(\alpha) = 0$. In this case, for fixed ρ_{XV}, R_Z is a constant.

$$R_Z = \frac{1}{2}\log\frac{(N_1+N_2)(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{N_1(P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})}.$$

Assume that $|\rho_{XV}| < 1$, when $\sqrt{Q}+\sqrt{P}\rho_{XV} > 0$, the coefficient of $g(\alpha)$ is less than 0, i.e., $-2(1-\rho_{XV}^2)(\sqrt{Q}+\sqrt{P}\rho_{XV})PQ\sqrt{Q}N_2 < 0$. Moreover, in this case, $\alpha_{min} \leq 1$. The reason

is that under the condition $\sqrt{Q}+\sqrt{P}\rho_{XV}>0$,

$$\begin{aligned}\alpha_{min}\le 1 &\Leftrightarrow -\frac{\sqrt{P}(\sqrt{P}+\sqrt{Q}\rho_{XV})}{\sqrt{Q}(\sqrt{Q}+\sqrt{P}\rho_{XV})}\le 1\\ &\Leftrightarrow -\sqrt{P}(\sqrt{P}+\sqrt{Q}\rho_{XV})\le\sqrt{Q}(\sqrt{Q}+\sqrt{P}\rho_{XV})\\ &\Leftrightarrow P+Q+2\sqrt{PQ}\rho_{XV}\ge 0.\end{aligned}$$

Therefore, when $\sqrt{Q}+\sqrt{P}\rho_{XV}>0$, $g(\alpha)\le 0$ as $\alpha\le\alpha_{min}$; $g(\alpha)\ge 0$ as $\alpha_{min}\le\alpha\le 1$; $g(\alpha)\le 0$ as $\alpha\ge 1$. So does $f'(\alpha)$. It is clear that $f(\alpha)$ is locally maximized at $\alpha=1$ and locally minimized at α_{min}. Note that

$$\begin{aligned}f(1) &= \frac{N_1+N_2}{N_1};\\ f(\alpha_{min}) &= \frac{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2}{P+Q+2\sqrt{PQ}\rho_{XV}+N_1}\\ &= \frac{(\sqrt{P}\rho_{XV}+\sqrt{Q})^2+P(1-\rho_{XV}^2)+N_1+N_2}{(\sqrt{P}\rho_{XV}+\sqrt{Q})^2+P(1-\rho_{XV}^2)+N_1};\\ \lim_{\alpha\to\infty} f(\alpha) &= \frac{P(1-\rho_{XV}^2)+N_1+N_2}{P(1-\rho_{XV}^2)+N_1}.\end{aligned}$$

It is easy to verify that $f(1)\ge\lim_{\alpha\to\infty} f(\alpha)$ and $f(\alpha_{min})\le\lim_{\alpha\to\infty} f(\alpha)$. So far, we have shown that $f(\alpha)$ is globally maximized at $\alpha=1$ and globally minimized at $\alpha=\alpha_{min}$. In addition,

$$R_Z=\frac{1}{2}\log\frac{P+Q+N_1+2\sqrt{PQ}\rho_{XV}}{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}}+\frac{1}{2}\log f(\alpha).$$

R_Z has the same property as $f(\alpha)$. Thus, we have proved the part (a) of this lemma. Similarly, part (b) can be easily derived.

Now let us prove the part (c). When $\sqrt{Q}+\sqrt{P}\rho_{XV}=0$, we have $\rho_{XV}=-\frac{\sqrt{Q}}{\sqrt{P}}$. In this case, since the absolute value of ρ_{XV} can not exceed 1, $P\ge Q$. We simplify $f(\alpha)$ as follows:

$$f_1(\alpha)=\frac{(1-\alpha)^2Q(P-Q)+(N_1+N_2)(P+\alpha^2Q-2\alpha Q)}{(1-\alpha)^2Q(P-Q)+N_1(P+\alpha^2Q-2\alpha Q)}.$$

Consider

$$f_1'(\alpha)=\frac{g_1(\alpha)}{\{(1-\alpha)^2Q(P-Q)+N_1(P+\alpha^2Q-2\alpha Q)\}^2},$$

where

$$g_1(\alpha)=2(1-\alpha)(P-Q)^2QN_2.$$

Clearly, when $P=Q$ and $\rho_{XV}=-1$, $g_1(\alpha)=0$. In this case, it is easy to verify that $R_Z=0$. If $P\ne Q$, when $\sqrt{Q}+\sqrt{P}\rho_{XV}=0$, $g_1(\alpha)\ge 0$ as $\alpha\le 1$ and $g_1(\alpha)\le 0$ as $\alpha\ge 1$. So does $f_1'(\alpha)$. Therefore, $f_1(\alpha)$ is maximized at $\alpha=1$. In this case, if we define $f_1(\alpha_{min})=\lim_{\alpha\to\infty} f_1(\alpha)$, we have

$$f_1(1) = \frac{N_1+N_2}{N_1};$$

$$f_1(\alpha_{min}) \;=\; \frac{P-Q+N_1+N_2}{P-Q+N_1}.$$

Clearly, $f_1(1) \geq \lim_{\alpha\to\infty} f_1(\alpha)$ since $P \geq Q$ in this case. So far, we have shown that $f_1(\alpha)$ is maximized at $\alpha = 1$ and minimized at α_{min}. In addition,

$$R_Z = \frac{1}{2}\log\frac{P+Q+N_1+2\sqrt{PQ}\rho_{XV}}{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}} + \frac{1}{2}\log f_1(\alpha).$$

R_Z has the same property as $f_1(\alpha)$. Thus, we have proved the part (c) of this lemma. This also completes this proof. ■

Appendix VIII

Lemma 4.4.6: If $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$,

$$\alpha_{min} \leq \alpha_{-0} \leq \alpha_{max} < 1, \quad \alpha_0 \leq \alpha_{00}, \quad \alpha_{min} \leq \alpha_{-00}.$$

Proof: First we prove that $\alpha_{max} < 1$. Since $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$, then

$$\begin{aligned}
\alpha_{max} &= \frac{PQ(1-\rho_{XV}^2) - N_1\sqrt{PQ}\rho_{XV}}{Q[P(1-\rho_{XV}^2)+N_1]} \\
&< \frac{PQ(1-\rho_{XV}^2) + N_1 Q}{Q[P(1-\rho_{XV}^2)+N_1]} \\
&= 1.
\end{aligned}$$

Secondly, we will show in the following that $\alpha_{-0} \leq \alpha_{max}$, if $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$.

$$\begin{aligned}
\alpha_{max} &\geq \alpha_{-0} \\
1-\alpha_{max} &\leq 1-\alpha_{-0} \\
\frac{\sqrt{Q}N_1(\sqrt{Q}+\sqrt{P}\rho_{XV})}{Q[P(1-\rho_{XV}^2)+N_1]} &\leq \frac{\sqrt{Q}(N_1+N_2)(\sqrt{Q}+\sqrt{P}\rho_{XV})}{Q[P(1-\rho_{XV}^2)+N_1+N_2]} \\
&\quad + \frac{P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)}}{Q[P(1-\rho_{XV}^2)+N_1+N_2]} \\
\frac{N_1(\sqrt{Q}+\sqrt{P}\rho_{XV})}{P(1-\rho_{XV}^2)+N_1} &\leq \frac{(N_1+N_2)(\sqrt{Q}+\sqrt{P}\rho_{XV})}{P(1-\rho_{XV}^2)+N_1+N_2} \\
&\quad + \frac{P(1-\rho_{XV}^2)\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2}}{P(1-\rho_{XV}^2)+N_1+N_2}.
\end{aligned}$$

Since $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$ and $\frac{N_1}{P(1-\rho_{XV}^2)+N_1} \leq \frac{N_1+N_2}{P(1-\rho_{XV}^2)+N_1+N_2}$, it is clear that $\alpha_{-0} \leq \alpha_{max}$.

Now let us prove that $\alpha_{min} \leq \alpha_{-0}$.

$$\begin{aligned}
\alpha_{min} &\leq \alpha_{-0} \\
1-\alpha_{min} &\geq 1-\alpha_{-0} \\
\frac{P+Q+2\sqrt{PQ}\rho_{XV}}{\sqrt{Q}(\sqrt{Q}+\sqrt{P}\rho_{XV})} &\geq \frac{\sqrt{Q}(N_1+N_2)(\sqrt{Q}+\sqrt{P}\rho_{XV})}{Q[P(1-\rho_{XV}^2)+N_1+N_2]}
\end{aligned}$$

$$
\begin{aligned}
& & & + \frac{P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)}}{Q[P(1-\rho_{XV}^2)+N_1+N_2]} \\
\frac{P+Q+2\sqrt{PQ}\rho_{XV}}{\sqrt{Q}+\sqrt{P}\rho_{XV}} & \geq & \frac{(N_1+N_2)(\sqrt{Q}+\sqrt{P}\rho_{XV})}{P(1-\rho_{XV}^2)+N_1+N_2} \\
& & + \frac{P(1-\rho_{XV}^2)\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2}}{P(1-\rho_{XV}^2)+N_1+N_2}
\end{aligned}
$$

$$
\left\{ \begin{array}{l} (P+Q+2\sqrt{PQ}\rho_{XV})P(1-\rho_{XV}^2) \\ +(P+Q+2\sqrt{PQ}\rho_{XV})(N_1+N_2) \end{array} \right\} \geq \left\{ \begin{array}{l} (Q+P\rho_{XV}^2+2\sqrt{PQ}\rho_{XV})(N_1+N_2) \\ +P(1-\rho_{XV}^2)(\sqrt{Q}+\sqrt{P}\rho_{XV}) \\ \cdot\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2} \end{array} \right\}
$$

$$
\left\{ \begin{array}{r} P(1-\rho_{XV}^2) \\ \cdot(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2) \end{array} \right\} \geq \left\{ \begin{array}{l} P(1-\rho_{XV}^2)(\sqrt{Q}+\sqrt{P}\rho_{XV}) \\ \cdot\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2} \end{array} \right\}
$$

$$
\begin{aligned}
\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2} &\geq \sqrt{Q}+\sqrt{P}\rho_{XV} \\
P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2 &\geq Q+P\rho_{XV}^2+2\sqrt{PQ}\rho_{XV} \\
P(1-\rho_{XV}^2)+N_1+N_2 &\geq 0.
\end{aligned}
$$

Similarly, $\alpha_{min} \leq \alpha_{-00}$ can be easily derived.

