Security for Correlated Sources across Wiretap Network

Author: Reevana Balmahoon

Supervisor: Dr Ling Cheng

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

in the

School of Electrical and Information Engineering
Faculty of Engineering
University of the Witwatersrand

July 2015

Declaration of Authorship

I, Reevana Balmahoon, declare that this thesis titled, 'Security for Correlated Sources across Wiretap Network' and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where I have consulted the published work of others, this is always clearly attributed.
- I have acknowledged all main sources of help.

Signed: ____

Date: ____

Abstract

This thesis presents research conducted for the security aspects of correlated sources across a wiretap network. Correlated sources are present in communication systems where protocols ensure that there is some predetermined information for sources to transmit. Systems that contain correlated sources are for example broadcast channels, smart grid systems, wireless sensor networks and social media networks. In these systems there exist common information between the nodes in a network, which gives rise to security risks as common information can be determined about more than one source. In this work the security aspects of correlated sources are investigated. Correlated source coding in terms of the Slepian-Wolf theorem is investigated to determine the amount of information leakage for various correlated source models. The perfect secrecy approach developed by Shannon has also been incorporated as a security approach. In order to explore these security aspects the techniques employed range from typical sequences used to prove Slepian-Wolf's theorem to coding methods incorporating matrix partitions for correlated sources.

A generalized correlated source model is presented and the procedure to determine the information leakage is initially illustrated using this model. A novel scenario for two correlated sources across a channel with eavesdroppers is also investigated. It is a basic model catering for the correlated source applications that have been detailed. The information leakage quantification is provided, where bounds specify the quantity of information leaked for various cases of eavesdropped channel information. The required transmission rates for perfect secrecy when some channel information has been wiretapped is further determined, followed by a method to reduce the key length required for perfect secrecy. The implementation thereafter provided shows how the information leakage is determined practically. In the same way using the information leakage quantification, Shannon's cipher system approach and practical implementation a novel two correlated source model where channel information and some source data symbols (predetermined information) are wiretapped is investigated. The adversary in this situation has access to more information than if a link is wiretapped only and can thus determine more about a particular source. This scenario caters for an application where the eavesdropper has access to some predetermined information. The security aspects and coding implementation have further been developed for a novel correlated source model with a heterogeneous encoding method. The model caters for situations where a wiretapper is able to easily access a particular source.

The interesting link between information theory and coding theory is explored for the novel models presented in this research. A matrix partition method is utilized and the information leakage for various cases of wiretapped syndromes are presented.

The research explores the security for correlated sources in the presence of wiretappers. Both the information leakage and Shannon's cipher system approach are used to achieve these security aspects. The implementation shows the practicality of using these security aspects in communications systems. The research contained herein is significant as evident from the various applications it may be used for and to the author's knowledge is novel.

Acknowledgements

A huge thank you to my supervisor, Prof Ling Cheng, without whom this research would not have been possible. Your support and guidance during the duration of this project has been immeasurable. Words cannot describe the profound impact your research style and professionalism has had on me. This research project was indeed an enjoyable one, thanks to you.

My parents Shireena and Vishunduth Balmahoon, thank you for your blessings for me to undertake this degree and for your moral support and unconditional understanding. Thank you to my sister, Tarika Balmahoon for your support and laughter throughout this project. I am grateful for the immense amount of support you all have provided even though we were physically apart.

Thanks to my colleagues and friends at the CeTAS research group for the assistance, moral support and memorable moments during this research.

Thank you to Telkom SA Ltd for the financial support during this research project. The financial assistance of CeTAS and the National Research Foundation (DAAD-NRF) towards this research is hereby acknowledged.

Contents

Declaration of Authorship **i**

Abstract **ii**

Acknowledgements **iv**

Contents **v**

List of Figures **vii**

1 Introduction **1**
1.1 Objective of Research 5
1.2 Outline of Thesis 6
1.3 List of Publications 7

2 Background **9**
2.1 Correlated Sources 11
2.1.1 Correlated Source Compression 11
2.1.2 Side Information and Multiple Correlated Sources 12
2.1.3 Feedback Applications 12
2.1.4 Security and Other Applications 13
2.2 Shannon's Cipher System and Wiretap Channels 15
2.2.1 Shannon's Cipher System 15
2.2.2 Wiretap Channels and Wiretap Channel II 16
2.3 Coding and Security Aspects for Correlated Sources 18
2.3.1 Matrix Partitions 19
2.3.2 Coding for Wiretap Channels 19

3 Techniques **21**
3.1 Shannon's Information Measures 22
3.1.1 *I*-Measure 23
3.1.2 Markov Model 24
3.2 Correlated Source Coding 25
3.2.1 Typical Sequences 26
3.2.2 Slepian-Wolf Coding 29
3.2.3 Shannon's Cipher System 34

3.3 Wiretap Networks 35

3.3.1 Ozarow and Wyner's Method 37

3.3.2 Generalized Hamming Weight 38

3.4 Coding Techniques for Correlated Sources 40

4 Information Leakage for Multiple Correlated Sources using Slepian-Wolf Coding 46

4.1 A Generalized Model for Multiple Correlated Sources 47

4.2 Two Correlated Source Model 49

4.3 Shannon's Cipher System Approach For Multiple Correlated Sources . . . 63

4.4 Shannon's Cipher System Approach for Two Correlated Sources 67

4.5 Information Leakage for the System using Matrix Partitions 72

5 Information Leakage of Slepian-Wolf Encoded Sequences for Two Correlated Sources with Partially Predetermined Information 79

5.1 Two Correlated Source Model with Partially Predetermined Information . 80

5.2 Shannon Cipher System Approach for Two Correlated Sources with Partially Predetermined Information 88

5.3 Information Leakage for the System using Matrix Partitions 94

6 Information Leakage for Correlated Sources using Heterogeneous Encoding Method 97

6.1 Correlated Source Model for Heterogeneous Encoding Method 97

6.2 Shannon Cipher Approach for Correlated Sources using Heterogeneous Encoding Method 106

6.3 Information Leakage for the System using