At the last, we will show that $\alpha_0 \leq \alpha_{00}$, if $\sqrt{P}\rho_{XV}+\sqrt{Q}>0$. Let

$$
f(N) = \frac{PQ(1-\rho_{XV}^2) - N\sqrt{PQ}\rho_{XV} + P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N)}}{Q[P(1-\rho_{XV}^2)+N]}.
$$

We will prove that $f(N)$ is a non-increasing function with respect to N. Note that $f(N)$ can be written as $f(N) = f_1(N) + f_2(N)$, where

$$
\begin{aligned}
f_1(N) &= \frac{PQ(1-\rho_{XV}^2) - N\sqrt{PQ}\rho_{XV}}{Q[P(1-\rho_{XV}^2)+N]}; \\
f_2(N) &= \frac{P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N)}}{Q[P(1-\rho_{XV}^2)+N]} \\
&= \frac{P(1-\rho_{XV}^2)}{\sqrt{Q}}\sqrt{\frac{(P(1-\rho_{XV}^2)+N+P\rho_{XV}^2+Q+2\sqrt{PQ}\rho_{XV})}{[P(1-\rho_{XV}^2)+N]^2}} \\
&= \frac{P(1-\rho_{XV}^2)}{\sqrt{Q}}\sqrt{\frac{1}{P(1-\rho_{XV}^2)+N} + \frac{(\rho_{XV}\sqrt{P}+\sqrt{Q})^2}{[P(1-\rho_{XV}^2)+N]^2}}.
\end{aligned}
$$

It is clear that the second term $f_2(N)$ is non-increasing with respect to N. Now let us consider the first term $f_1(N)$,

$$
\begin{aligned}
f_1{}'(N) &= \frac{-\sqrt{PQ}\rho_{XV}Q[P(1-\rho_{XV}^2)+N] - Q[PQ(1-\rho_{XV}^2) - N\sqrt{PQ}\rho_{XV}]}{Q^2[P(1-\rho_{XV}^2)+N]^2} \\
&= \frac{-PQ\sqrt{Q}(1-\rho_{XV}^2)(\sqrt{P}\rho_{XV}+\sqrt{Q})}{Q^2[P(1-\rho_{XV}^2)+N]^2}.
\end{aligned}
$$

When $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$, $f_1{}'(N) \leq 0$. So $f_1(N)$ is non-increasing with respect to N. Therefore, as a summation of $f_1(N)$ and $f_2(N)$, $f(N)$ is a non-increasing function with respect to N.

Note that

$$\alpha_0 = f(N_1 + N_2), \quad \alpha_{00} = f(N_1).$$

Since $f(N)$ is a non-increasing function with respect to N, we have $\alpha_0 \leq \alpha_{00}$. This completes the proof.

■

Appendix IX

Lemma 4.4.10: If $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$,

$$1 < \alpha_{max} \leq \alpha_0 \leq \alpha_{min}, \quad \alpha_{-00} \leq \alpha_{-0}, \quad \alpha_{00} \leq \alpha_{min}.$$

Proof: First we prove that $\alpha_{max} > 1$. Since $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$, then

$$\begin{aligned} \alpha_{max} &= \frac{PQ(1-\rho_{XV}^2) - N_1\sqrt{PQ}\rho_{XV}}{Q[P(1-\rho_{XV}^2) + N_1]} \\ &> \frac{PQ(1-\rho_{XV}^2) + N_1 Q}{Q[P(1-\rho_{XV}^2) + N_1]} \\ &= 1. \end{aligned}$$

Secondly, we will show in the following that $\alpha_{max} \leq \alpha_0$, if $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$.

$$\begin{aligned} \alpha_{max} &\leq \alpha_0 \\ \alpha_{max} - 1 &\leq \alpha_0 - 1 \\ -\frac{\sqrt{Q}N_1(\sqrt{Q} + \sqrt{P}\rho_{XV})}{Q[P(1-\rho_{XV}^2) + N_1]} &\leq -\frac{\sqrt{Q}(N_1+N_2)(\sqrt{Q} + \sqrt{P}\rho_{XV})}{Q[P(1-\rho_{XV}^2) + N_1 + N_2]} \\ &\quad + \frac{P(1-\rho_{XV}^2)\sqrt{Q(P + Q + 2\sqrt{PQ}\rho_{XV} + N_1 + N_2)}}{Q[P(1-\rho_{XV}^2) + N_1 + N_2]} \\ -\frac{N_1(\sqrt{Q} + \sqrt{P}\rho_{XV})}{P(1-\rho_{XV}^2) + N_1} &\leq -\frac{(N_1+N_2)(\sqrt{Q} + \sqrt{P}\rho_{XV})}{P(1-\rho_{XV}^2) + N_1 + N_2} \\ &\quad + \frac{P(1-\rho_{XV}^2)\sqrt{P + Q + 2\sqrt{PQ}\rho_{XV} + N_1 + N_2}}{P(1-\rho_{XV}^2) + N_1 + N_2}. \end{aligned}$$

Since $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$ and $\frac{N_1}{P(1-\rho_{XV}^2)+N_1} \leq \frac{N_1+N_2}{P(1-\rho_{XV}^2)+N_1+N_2}$, it is clear that $\alpha_{max} \leq \alpha_0$.

Now let us prove that $\alpha_0 \leq \alpha_{min}$.

$$\begin{aligned} \alpha_{min} &\geq \alpha_0 \\ \alpha_{min} - 1 &\geq \alpha_0 - 1 \\ -\frac{P + Q + 2\sqrt{PQ}\rho_{XV}}{\sqrt{Q}(\sqrt{Q} + \sqrt{P}\rho_{XV})} &\geq -\frac{\sqrt{Q}(N_1+N_2)(\sqrt{Q} + \sqrt{P}\rho_{XV})}{Q[P(1-\rho_{XV}^2) + N_1 + N_2]} \\ &\quad + \frac{P(1-\rho_{XV}^2)\sqrt{Q(P + Q + 2\sqrt{PQ}\rho_{XV} + N_1 + N_2)}}{Q[P(1-\rho_{XV}^2) + N_1 + N_2]} \end{aligned}$$

$$
\begin{aligned}
-\frac{P+Q+2\sqrt{PQ}\rho_{XV}}{\sqrt{Q}+\sqrt{P}\rho_{XV}} &\geq -\frac{(N_1+N_2)(\sqrt{Q}+\sqrt{P}\rho_{XV})}{P(1-\rho_{XV}^2)+N_1+N_2} \\
&\quad +\frac{P(1-\rho_{XV}^2)\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2}}{P(1-\rho_{XV}^2)+N_1+N_2}
\end{aligned}
$$

$$
\left\{ \begin{array}{l} (P+Q+2\sqrt{PQ}\rho_{XV})P(1-\rho_{XV}^2) \\ +(P+Q+2\sqrt{PQ}\rho_{XV})(N_1+N_2) \end{array} \right\} \geq \left\{ \begin{array}{l} (Q+P\rho_{XV}^2+2\sqrt{PQ}\rho_{XV})(N_1+N_2) \\ -P(1-\rho_{XV}^2)(\sqrt{Q}+\sqrt{P}\rho_{XV}) \\ \cdot\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2} \end{array} \right\}
$$

$$
\left\{ \begin{array}{r} P(1-\rho_{XV}^2) \\ \cdot(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2) \end{array} \right\} \geq \left\{ \begin{array}{l} -P(1-\rho_{XV}^2)(\sqrt{Q}+\sqrt{P}\rho_{XV}) \\ \cdot\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2} \end{array} \right\}
$$

$$
\begin{aligned}
\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2} &\geq -(\sqrt{Q}+\sqrt{P}\rho_{XV}) \\
P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2 &\geq Q+P\rho_{XV}^2+2\sqrt{PQ}\rho_{XV} \\
P(1-\rho_{XV}^2)+N_1+N_2 &\geq 0.
\end{aligned}
$$

Similarly, $\alpha_{00} \leq \alpha_{min}$ can be easily derived.

At the last, we will show that $\alpha_{-00} \leq \alpha_{-0}$, if $\sqrt{P}\rho_{XV}+\sqrt{Q}<0$. Let

$$
f(N) = \frac{PQ(1-\rho_{XV}^2) - N\sqrt{PQ}\rho_{XV} - P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N)}}{Q[P(1-\rho_{XV}^2)+N]},
$$

We will prove that $f(N)$ is a non-decreasing function with respect to N. Note that $f(N)$ can be written as $f(N) = f_1(N) + f_2(N)$, where

$$
\begin{aligned}
f_1(N) &= \frac{PQ(1-\rho_{XV}^2) - N\sqrt{PQ}\rho_{XV}}{Q[P(1-\rho_{XV}^2)+N]}; \\
f_2(N) &= -\frac{P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N)}}{Q[P(1-\rho_{XV}^2)+N]} \\
&= -\frac{P(1-\rho_{XV}^2)}{\sqrt{Q}}\sqrt{\frac{(P(1-\rho_{XV}^2)+N+P\rho_{XV}^2+Q+2\sqrt{PQ}\rho_{XV})}{[P(1-\rho_{XV}^2)+N]^2}} \\
&= -\frac{P(1-\rho_{XV}^2)}{\sqrt{Q}}\sqrt{\frac{1}{P(1-\rho_{XV}^2)+N}+\frac{(\rho_{XV}\sqrt{P}+\sqrt{Q})^2}{[P(1-\rho_{XV}^2)+N]^2}}.
\end{aligned}
$$

It is clear that the second term $f_2(N)$ is non-decreasing with respect to N. Now let us consider the first term $f_1(N)$,

$$
\begin{aligned}
f_1{}'(N) &= \frac{-\sqrt{PQ}\rho_{XV}Q[P(1-\rho_{XV}^2)+N] - Q[PQ(1-\rho_{XV}^2) - N\sqrt{PQ}\rho_{XV}]}{Q^2[P(1-\rho_{XV}^2)+N]^2} \\
&= \frac{-PQ\sqrt{Q}(1-\rho_{XV}^2)(\sqrt{P}\rho_{XV}+\sqrt{Q})}{Q^2[P(1-\rho_{XV}^2)+N]^2}.
\end{aligned}
$$

When $\sqrt{P}\rho_{XV}+\sqrt{Q} \geq 0$, $f_1{}'(N) > 0$. So $f_1(N)$ is also non-decreasing with respect to N. Therefore, as a summation of $f_1(N)$ and $f_2(N)$, $f(N)$ is a non-decreasing function with respect to N.

Note that

$$\alpha_{-0} = f(N_1 + N_2), \quad \alpha_{-00} = f(N_1).$$

Since $f(N)$ is a non-decreasing function with respect to N, we have $\alpha_{-0} \geq \alpha_{-00}$. This completes the proof. ■

Appendix X

Lemma 4.4.7: If $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$,

$$N_2 \geq N_{high} \Longrightarrow \alpha_{-0} \leq \alpha_0 \leq \alpha_{max},$$

where

$$N_{high} = P(1-\rho_{XV}^2) + N_1 + \frac{[P(1-\rho_{XV}^2)+N_1]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}.$$

Proof: Since $\alpha_{-0} \leq \alpha_0$ is always valid, we only need to prove that $\alpha_0 \leq \alpha_{max}$.

$$\begin{aligned}
\alpha_{max} &\geq \alpha_0 \\
1-\alpha_{max} &\leq 1-\alpha_0 \\
\frac{\sqrt{Q}N_1(\sqrt{Q}+\sqrt{P}\rho_{XV})}{Q[P(1-\rho_{XV}^2)+N_1]} &\leq \frac{\sqrt{Q}(N_1+N_2)(\sqrt{Q}+\sqrt{P}\rho_{XV})}{Q[P(1-\rho_{XV}^2)+N_1+N_2]} \\
&\quad - \frac{P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)}}{Q[P(1-\rho_{XV}^2)+N_1+N_2]} \\
\frac{N_1(\sqrt{Q}+\sqrt{P}\rho_{XV})}{P(1-\rho_{XV}^2)+N_1} &\leq \frac{(N_1+N_2)(\sqrt{Q}+\sqrt{P}\rho_{XV})}{P(1-\rho_{XV}^2)+N_1+N_2} \\
&\quad - \frac{P(1-\rho_{XV}^2)\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2}}{P(1-\rho_{XV}^2)+N_1+N_2}
\end{aligned}$$

$$\left\{ \begin{array}{r} N_1(\sqrt{Q}+\sqrt{P}\rho_{XV})[P(1-\rho_{XV}^2)+N_1] \\ +N_1N_2(\sqrt{Q}+\sqrt{P}\rho_{XV}) \end{array} \right\} \leq \left\{ \begin{array}{l} N_1(\sqrt{Q}+\sqrt{P}\rho_{XV})[P(1-\rho_{XV}^2)+N_1] \\ +N_2(\sqrt{Q}+\sqrt{P}\rho_{XV})[P(1-\rho_{XV}^2)+N_1] \\ -[P(1-\rho_{XV}^2)+N_1]P(1-\rho_{XV}^2) \\ \cdot\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2} \end{array} \right\}$$

$$\begin{aligned}
P(1-\rho_{XV}^2)[P(1-\rho_{XV}^2)+N_1]\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2} &\leq P(1-\rho_{XV}^2)N_2(\sqrt{Q}+\sqrt{P}\rho_{XV}) \\
(P(1-\rho_{XV}^2)+N_1)^2(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2) &\leq N_2^2(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 \\
(P(1-\rho_{XV}^2)+N_1)^2((\sqrt{Q}+\sqrt{P}\rho_{XV})^2+P(1-\rho_{XV}^2)+N_1+N_2) &\leq N_2^2(\sqrt{Q}+\sqrt{P}\rho_{XV})^2
\end{aligned}$$

$$\begin{aligned}
(P(1-\rho_{XV}^2)+N_1)^2(P(1-\rho_{XV}^2)+N_1+N_2) &\leq \left\{ \begin{array}{l} (P(1-\rho_{XV}^2)+N_1+N_2) \\ \cdot(N_2-P(1-\rho_{XV}^2)-N_1)(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 \end{array} \right\} \\
(P(1-\rho_{XV}^2)+N_1)^2 &\leq (N_2-P(1-\rho_{XV}^2)-N_1)(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 \\
\frac{(P(1-\rho_{XV}^2)+N_1)^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2} &\leq (N_2-P(1-\rho_{XV}^2)-N_1)
\end{aligned}$$

$$P(1-\rho_{XV}^2)+N_1+\frac{(P(1-\rho_{XV}^2)+N_1)^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2} \quad \leq \quad N_2.$$

■

Appendix XI

Lemma 4.4.8: If $\sqrt{P}\rho_{XV}+\sqrt{Q}>0$,

$$N_{low} \leq N_2 \leq N_{high} \Longrightarrow \alpha_{max} \leq \alpha_0 \leq 1,$$

where

$$\begin{aligned} N_{high} &= P(1-\rho_{XV}^2)+N_1+\frac{[P(1-\rho_{XV}^2)+N_1]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}; \\ N_{low} &= P(1-\rho_{XV}^2)-N_1+\frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}. \end{aligned}$$

Proof: By the proof of Lemma 4.4.7, we have

$$N_2 \leq P(1-\rho_{XV}^2)+N_1+\frac{[P(1-\rho_{XV}^2)+N_1]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2} \Longrightarrow \alpha_{max} \leq \alpha_0.$$

By the proof of Lemma 4.4.9, we have

$$N_2 \geq P(1-\rho_{XV}^2)-N_1+\frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2} \Longrightarrow \alpha_0 \leq 1.$$

Let

$$\begin{aligned} N_{high} &= P(1-\rho_{XV}^2)+N_1+\frac{[P(1-\rho_{XV}^2)+N_1]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}; \\ N_{low} &= P(1-\rho_{XV}^2)-N_1+\frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}. \end{aligned}$$

We can easily get that

$$N_{low} \leq N_2 \leq N_{high} \Longrightarrow \alpha_{max} \leq \alpha_0 \leq 1,$$

■

Appendix XII

Lemma 4.4.9: If $\sqrt{P}\rho_{XV}+\sqrt{Q}>0$,

$$N_2 \leq N_{low} \Longrightarrow \alpha_0 \geq 1,$$

where

$$N_{low} = P(1-\rho_{XV}^2)-N_1+\frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}.$$

Proof: Consider $\alpha_0 \geq 1$ when $\sqrt{P}\rho_{XV} + \sqrt{Q} > 0$.

$$\alpha_0 \geq 1$$

$$\frac{PQ(1-\rho_{XV}^2) - (N_1+N_2)\sqrt{PQ}\rho_{XV} + P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)}}{Q[P(1-\rho_{XV}^2)+N_1+N_2]} \geq 1$$

$$\begin{aligned} P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)} &\geq \sqrt{Q}(N_1+N_2)(\sqrt{Q}+\sqrt{P}\rho_{XV}) \\ P^2(1-\rho_{XV}^2)^2((\sqrt{Q}+\sqrt{P}\rho_{XV})^2 + P(1-\rho_{XV}^2)+N_1+N_2) &\geq (N_1+N_2)^2(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 \end{aligned}$$

$$\begin{aligned} P^2(1-\rho_{XV}^2)^2(P(1-\rho_{XV}^2)+N_1+N_2) &\geq (P(1-\rho_{XV}^2)+N_1+N_2) \\ &\quad \cdot(N_1+N_2-P(1-\rho_{XV}^2))(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 \\ P^2(1-\rho_{XV}^2)^2 &\geq (N_1+N_2-P(1-\rho_{XV}^2))(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 \\ P(1-\rho_{XV}^2) - N_1 + \frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2} &\geq N_2. \end{aligned}$$

■

Appendix XIII

Lemma 4.4.11: If $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$,

$$N_2 \geq N_{high} \Longrightarrow \alpha_{max} \leq \alpha_{-0} \leq \alpha_0,$$

where

$$N_{high} = P(1-\rho_{XV}^2) + N_1 + \frac{[P(1-\rho_{XV}^2)+N_1]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}.$$

Proof: Since $\alpha_{-0} \leq \alpha_0$ is always valid, we only need to prove that $\alpha_{max} \leq \alpha_{-0}$.

$$\begin{aligned} \alpha_{max} &\leq \alpha_{-0} \\ \alpha_{max} - 1 &\leq \alpha_{-0} - 1 \\ -\frac{\sqrt{Q}N_1(\sqrt{Q}+\sqrt{P}\rho_{XV})}{Q[P(1-\rho_{XV}^2)+N_1]} &\leq -\frac{\sqrt{Q}(N_1+N_2)(\sqrt{Q}+\sqrt{P}\rho_{XV})}{Q[P(1-\rho_{XV}^2)+N_1+N_2]} \\ &\quad -\frac{P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)}}{Q[P(1-\rho_{XV}^2)+N_1+N_2]} \\ -\frac{N_1(\sqrt{Q}+\sqrt{P}\rho_{XV})}{P(1-\rho_{XV}^2)+N_1} &\leq -\frac{(N_1+N_2)(\sqrt{Q}+\sqrt{P}\rho_{XV})}{P(1-\rho_{XV}^2)+N_1+N_2} \\ &\quad -\frac{P(1-\rho_{XV}^2)\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2}}{P(1-\rho_{XV}^2)+N_1+N_2} \end{aligned}$$

$$\left\{ \begin{array}{r} -N_1(\sqrt{Q}+\sqrt{P}\rho_{XV})[P(1-\rho_{XV}^2)+N_1] \\ -N_1N_2(\sqrt{Q}+\sqrt{P}\rho_{XV}) \end{array} \right\} \leq \left\{ \begin{array}{l} -N_1(\sqrt{Q}+\sqrt{P}\rho_{XV})[P(1-\rho_{XV}^2)+N_1] \\ -N_2(\sqrt{Q}+\sqrt{P}\rho_{XV})[P(1-\rho_{XV}^2)+N_1] \\ -[P(1-\rho_{XV}^2)+N_1]P(1-\rho_{XV}^2) \\ \cdot\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2} \end{array} \right\}$$

$$P(1-\rho_{XV}^2)[P(1-\rho_{XV}^2)+N_1]\sqrt{P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2} \leq -P(1-\rho_{XV}^2)N_2(\sqrt{Q}+\sqrt{P}\rho_{XV})$$

$$\begin{array}{rcl} (P(1-\rho_{XV}^2)+N_1)^2(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2) & \leq & N_2^2(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 \\ (P(1-\rho_{XV}^2)+N_1)^2((\sqrt{Q}+\sqrt{P}\rho_{XV})^2+P(1-\rho_{XV}^2)+N_1+N_2) & \leq & N_2^2(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 \end{array}$$

$$\begin{array}{rcl} (P(1-\rho_{XV}^2)+N_1)^2(P(1-\rho_{XV}^2)+N_1+N_2) & \leq & (P(1-\rho_{XV}^2)+N_1+N_2) \\ & & \cdot(N_2-P(1-\rho_{XV}^2)-N_1)(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 \\ (P(1-\rho_{XV}^2)+N_1)^2 & \leq & (N_2-P(1-\rho_{XV}^2)-N_1)(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 \\ \frac{(P(1-\rho_{XV}^2)+N_1)^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2} & \leq & (N_2-P(1-\rho_{XV}^2)-N_1) \\ P(1-\rho_{XV}^2)+N_1+\frac{(P(1-\rho_{XV}^2)+N_1)^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2} & \leq & N_2. \end{array}$$

■

Appendix XIV

Lemma 4.4.12: If $\sqrt{P}\rho_{XV}+\sqrt{Q}<0$,

$$N_{low} \leq N_2 \leq N_{high} \Longrightarrow 1 \leq \alpha_{-0} \leq \alpha_{max},$$

where

$$\begin{array}{rcl} N_{high} & = & P(1-\rho_{XV}^2)+N_1+\frac{[P(1-\rho_{XV}^2)+N_1]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}; \\ N_{low} & = & P(1-\rho_{XV}^2)-N_1+\frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}. \end{array}$$

Proof: By the proof of Lemma 4.4.11, we have

$$N_2 \leq P(1-\rho_{XV}^2)+N_1+\frac{[P(1-\rho_{XV}^2)+N_1]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2} \Longrightarrow \alpha_{max} \geq \alpha_{-0}.$$

By the proof of Lemma 4.4.13, we have

$$N_2 \geq P(1-\rho_{XV}^2)-N_1+\frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2} \Longrightarrow \alpha_{-0} \geq 1.$$

Let

$$N_{high} = P(1-\rho_{XV}^2)+N_1+\frac{[P(1-\rho_{XV}^2)+N_1]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2};$$

$$N_{low} = P(1-\rho_{XV}^2) - N_1 + \frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}.$$

We can easily get that

$$N_{low} \le N_2 \le N_{high} \Longrightarrow 1 \le \alpha_{-0} \le \alpha_{max}.$$

■

Appendix XV

Lemma 4.4.13: If $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$,

$$N_2 \le N_{low} \Longrightarrow \alpha_{-0} \le 1,$$

where

$$N_{low} = P(1-\rho_{XV}^2) - N_1 + \frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}.$$

Proof: Consider $\alpha_{-0} \le 1$ when $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$.

$$\alpha_{-0} \le 1$$

$$\frac{PQ(1-\rho_{XV}^2) - (N_1+N_2)\sqrt{PQ}\rho_{XV} - P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)}}{Q[P(1-\rho_{XV}^2)+N_1+N_2]} \le 1$$

$$\begin{aligned} -\sqrt{Q}(N_1+N_2)(\sqrt{Q}+\sqrt{P}\rho_{XV}) &\le P(1-\rho_{XV}^2)\sqrt{Q(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)} \\ (N_1+N_2)^2(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 &\le P^2(1-\rho_{XV}^2)^2((\sqrt{Q}+\sqrt{P}\rho_{XV})^2 + P(1-\rho_{XV}^2) + N_1 + N_2) \end{aligned}$$

$$\begin{aligned} \left\{ \begin{array}{r} (P(1-\rho_{XV}^2)+N_1+N_2) \\ \cdot(N_1+N_2-P(1-\rho_{XV}^2))(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 \end{array} \right\} &\le P^2(1-\rho_{XV}^2)^2(P(1-\rho_{XV}^2)+N_1+N_2) \\ (N_1+N_2-P(1-\rho_{XV}^2))(\sqrt{Q}+\sqrt{P}\rho_{XV})^2 &\le P^2(1-\rho_{XV}^2)^2 \\ N_2 &\le P(1-\rho_{XV}^2) - N_1 + \frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{Q}+\sqrt{P}\rho_{XV})^2}. \end{aligned}$$

■

Appendix XVI

Lemma 5.3.1: A randomly chosen binary matrix H with K rows and N columns has rank K with probability approaching 1 as N goes to infinity and $\frac{K}{N} = R$.

Proof: We consider the K by N binary matrices with rank K. Because there are $2^N - 1$ choices for the first row of H; there are $2^N - 2$ choices for the second row of H once the first row is chosen (any N-vector not in the one dimensional subspace spanned by the first row of H will do, and there are 2^i vectors in a i-dimensional subspace); there are $2^N - 2^2$ choices for the third row of H once the first two rows are chosen (any N-vector not

in the two-dimensional subspace spanned by the first two rows will do), etc. So, there are

$$(2^N-1)(2^N-2)(2^N-4)\cdots(2^N-2^{K-1})$$

possible K by N binary matrices with rank K since there rows are K linearly independent N-vectors.

It is clear that the number of all possible H with K rows and N columns is 2^{NK}. Let the probability that a randomly chosen binary matrix H has rank K be P_N. Then,

$$\begin{aligned} P_N &= \frac{(2^N-1)(2^N-2)(2^N-4)\cdots(2^N-2^{K-1})}{2^{NK}} \\ &= (1-\frac{1}{2^N})(1-\frac{1}{2^{N-1}})(1-\frac{1}{2^{N-2}})\cdots(1-\frac{1}{2^{N-K+1}}) \\ &\geq (1-\frac{1}{2^{N-K+1}})^K \\ &\overset{(a)}{=} (1-\frac{1}{2^{N(1-R)+1}})^{NR}, \end{aligned}$$

where (a) follows that $R=\frac{K}{N}$. Therefore, we have

$$(1-\frac{1}{2^{N(1-R)+1}})^{NR} \leq P_N \leq 1.$$

Recall that

$$\lim_{x\to-\infty}(1+\frac{1}{x})^x = e.$$

Note that

$$\lim_{N\to\infty}(1-\frac{1}{2^{N(1-R)+1}})^{NR} = \lim_{N\to\infty} e^{-\frac{NR}{2^{N(1-R)+1}}} = e^0 = 1.$$

Therefore, we have $\lim_{N\to\infty} P_N \geq 1$. In addition that $P_N \leq 1$, we have $\lim_{N\to\infty} P_N = 1$ and thus complete the proof. ■

Appendix XVII

Lemma 5.4.1: The solution set of the equation (5.7) is a coset of C_2. Here C_2 is the dual code of the code generated by the matrix H_2.

Proof: Denote the solution set of the equation (5.7) is $\mathbf{s}+C_2$. Let $\mathbf{x}(\mathbf{s})$ be a solution of the equation equation (5.7). In the following, we show that $\mathbf{s}+C_2$ is the coset $\mathbf{x}(\mathbf{s})+C_2$.

Let $\mathbf{v}$ be any sequence in the solution set $\mathbf{s}+C_2$. Then,

$$\mathbf{v}{\mathrm{H}_2}^{\mathrm{T}} = \mathbf{x}(\mathbf{s}){\mathrm{H}_2}^{\mathrm{T}} = \left[\begin{array}{cc} \mathbf{0} & \mathbf{s} \end{array}\right].$$

Therefore,

$$(\mathbf{v}-\mathbf{x}(\mathbf{s})){\mathrm{H}_2}^{\mathrm{T}} = \mathbf{0}.$$

Thus we have $\mathbf{v}-\mathbf{x}(\mathbf{s}) \in C_2$ and $\mathbf{v} \in \mathbf{x}(\mathbf{s})+C_2$. So far we have shown that $\mathbf{s}+C_2 \subseteq \mathbf{x}(\mathbf{s})+C_2$.

Note that $\mathbf{s}+C_2$ and $\mathbf{x}(\mathbf{s})+C_2$ have the same amount of sequences, which is equal to $|C_2|$. In addition that $\mathbf{s}+C_2 \subseteq \mathbf{x}(\mathbf{s})+C_2$, we complete the proof that $\mathbf{s}+C_2$ is the coset $\mathbf{x}(\mathbf{s})+C_2$. ■

Appendix XVIII

Lemma 4.4.16: N_{low}, which is defined in (4.67), with respect to ρ_{XV} has the following properties:

(a) when $P = Q$, N_{low} is decreasing as $-1 \leq \rho_{XV} \leq 1$;

(b) when $P > Q$, N_{low} is increasing as $-1 \leq \rho_{XV} \leq -\frac{\sqrt{Q}}{\sqrt{P}}$ and decreasing as $-\frac{\sqrt{Q}}{\sqrt{P}} \leq \rho_{XV} \leq 1$;

(c) when $P < Q$, N_{low} is increasing as $-1 \leq \rho_{XV} \leq \delta_0$ and decreasing as $\delta_0 \leq \rho_{XV} \leq 1$, where

$$\delta_0 = \frac{2\sqrt{6}}{3}\sqrt{\frac{Q-P}{P}}\cos\frac{\theta-\pi}{3} - \sqrt{\frac{Q}{P}}, \qquad \theta = \arccos\frac{3\sqrt{6}}{8}\sqrt{\frac{Q-P}{Q}}.$$

Proof: Consider

$$f(\delta) = N_{low}|_{\rho_{XV}=\delta} = P(1-\delta^2) - N_1 + \frac{[P(1-\delta^2)]^2}{(\sqrt{P}\delta + \sqrt{Q})^2}.$$

Calculate the derivative of $f(\delta)$ with respect to δ. We have

$$\begin{aligned} f'(\delta) &= -\frac{2P}{(\sqrt{P}\delta+\sqrt{Q})^3}\{\sqrt{P}(\sqrt{P}+\sqrt{Q}\delta)^2 + \sqrt{Q}\delta(\sqrt{P}\delta+\sqrt{Q})^2\} \\ &= -\frac{2P^2\sqrt{Q}}{(\sqrt{P}\delta+\sqrt{Q})^3}\{\delta^3 + 3\frac{\sqrt{Q}}{\sqrt{P}}\delta^2 + (2+\frac{Q}{P})\delta + \frac{\sqrt{P}}{\sqrt{Q}}\} \\ &= -\frac{2\sqrt{PQ}}{(\delta+\frac{\sqrt{Q}}{\sqrt{P}})^3}\{(\delta+\frac{\sqrt{Q}}{\sqrt{P}})^3 + 2\frac{P-Q}{P}(\delta+\frac{\sqrt{Q}}{\sqrt{P}}) + \frac{(P-Q)^2}{P\sqrt{PQ}}\}. \end{aligned}$$

If $P = Q$, it is easy to verify that

$$f'(\delta) = -2\sqrt{PQ}.$$

Otherwise, we let

$$g(x) = x^3 + 2\frac{P-Q}{P}x + \frac{(P-Q)^2}{P\sqrt{PQ}}.$$

Consider the cubic equation $g(x) = 0$. Let

$$a = 1; \quad b = 0; \quad c = 2\frac{P-Q}{P}; \quad d = \frac{(P-Q)^2}{P\sqrt{PQ}},$$

and

$$\begin{aligned} A &= b^2 - 3ac = -6\frac{P-Q}{P}; \\ B &= bc - 9ad = -9\frac{(P-Q)^2}{P\sqrt{PQ}}; \\ C &= c^2 - 3bd = 4\frac{(P-Q)^2}{P^2}. \end{aligned}$$

By Shengjin's Formula [14], we can calculate the discriminant as follows:

$$\Delta = B^2 - 4AC = 3\frac{(P-Q)^3}{P^3Q}(27P+5Q).$$

Therefore, under the assumption that $P, Q > 0$, we have

$$\Delta > 0, \text{ if } P > Q \quad \text{and} \quad \Delta < 0, \text{ if } P < Q.$$

By Shengjins Distinguishing Means [14], if $P > Q$, $g(x)$ has only one real root; Otherwise, if $P < Q$, $g(x)$ has three distinct real roots.

Consider the situation when $P > Q$. Let

$$\begin{aligned} Y_1 &= Ab + 3a(-B + \sqrt{\Delta})/2 \\ &= \frac{27(P-Q)^2}{2P\sqrt{PQ}}(\sqrt{\frac{P+5Q/27}{P-Q}} + 1); \\ Y_2 &= Ab + 3a(-B - \sqrt{\Delta})/2 \\ &= -\frac{27(P-Q)^2}{2P\sqrt{PQ}}(\sqrt{\frac{P+5Q/27}{P-Q}} - 1). \end{aligned}$$

By Shengjin's Formula [14], the only real root is

$$\begin{aligned} x_0 &= \frac{-b - \sqrt[3]{Y_1} - \sqrt[3]{Y_2}}{3a} \\ &= -\sqrt[3]{\frac{(P-Q)^2}{2P\sqrt{PQ}}}(\sqrt[3]{\sqrt{\frac{P+5Q/27}{P-Q}} + 1} - \sqrt[3]{\sqrt{\frac{P+5Q/27}{P-Q}} - 1}). \end{aligned}$$

Correspondingly, the only real root of equation $f'(\delta) = 0$ is

$$\delta_r = x_0 - \frac{\sqrt{Q}}{\sqrt{P}}.$$

It is clear that $\delta_r < -\frac{\sqrt{Q}}{\sqrt{P}}$, since $x_0 < 0$. Therefore, we have $f'(\delta) \geq 0$, if $\delta_r \leq \delta \leq -\frac{\sqrt{Q}}{\sqrt{P}}$; otherwise, $f'(\delta) \leq 0$. However, we only care about the δ such that $-1 \leq \delta \leq 1$. If $\delta_r \leq -1$, then $f(\delta)$, also $N_{low}|_{\rho_{XV}=\delta}$, is increasing as $-1 \leq \delta \leq -\frac{\sqrt{Q}}{\sqrt{P}}$ and decreasing as $-\frac{\sqrt{Q}}{\sqrt{P}} \leq \delta \leq 1$.

In the following, we will prove that $\delta_r < -1$. It is known that $f'(\delta)|_{\delta=\delta_r} = 0$. Here, we calculate $f'(\delta)|_{\delta=-1}$.

$$\begin{aligned} f'(\delta)|_{\delta=-1} &= -\frac{2\sqrt{PQ}}{(-1+\frac{\sqrt{Q}}{\sqrt{P}})^3}\{(-1+\frac{\sqrt{Q}}{\sqrt{P}})^3 + 2\frac{P-Q}{P}(-1+\frac{\sqrt{Q}}{\sqrt{P}}) + \frac{(P-Q)^2}{P\sqrt{PQ}}\} \\ &= 2P > 0. \end{aligned}$$

Since $f'(\delta) > 0$ only happens when $\delta_r \leq \delta \leq -\frac{\sqrt{Q}}{\sqrt{P}}$, so we have $\delta_r \leq -1$.

Now let us consider the situation when $P < Q$. Let

$$\begin{aligned} T &= \frac{2Ab - 3aB}{2A\sqrt{A}} = \frac{3\sqrt{6}}{8}\sqrt{\frac{Q-P}{Q}}; \\ \theta &= \arccos T. \end{aligned}$$

By Shengjin's Formula [14], the three distinct roots are

$$\begin{aligned} x_1 &= \frac{-b - 2\sqrt{A}\cos\frac{\theta}{3}}{3a} = \frac{2\sqrt{6}}{3}\sqrt{\frac{Q-P}{P}}\cos\frac{\theta+3\pi}{3}; \\ x_2 &= \frac{-b + \sqrt{A}(\cos\frac{\theta}{3} + \sqrt{3}\sin\frac{\theta}{3})}{3a} = \frac{2\sqrt{6}}{3}\sqrt{\frac{Q-P}{P}}\cos\frac{\theta-\pi}{3}; \\ x_3 &= \frac{-b + \sqrt{A}(\cos\frac{\theta}{3} - \sqrt{3}\sin\frac{\theta}{3})}{3a} = \frac{2\sqrt{6}}{3}\sqrt{\frac{Q-P}{P}}\cos\frac{\theta+\pi}{3}. \end{aligned}$$

It is easy to verify that $x_2 \geq x_3 \geq 0 \geq x_1$. Correspondingly, the three distinct real roots of equation $f'(\delta) = 0$ are

$$\delta_{r_1} = x_1 - \frac{\sqrt{Q}}{\sqrt{P}}; \quad \delta_{r_2} = x_2 - \frac{\sqrt{Q}}{\sqrt{P}}; \quad \delta_{r_3} = x_3 - \frac{\sqrt{Q}}{\sqrt{P}}.$$

It is clear that $\delta_{r_2} \geq \delta_{r_3} \geq -\frac{\sqrt{Q}}{\sqrt{P}} \geq \delta_{r_1}$. Therefore, we have $f'(\delta) \geq 0$, if $\delta_{r_1} \leq \delta \leq -\frac{\sqrt{Q}}{\sqrt{P}}$ or $\delta_{r_3} \leq \delta \leq \delta_{r_2}$; otherwise, $f'(\delta) \leq 0$. However, we only care about the δ such that $-1 \leq \delta \leq 1$. If $\delta_{r_3} \leq -1 \leq \delta_2$, then $f(\delta)$, also $N_{low}|_{\rho_{XV}=\delta}$, is increasing as $-1 \leq \delta \leq \delta_{r_2}$ and decreasing as $\delta_{r_2} \leq \delta \leq 1$.

In the following, we will prove that $\delta_{r_3} \leq -1 \leq \delta_{r_2}$. It is known that $f'(\delta) > 0$ when $\delta_{r_1} \leq \delta \leq -\frac{\sqrt{Q}}{\sqrt{P}}$ or $\delta_{r_3} \leq \delta \leq \delta_{r_2}$. Since $P < Q$, $-\frac{\sqrt{Q}}{\sqrt{P}} < -1$. Thus, we only need to prove that $f'(\delta)|_{\delta=-1} > 0$. Note that $f'(\delta)|_{\delta=-1} = 2P > 0$. Let $\delta_0 = \delta_{r_2}$. Thus we complete the proof. ■

Appendix XIX

Lemma 4.4.17: N_{high}, which is defined in (4.66), with respect to ρ_{XV} has the following properties:

(a) when $P = Q$, N_{high} is decreasing as $-1 \leq \rho_{XV} \leq 1$;

(b) when $P > Q$, N_{high} is increasing as $-1 \leq \rho_{XV} \leq -\frac{\sqrt{Q}}{\sqrt{P}}$ and decreasing as $-\frac{\sqrt{Q}}{\sqrt{P}} \leq \rho_{XV} \leq 1$;

(c) when $P < Q$, if $N_1 \geq \sqrt[4]{P}(\sqrt[4]{P} + \sqrt[4]{Q})(\sqrt{Q} - \sqrt{P})$, N_{high} is increasing as $-1 \leq \rho_{XV} \leq \delta_{00}$ and decreasing as $\delta_{00} \leq \rho_{XV} \leq 1$; otherwise, N_{high} is decreasing as $-1 \leq \rho_{XV} \leq 1$. Here

$$\delta_{00} = \frac{2\sqrt{6}}{3}\sqrt{\frac{Q-P-N_1}{P}}\cos\frac{\phi-\pi}{3} - \sqrt{\frac{Q}{P}}, \qquad \phi = \arccos\frac{3\sqrt{6}}{8}\sqrt{\frac{Q-P-N_1}{Q}}.$$

Proof: Consider

$$f(\delta) = N_{high}|_{\rho_{XV}=\delta} = P(1-\delta^2) + N_1 + \frac{[P(1-\delta^2)+N_1]^2}{(\sqrt{P}\delta + \sqrt{Q})^2}.$$

Calculate the derivative of $f(\delta)$ with respect to δ. We have

$$\begin{aligned} f'(\delta) &= -\frac{2\sqrt{P}}{(\sqrt{P}\delta+\sqrt{Q})^3}\{(P+N_1+\sqrt{PQ}\delta)^2 + \sqrt{PQ}\delta(\sqrt{P}\delta+\sqrt{Q})^2\} \\ &= -\frac{2P^2\sqrt{Q}}{(\sqrt{P}\delta+\sqrt{Q})^3}\{\delta^3 + 3\frac{\sqrt{Q}}{\sqrt{P}}\delta^2 + \frac{2P+2N_1+Q}{P}\delta + \frac{(P+N_1)^2}{P\sqrt{PQ}}\} \\ &= -\frac{2\sqrt{PQ}}{(\delta+\frac{\sqrt{Q}}{\sqrt{P}})^3}\{(\delta+\frac{\sqrt{Q}}{\sqrt{P}})^3 + 2\frac{P+N_1-Q}{P}(\delta+\frac{\sqrt{Q}}{\sqrt{P}}) + \frac{(P+N_1-Q)^2}{P\sqrt{PQ}}\}. \end{aligned}$$

If $P+N_1 = Q$, it is easy to verify that

$$f'(\delta) = -2\sqrt{PQ}.$$

Otherwise, we let

$$g(x) = x^3 + 2\frac{P+N_1-Q}{P}x + \frac{(P+N_1-Q)^2}{P\sqrt{PQ}}.$$

Consider the cubic equation $g(x) = 0$. Let

$$a = 1; \quad b = 0; \quad c = 2\frac{P+N_1-Q}{P}; \quad d = \frac{(P+N_1-Q)^2}{P\sqrt{PQ}},$$

and

$$\begin{aligned} A &= b^2 - 3ac = -6\frac{P+N_1-Q}{P}; \\ B &= bc - 9ad = -9\frac{(P+N_1-Q)^2}{P\sqrt{PQ}}; \\ C &= c^2 - 3bd = 4\frac{(P+N_1-Q)^2}{P^2}. \end{aligned}$$

By Shengjin's Formula [14], we can calculate the discriminant as follows:

$$\Delta = B^2 - 4AC = 3\frac{(P+N_1-Q)^3}{P^3Q}(27(P+N_1)+5Q).$$

Therefore, under the assumption that $P, Q > 0$, we have

$$\Delta > 0, \text{ if } P+N_1 > Q \quad \text{and} \quad \Delta < 0, \text{ if } P+N_1 < Q.$$

By Shengjins Distinguishing Means [14], if $P+N_1 > Q$, $g(x)$ has only one real root; Otherwise, if $P+N_1 < Q$, $g(x)$ has three distinct real roots.

Consider the situation when $P+N_1 > Q$. Let

$$Y_1 = Ab + 3a(-B+\sqrt{\Delta})/2$$

$$
\begin{aligned}
&= \frac{27(P-Q)^2}{2P\sqrt{PQ}}(\sqrt{\frac{P+5Q/27}{P-Q}}+1);\\
Y_2 &= Ab+3a(-B-\sqrt{\Delta})/2\\
&= -\frac{27(P+N_1-Q)^2}{2P\sqrt{PQ}}(\sqrt{\frac{P+N_1+5Q/27}{P+N_1-Q}}-1).
\end{aligned}
$$

By Shengjin's Formula [14], the only real root is

$$
\begin{aligned}
x_0 &= \frac{-b-\sqrt[3]{Y_1}-\sqrt[3]{Y_2}}{3a}\\
&= -\sqrt[3]{\frac{(P+N_1-Q)^2}{2P\sqrt{PQ}}}(\sqrt[3]{\sqrt{\frac{P+N_1+5Q/27}{P+N_1-Q}}+1}-\sqrt[3]{\sqrt{\frac{P+N_1+5Q/27}{P+N_1-Q}}-1}).
\end{aligned}
$$

Correspondingly, the only real root of equation $f'(\delta)=0$ is

$$\delta_r = x_0 - \frac{\sqrt{Q}}{\sqrt{P}}.$$

It is clear that $\delta_r < -\frac{\sqrt{Q}}{\sqrt{P}}$, since $x_0 < 0$. Therefore, we have $f'(\delta) \geq 0$, if $\delta_r \leq \delta \leq -\frac{\sqrt{Q}}{\sqrt{P}}$; otherwise, $f'(\delta) \leq 0$. However, we only care about the δ such that $-1 \leq \delta \leq 1$. If $P \leq Q < P+N_1$, we have $\delta_r < -\frac{\sqrt{Q}}{\sqrt{P}} \leq -1$. Then $f(\delta)$, also $N_{high}|_{rho_{XV}=\delta}$, is decreasing as $-1 \leq \delta \leq 1$. Otherwise, if $P > Q$ and $\delta_r \leq -1$, then $f(\delta)$, also $N_{high}|_{rho_{XV}=\delta}$, is increasing as $-1 \leq \delta \leq -\frac{\sqrt{Q}}{\sqrt{P}}$ and decreasing as $-\frac{\sqrt{Q}}{\sqrt{P}} \leq \delta \leq 1$.

In the following, we will prove that when $P > Q$, $\delta_r < -1$. It is known that $f'(\delta)|_{\delta=\delta_r} = 0$. Here, we calculate $f'(\delta)|_{\delta=-1}$.

$$
\begin{aligned}
f'(\delta)|_{\delta=-1} &= -\frac{2\sqrt{PQ}}{(-1+\frac{\sqrt{Q}}{\sqrt{P}})^3}\{(-1+\frac{\sqrt{Q}}{\sqrt{P}})^3 + 2\frac{P+N_1-Q}{P}(-1+\frac{\sqrt{Q}}{\sqrt{P}}) + \frac{(P+N_1-Q)^2}{P\sqrt{PQ}}\}\\
&= -\frac{2\sqrt{P}}{(\sqrt{Q}-\sqrt{P})^3}\{(P+N_1-\sqrt{PQ})^2 - \sqrt{PQ}(\sqrt{Q}-\sqrt{P})^2\}\\
&= -\frac{2\sqrt{P}}{(\sqrt{Q}-\sqrt{P})^3}\{(P+N_1-\sqrt{PQ})^2 - \sqrt{PQ}(\sqrt{Q}-\sqrt{P})^2\}\\
&\geq -\frac{2\sqrt{P}}{(\sqrt{Q}-\sqrt{P})^3}\{(P-\sqrt{PQ})^2 - \sqrt{PQ}(\sqrt{Q}-\sqrt{P})^2\}\\
&= -\frac{2\sqrt{P}}{(\sqrt{Q}-\sqrt{P})^3}\{(P-\sqrt{PQ})^2 - \sqrt{PQ}(\sqrt{Q}-\sqrt{P})^2\}\\
&= 2P > 0.
\end{aligned}
$$

Since $f'(\delta) > 0$ only happens when $\delta_r \leq \delta \leq -\frac{\sqrt{Q}}{\sqrt{P}}$, so we have $\delta_r \leq -1$.

Now let us consider the situation when $P + N_1 < Q$. Let

$$T = \frac{2Ab-3aB}{2A\sqrt{A}} = \frac{3\sqrt{6}}{8}\sqrt{\frac{Q-P-N_1}{Q}};$$

$$\phi = \arccos T.$$

By Shengjin's Formula [14], the three distinct roots are

$$\begin{aligned}
x_1 &= \frac{-b-2\sqrt{A}\cos\frac{\theta}{3}}{3a} = \frac{2\sqrt{6}}{3}\sqrt{\frac{Q-P-N_1}{P}}\cos\frac{\phi+3\pi}{3};\\
x_2 &= \frac{-b+\sqrt{A}(\cos\frac{\theta}{3}+\sqrt{3}\sin\frac{\phi}{3})}{3a} = \frac{2\sqrt{6}}{3}\sqrt{\frac{Q-P-N_1}{P}}\cos\frac{\phi-\pi}{3};\\
x_3 &= \frac{-b+\sqrt{A}(\cos\frac{\theta}{3}-\sqrt{3}\sin\frac{\phi}{3})}{3a} = \frac{2\sqrt{6}}{3}\sqrt{\frac{Q-P-N_1}{P}}\cos\frac{\phi+\pi}{3}.
\end{aligned}$$

It is easy to verify that $x_2 \geq x_3 \geq 0 \geq x_1$. Correspondingly, the three distinct real roots of equation $f'(\delta)=0$ are

$$\delta_{r_1} = x_1 - \frac{\sqrt{Q}}{\sqrt{P}}; \quad \delta_{r_2} = x_2 - \frac{\sqrt{Q}}{\sqrt{P}}; \quad \delta_{r_3} = x_3 - \frac{\sqrt{Q}}{\sqrt{P}}.$$

It is clear that $\delta_{r_2} \geq \delta_{r_3} \geq -\frac{\sqrt{Q}}{\sqrt{P}} \geq \delta_{r_1}$. Therefore, we have $f'(\delta) \geq 0$, if $\delta_{r_1} \leq \delta \leq -\frac{\sqrt{Q}}{\sqrt{P}}$ or $\delta_{r_3} \leq \delta \leq \delta_{r_2}$; otherwise, $f'(\delta) \leq 0$. However, we only care about the δ such that $-1 \leq \delta \leq 1$. If $\delta_{r_3} \leq -1 \leq \delta_2$, then $f(\delta)$, also $N_{high}|_{\rho_{XV}=\delta}$, is increasing as $-1 \leq \delta \leq \delta_{r_2}$ and decreasing as $\delta_{r_2} \leq \delta \leq 1$. Otherwise, if $\delta_{r_3} \leq \delta_2 \leq -1$, then $f(\delta)$, also $N_{high}|_{\rho_{XV}=\delta}$, is decreasing as $-1 \leq \delta \leq 1$. In the following, we will prove that

$$\begin{aligned}
&\delta_{r_3} \leq -1 \leq \delta_{r_2}, \qquad \text{when } N_1 \leq \sqrt[4]{P}(\sqrt[4]{P}+\sqrt[4]{Q})(\sqrt{Q}-\sqrt{P});\\
&\delta_{r_3} \leq \delta_{r_2} \leq -1, \qquad \text{when } \sqrt[4]{P}(\sqrt[4]{P}+\sqrt[4]{Q})(\sqrt{Q}-\sqrt{P}) \leq N_1 \leq Q-P.
\end{aligned}$$

It is known that $f'(\delta) > 0$ when $\delta_{r_1} \leq \delta \leq -\frac{\sqrt{Q}}{\sqrt{P}}$ or $\delta_{r_3} \leq \delta \leq \delta_{r_2}$. Since $P+N_1 < Q$, $-\frac{\sqrt{Q}}{\sqrt{P}} < -1$. Thus, if $f'(\delta)|_{\delta=-1} \geq 0$, then $\delta_{r_3} \leq -1 \leq \delta_{r_2}$. Note that

$$\begin{aligned}
f'(\delta)|_{\delta=-1} &= -\frac{2\sqrt{P}}{(\sqrt{Q}-\sqrt{P})^3}\{(P+N_1-\sqrt{PQ})^2 - \sqrt{PQ}(\sqrt{Q}-\sqrt{P})^2\}\\
&= -\frac{2\sqrt{P}}{(\sqrt{Q}-\sqrt{P})^3}(N_1+\sqrt[4]{P}(\sqrt[4]{Q}-\sqrt[4]{P})(\sqrt{Q}-\sqrt{P}))(N_1-\sqrt[4]{P}(\sqrt[4]{P}+\sqrt[4]{Q})(\sqrt{Q}-\sqrt{P})).
\end{aligned}$$

It is clear that if $N_1 \leq \sqrt[4]{P}(\sqrt[4]{P}+\sqrt[4]{Q})(\sqrt{Q}-\sqrt{P})$, $f'(\delta)|_{\delta=-1} > 0$. In this case, $\delta_{r_3} \leq -1 \leq \delta_{r_2}$. Otherwise, if $\sqrt[4]{P}(\sqrt[4]{P}+\sqrt[4]{Q})(\sqrt{Q}-\sqrt{P}) \leq N_1 \leq Q-P$, $f'(\delta)|_{\delta=-1} \leq 0$. In addition,

$$\begin{aligned}
f'(\delta)\big|_{\delta=-\frac{\sqrt{P+N_1}}{\sqrt{P}}} &= -\frac{2\sqrt{PQ}}{(-\frac{\sqrt{P+N_1}}{\sqrt{P}}+\frac{\sqrt{Q}}{\sqrt{P}})^3}\cdot\\
&\quad \{(-\frac{\sqrt{P+N_1}}{\sqrt{P}}+\frac{\sqrt{Q}}{\sqrt{P}})^3 + 2\frac{P+N_1-Q}{P}(-\frac{\sqrt{P+N_1}}{\sqrt{P}}+\frac{\sqrt{Q}}{\sqrt{P}}) + \frac{(P+N_1-Q)^2}{P\sqrt{PQ}}\}\\
&= 2\sqrt{P(P+N_1)} > 0.
\end{aligned}$$

Thus we have $\delta_{r_3} \leq -\frac{\sqrt{P+N_1}}{\sqrt{P}} \leq \delta_{r_2}$. Since $-1 > -\frac{\sqrt{P+N_1}}{\sqrt{P}}$ and $f'(\delta)|_{\delta=-1} \leq 0$ when $\sqrt[4]{P}(\sqrt[4]{P}+\sqrt[4]{Q})(\sqrt{Q}-\sqrt{P}) \leq N_1 \leq Q-P$, so in this case, we have $\delta_{r_3} \leq \delta_{r_2} \leq -1$. Let $\delta_{00} = \delta_{r_2}$. We complete the proof. ■

Appendix XX

Lemma 4.4.18: $R(\alpha_{max})$, $R_Z(1)$ and $R(\alpha_*)$ with respect to ρ_{XV} have the following properties:

(a) $R(\alpha_{max})$ is increasing as $-1 \le \rho_{XV} \le 0$; decreasing as $0 \le \rho_{XV} \le 1$; maximized at $\rho_{XV} = 0$.

(b) $R_Z(1)$ is increasing as $-1 \le \rho_{XV} \le 1$.

(c) $R(\alpha_*)$ satisfies the following inequalities.

$$\begin{aligned}
R(\alpha_0)|_{\rho_{XV}} &\le R(\alpha_0)|_{\rho_{XV}=\delta_1} && \text{if } \rho_{XV} \le \delta_1,\\
R(\alpha_0)|_{\rho_{XV}} &\le R(\alpha_0)|_{\rho_{XV}=\delta_2} && \text{if } |\rho_{XV}| \ge \delta_2,\\
R(\alpha_{-0})|_{\rho_{XV}} &\le R(\alpha_{-0})|_{\rho_{XV}=\delta_2^-} && \text{if } -1 \le \rho_{XV} \le \delta_2^- < -\sqrt{Q}/\sqrt{P},\\
R(\alpha_{-0})|_{\rho_{XV}} &\le R(\alpha_{-0})|_{\rho_{XV}=\delta_1^-} && \text{if } -1 \le \rho_{XV} \le \delta_1^- < -\sqrt{Q}/\sqrt{P}.
\end{aligned}$$

In particular,

$$\begin{aligned}
R(\alpha_0)|_{\rho_{XV}=\delta_1} &= R_Z(1)|_{\rho_{XV}=\delta_1}, & R(\alpha_0)|_{\rho_{XV}=\delta_2} &= R(\alpha_{max})|_{\rho_{XV}=\delta_2},\\
R(\alpha_{-0})|_{\rho_{XV}=\delta_1^-} &\le R(\alpha_0)|_{\rho_{XV}=\delta_1}, & R(\alpha_{-0})|_{\rho_{XV}=\delta_2^-} &\le R(\alpha_0)|_{\rho_{XV}=\delta_2}.
\end{aligned}$$

Proof: First, we consider $R(\alpha_{max})$. From (4.62),

$$R(\alpha_{max}) = \frac{1}{2}\log(1 + \frac{P(1-\rho_{XV}^2)}{N_1}).$$

Since $|\rho_{XV}| \le 1$, it is clear that $R(\alpha_{max})$ is increasing with respect ρ_{XV} as $-1 \le \rho_{XV} \le 0$, is decreasing as $0 \le \rho_{XV} \le 1$, and is maximized at $\rho_{XV} = 0$.

Secondly, we consider $R_Z(1)$. From (4.65),

$$R_Z(1) = \frac{1}{2}\log\frac{(P+Q+2\sqrt{PQ}\rho_{XV}+N_1)(N_1+N_2)}{(P+Q+2\sqrt{PQ}\rho_{XV}+N_1+N_2)N_1}.$$

In addition to $|\rho_{XV}| \le 1$, it is clear that $R_Z(1)$ is increasing with respect to ρ_{XV} as $-1 \le \rho_{XV} \le 1$.

At the last, we consider $R(\alpha_0)$ and $R(\alpha_{-0})$. First, referring to the definitions of α_0 in (4.56), $R(\alpha)$ in (4.47) and $R_Z(\alpha)$ in (4.49), we have

$$\begin{aligned}
R(\alpha_0) &= \frac{1}{2}\log\frac{P(1-\rho_{XV}^2)(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{(1-\alpha_0)^2PQ(1-\rho_{XV}^2)+N_1(P+{\alpha_0}^2Q+2\alpha_0\sqrt{PQ}\rho_{XV})}\\
&= -\frac{1}{2}\log\{\frac{N_1}{P(1-\rho_{XV}^2)+N_1}+f(\rho_{XV})\};\\
R_Z(\alpha_0) &= \frac{1}{2}\log(\frac{(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{(P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})}\cdot\\
&\quad \frac{\{(1-\alpha_0)^2PQ(1-\rho_{XV}^2)+(N_1+N_2)(P+{\alpha_0}^2Q+2\alpha_0\sqrt{PQ}\rho_{XV})\}}{\{(1-\alpha_0)^2PQ(1-\rho_{XV}^2)+N_1(P+{\alpha_0}^2Q+2\alpha_0\sqrt{PQ}\rho_{XV})\}})\\
&= \frac{1}{2}\log(1-\frac{N_2}{(P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})})(1+\frac{N_2}{g(\rho_{XV})+N_1}),
\end{aligned}$$

where

$$f(\rho_{XV}) = \frac{P(1-\rho_{XV}^2)\{\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}}[P(1-\rho_{XV}^2)+N_1] - N_2(\sqrt{P}\rho_{XV}+\sqrt{Q})\}^2}{(P+Q+N_1+2\sqrt{PQ}\rho_{XV})[P(1-\rho_{XV}^2)+N_1][P(1-\rho_{XV}^2)+N_1+N_2]^2},$$

$$g(\rho_{XV}) = \frac{\{P(1-\rho_{XV}^2)\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}} - (N_1+N_2)(\sqrt{P}\rho_{XV}+\sqrt{Q})\}^2}{[P(1-\rho_{XV}^2)+N_1+N_2]^2 + P(1-\rho_{XV}^2)\{\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}} + (\sqrt{P}\rho_{XV}+\sqrt{Q})\}^2}.$$

First, let us consider $f(\rho_{XV})$. Let

$$f_1(\rho_{XV}) = \sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}}[P(1-\rho_{XV}^2)+N_1] - N_2(\sqrt{P}\rho_{XV}+\sqrt{Q}).$$

Then we have if $\sqrt{P}\rho_{XV}+\sqrt{Q} \geq 0$,

$$\begin{aligned}
f_1(\rho_{XV}) &= 0 \\
N_2(\sqrt{P}\rho_{XV}+\sqrt{Q}) &= \sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}}[P(1-\rho_{XV}^2)+N_1] \\
N_2^2(\sqrt{P}\rho_{XV}+\sqrt{Q})^2 &= (P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})[P(1-\rho_{XV}^2)+N_1]^2 \\
N_2 &= P(1-\rho_{XV}^2)+N_1+\frac{[P(1-\rho_{XV}^2)+N_1]^2}{(\sqrt{P}\rho_{XV}+\sqrt{Q})^2} \\
N_2 &= N_{high}|_{\rho_{XV}}.
\end{aligned}$$

If δ_2 is the only correlation coefficient or the larger solution to the equation $N_2 = N_{high}|_{\rho_{XV}}$, then by Lemma 4.4.17, $\sqrt{P}\rho_{XV}+\sqrt{Q} \geq 0$. It is clear that $f_1(\delta_2) = 0$ and $f(\delta_2) = 0$. Note that for $|\rho_{XV}| \geq |\delta_2|$, $f(\rho_{XV}) \geq f(\delta_2)$. Correspondingly, we have

$$R(\alpha_0)|_{\rho_{XV}} \leq R(\alpha_0)|_{\rho_{XV}=\delta_2}, \quad \text{for } |\rho_{XV}| \geq |\delta_2|.$$

In particular,

$$\begin{aligned}
R(\alpha_0)|_{\rho_{XV}=\delta_2} &= -\frac{1}{2}\log\{\frac{N_1}{P(1-{\delta_2}^2)+N_1} + f(\delta_2)\} \\
&= \frac{1}{2}\log(1+\frac{P(1-{\delta_2}^2)}{N_1}) \\
&= R(\alpha_{max})|_{\rho_{XV}=\delta_2}.
\end{aligned}$$

Furthermore, if δ_2^- is another solution to the equation $N_2 = N_{high}|_{\rho_{XV}}$ and $\sqrt{P}\delta_2^- + \sqrt{Q} \geq 0$, then $\delta_2^- < 0$. By Lemma 4.4.17, $|\delta_2^-| \geq |\delta_2|$. Note that $f_1(\delta_2^-) = 0$ and $f(\delta_2^-) = 0$. Then for $-1 \leq \rho_{XV} \leq \delta_2^-$, $f(\rho_{XV}) \geq f(\delta_2^-)$. Correspondingly, we have

$$R(\alpha_0)|_{\rho_{XV}} \leq R(\alpha_0)|_{\rho_{XV}=\delta_2^-}, \quad \text{for } -1 \leq \rho_{XV} \leq \delta_2^-.$$

In particular,

$$\begin{aligned}
R(\alpha_0)|_{\rho_{XV}=\delta_2^-} &= -\frac{1}{2}\log\{\frac{N_1}{P(1-\delta_2^{-2})+N_1} + f(\delta_2^-)\} \\
&= \frac{1}{2}\log(1+\frac{P(1-\delta_2^{-2})}{N_1})
\end{aligned}$$

$$= \quad R(\alpha_{max})|_{\rho_{XV}=\delta_2^-}.$$

Clearly, since $|\delta_2^-| \geq |\delta_2|$,

$$R(\alpha_0)|_{\rho_{XV}=\delta_2^-} \leq R(\alpha_0)|_{\rho_{XV}=\delta_2}.$$

Now let us consider $g(\rho_{XV})$. Let

$$g_1(\rho_{XV}) = P(1-\rho_{XV}^2)\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}} - (N_1+N_2)(\sqrt{P}\rho_{XV}+\sqrt{Q}).$$

Then we have if $\sqrt{P}\rho_{XV}+\sqrt{Q} \geq 0$,

$$\begin{aligned}
g_1(\rho_{XV}) &= 0 \\
(N_1+N_2)(\sqrt{P}\rho_{XV}+\sqrt{Q}) &= P(1-\rho_{XV}^2)\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}} \\
(N_1+N_2)^2(\sqrt{P}\rho_{XV}+\sqrt{Q})^2 &= (P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})[P(1-\rho_{XV}^2)]^2 \\
N_2 &= P(1-\rho_{XV}^2) - N_1 + \frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{P}\rho_{XV}+\sqrt{Q})^2} \\
N_2 &= N_{low}|_{\rho_{XV}}.
\end{aligned}$$

If δ_1 is the only correlation coefficient or the larger solution to the equation $N_2 = N_{low}|_{\rho_{XV}}$, then by Lemma 4.4.17, $\sqrt{P}\rho_{XV}+\sqrt{Q} \geq 0$. It is clear that $g_1(\delta_1) = 0$ and $g(\delta_1) = 0$. Then for $-1 \leq \rho_{XV} \leq \delta_1$, $g(\rho_{XV}) \geq g(\delta_1)$. Correspondingly, we have

$$R_Z(\alpha_0)|_{\rho_{XV}} \leq R_Z(\alpha_0)|_{\rho_{XV}=\delta_1}, \quad \text{for } -1 \leq \rho_{XV} \leq \delta_1.$$

In particular,

$$\begin{aligned}
R_Z(\alpha_0)|_{\rho_{XV}=\delta_1} &= \frac{1}{2}\log(1-\frac{N_2}{(P+Q+N_1+N_2+2\sqrt{PQ}\delta_1)})(1+\frac{N_2}{g(\delta_1)+N_1}) \\
&= R_Z(1)|_{\rho_{XV}=\delta_1}.
\end{aligned}$$

Note that from (4.58) we have $R(\alpha_0) = R_Z(\alpha_0)$. As we have discussed above, we can draw such a conclusion that

$$\begin{aligned}
&R(\alpha_0)|_{\rho_{XV}} \leq R(\alpha_0)|_{\rho_{XV}=\delta_2}, && \text{for } |\rho_{XV}| \geq |\delta_2|; \\
&R(\alpha_0)|_{\rho_{XV}} \leq R(\alpha_0)|_{\rho_{XV}=\delta_1}, && \text{for } -1 \leq \rho_{XV} \leq \delta_1.
\end{aligned}$$

Furthermore,

$$R(\alpha_0)|_{\rho_{XV}=\delta_2^-} \leq R(\alpha_0)|_{\rho_{XV}=\delta_2} = R(\alpha_{max})|_{\rho_{XV}=\delta_2}, \quad R(\alpha_0)|_{\rho_{XV}=\delta_1} = R_Z(1)|_{\rho_{XV}=\delta_1}.$$

Similarly, applying α_{-0} defined in (4.57) to $R(\alpha)$ and $R_Z(\alpha)$, we have

$$\begin{aligned}
R(\alpha_{-0}) &= \frac{1}{2}\log\frac{P(1-\rho_{XV}^2)(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{(1-\alpha_{-0})^2PQ(1-\rho_{XV}^2)+N_1(P+\alpha_{-0}{}^2Q+2\alpha_{-0}\sqrt{PQ}\rho_{XV})} \\
&= -\frac{1}{2}\log\{\frac{N_1}{P(1-\rho_{XV}^2)+N_1} + ff(\rho_{XV})\};
\end{aligned}$$

$$
\begin{aligned}
R_Z(\alpha_{-0}) &= \frac{1}{2}\log\Big(\frac{(P+Q+N_1+2\sqrt{PQ}\rho_{XV})}{(P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})}\cdot \\
&\quad \frac{\{(1-\alpha_{-0})^2PQ(1-\rho_{XV}^2)+(N_1+N_2)(P+{\alpha_{-0}}^2Q+2\alpha_{-0}\sqrt{PQ}\rho_{XV})\}}{\{(1-\alpha_{-0})^2PQ(1-\rho_{XV}^2)+N_1(P+{\alpha_{-0}}^2Q+2\alpha_{-0}\sqrt{PQ}\rho_{XV})\}}\Big) \\
&= \frac{1}{2}\log(1-\frac{N_2}{(P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})})(1+\frac{N_2}{gg(\rho_{XV})+N_1}),
\end{aligned}
$$

where

$$
ff(\rho_{XV})=\frac{P(1-\rho_{XV}^2)\{\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}}[P(1-\rho_{XV}^2)+N_1]+N_2(\sqrt{P}\rho_{XV}+\sqrt{Q})\}^2}{(P+Q+N_1+2\sqrt{PQ}\rho_{XV})[P(1-\rho_{XV}^2)+N_1][P(1-\rho_{XV}^2)+N_1+N_2]^2},
$$

$$
gg(\rho_{XV})=\frac{\{P(1-\rho_{XV}^2)\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}}+(N_1+N_2)(\sqrt{P}\rho_{XV}+\sqrt{Q})\}^2}{[P(1-\rho_{XV}^2)+N_1+N_2]^2+P(1-\rho_{XV}^2)\{\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}}-(\sqrt{P}\rho_{XV}+\sqrt{Q})\}^2}.
$$

First, let us consider $ff(\rho_{XV})$. Let

$$
ff_1(\rho_{XV})=\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}}[P(1-\rho_{XV}^2)+N_1]+N_2(\sqrt{P}\rho_{XV}+\sqrt{Q}).
$$

Then we have if $\sqrt{P}\rho_{XV}+\sqrt{Q}<0$,

$$
\begin{aligned}
ff_1(\rho_{XV}) &= 0 \\
-N_2(\sqrt{P}\rho_{XV}+\sqrt{Q}) &= \sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}}[P(1-\rho_{XV}^2)+N_1] \\
N_2^2(\sqrt{P}\rho_{XV}+\sqrt{Q})^2 &= (P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})[P(1-\rho_{XV}^2)+N_1]^2 \\
N_2 &= P(1-\rho_{XV}^2)+N_1+\frac{[P(1-\rho_{XV}^2)+N_1]^2}{(\sqrt{P}\rho_{XV}+\sqrt{Q})^2} \\
N_2 &= N_{high}|_{\rho_{XV}}.
\end{aligned}
$$

Suppose there is δ_2^- such that $\sqrt{P}\delta_2^-+\sqrt{Q}<0$ and $N_2=N_{high}|_{\rho_{XV}=\delta_2^-}$. By Lemma 4.4.17, $\delta_2^-\le\delta_2$ and $|\delta_2^-|\ge|\delta_2|$. Note that $ff_1(\delta_2^-)=0$ and $ff(\delta_2^-)=0$. Then for $-1\le\rho_{XV}\le\delta_2^-$, $ff(\rho_{XV})\ge ff(\delta_2^-)$. Correspondingly, we have

$$
R(\alpha_{-0})|_{\rho_{XV}}\le R(\alpha_{-0})|_{\rho_{XV}=\delta_2^-},\quad \text{for } -1\le\rho_{XV}\le\delta_2^-.
$$

In particular, since $|\delta_2^-|\ge|\delta_2|$,

$$
\begin{aligned}
R(\alpha_{-0})|_{\rho_{XV}=\delta_2^-} &= -\frac{1}{2}\log\{\frac{N_1}{P(1-{\delta_2^-}^2)+N_1}+ff(\delta_2^-)\} \\
&= \frac{1}{2}\log(1+\frac{P(1-{\delta_2^-}^2)}{N_1}) \\
&= R(\alpha_{max})|_{\rho_{XV}=\delta_2^-} \\
&\le R(\alpha_{max})|_{\rho_{XV}=\delta_2}=R(\alpha_0)|_{\rho_{XV}=\delta_2}.
\end{aligned}
$$

Now let us consider $gg(\rho_{XV})$. Let

$$
gg_1(\rho_{XV})=P(1-\rho_{XV}^2)\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}}+(N_1+N_2)(\sqrt{P}\rho_{XV}+\sqrt{Q}).
$$

Then we have if $\sqrt{P}\rho_{XV} + \sqrt{Q} < 0$,

$$\begin{aligned} gg_1(\rho_{XV}) &= 0 \\ -(N_1+N_2)(\sqrt{P}\rho_{XV}+\sqrt{Q}) &= P(1-\rho_{XV}^2)\sqrt{P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV}} \\ (N_1+N_2)^2(\sqrt{P}\rho_{XV}+\sqrt{Q})^2 &= (P+Q+N_1+N_2+2\sqrt{PQ}\rho_{XV})[P(1-\rho_{XV}^2)]^2 \\ N_2 &= P(1-\rho_{XV}^2) - N_1 + \frac{[P(1-\rho_{XV}^2)]^2}{(\sqrt{P}\rho_{XV}+\sqrt{Q})^2} \\ N_2 &= N_{low}|_{\rho_{XV}}. \end{aligned}$$

Suppose there is δ_1^- such that $\sqrt{P}\delta_1^- + \sqrt{Q} < 0$ and $N_2 = N_{low}|_{\rho_{XV}=\delta_1^-}$. By Lemma 4.4.16, $\delta_1^- \le \delta_1$. Note that $gg_1(\delta_1^-) = 0$ and $gg(\delta_1^-) = 0$. Then for $-1 \le \rho_{XV} \le \delta_1^-$, $gg(\rho_{XV}) \ge gg(\delta_1^-)$. Correspondingly, we have

$$R_Z(\alpha_{-0})|_{\rho_{XV}} \le R_Z(\alpha_{-0})|_{\rho_{XV}=\delta_1^-}, \quad \text{for } -1 \le \rho_{XV} \le \delta_1^-.$$

In particular, since $\delta_1^- \le \delta_1$,

$$\begin{aligned} R_Z(\alpha_{-0})|_{\rho_{XV}=\delta_1^-} &= \frac{1}{2}\log(1 - \frac{N_2}{(P+Q+N_1+N_2+2\sqrt{PQ}\delta_1^-)})(1+\frac{N_2}{gg(\delta_1^-)+N_1}) \\ &= R_Z(1)|_{\rho_{XV}=\delta_1^-} \\ &\le R_Z(1)|_{\rho_{XV}=\delta_1} = R(\alpha_0)|_{\rho_{XV}=\delta_1}. \end{aligned}$$

Note that from (4.59) we have $R(\alpha_{-0}) = R_Z(\alpha_{-0})$. As we have discussed above, we can draw such a conclusion that

$$R(\alpha_{-0})|_{\rho_{XV}} \le R(\alpha_{-0})|_{\rho_{XV}=\delta_2^-} \le R(\alpha_0)|_{\rho_{XV}=\delta_2}, \qquad \text{for } -1 \le \rho_{XV} \le \delta_2^- < -\frac{\sqrt{Q}}{\sqrt{P}};$$

$$R(\alpha_{-0})|_{\rho_{XV}} \le R(\alpha_{-0})|_{\rho_{XV}=\delta_1^-} \le R(\alpha_0)|_{\rho_{XV}=\delta_1}, \qquad \text{for } -1 \le \rho_{XV} \le \delta_1^- < -\frac{\sqrt{Q}}{\sqrt{P}}.$$

■

List of Tables

List of Figures

List of Symbols

Symbol	Description
X	random variable
x	sample value
$\mathbf{x}, x^N$	sample vector
$\mathbf{X}, X^N$	random vector
$\mathcal{X}$	range of X
$\|\mathcal{X}\|$	cardinality of $\mathcal{X}$
R	transmission rate
Δ, d	equivocation
P_e	error probability
C	channel capacity
C_M	capacity of the main channel
C_{MW}	capacity of the overall wiretap channel
C_s	secrecy capacity
R_s	secret rate
$\mathcal{R}$	rate equivocation region
K	covariance matrix
ρ_{XV}	correlation coefficient of X and V
H	matrix
I	identity matrix
H^{T}	transpose of the matrix H
$< \cdot >_{\mathrm{H}}$	average over all possible matrices H
$\mathrm{E}(\cdot)$	expectation operator
$\lfloor x \rfloor$	the maximal integer which is not larger than x
$h(\cdot)$	binary entropy function
$w(\cdot)$	Hamming weight function
$\mathbf{1}(\cdot)$	truth function
$H(X)$	entropy of X
$H(X,Y)$	joint entropy of X and Y

$H(Y\|X)$	entropy of Y conditional on X
$I(X;Y)$	mutual information of X and Y
$T_X^N(\epsilon)$	typical set of ϵ-typical sequences with respect to $p_X(x)$
$X \sim \mathcal{N}(0, \sigma_X^2)$	X has normal distribution with mean zero and variance σ_X^2

Biography

Yanling Chen was born in Henan, China, on October 14, 1979. She received the B.S. degree in 2001 and the M.S. degree in 2004, both in applied mathematics from Nankai University, Tianjin, China. In 2004, she joined the Digital Communication group in the Institute for Experimental Mathematics, University of Duisburg-Essen, Essen, Germany. There she, under the supervision of Prof. A. J. Han Vinck, worked on her Ph.D. thesis which she successfully finished in 2007.

Her research interests include information theory, coding theory and cryptography. A list of her publications is as follows.

1. Yanling Chen and A.J. Han Vinck, "Wiretap channel with side information," to appear in *IEEE Trans. Info. Theory*, January 2008.

2. Yanling Chen and A.J. Han Vinck, "An achievable region of Gaussian wiretap channel with side information," *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, June 24-29, 2007.

3. Yanling Chen and A.J. Han Vinck, "Wiretap channel with side information," *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, Washington, July 9-14, 2006.

4. Yanling Chen and A.J. Han Vinck, "Notes on refined Fibonacci codes," *Proc. Winter school on Coding and Information Theory*, Bratislava, Slovakia, February 20-25, 2005.

5. Yanling Chen, Lusheng Chen and Fangwei Fu, "Cryptanalysis of two group signature schemes," *Journal of Electronics and Information Technology*, vol.27, no.2, pp. 235-238, 2005.

6. Qingpo Zhang, Caiyun Chen, Lusheng Chen and Yanling Chen, "ElGamal cryptosystem and digital signature scheme based on polynomials over finite fields," *Journal on Communications*, vol.26, no.5, pp. 69-72, 2005.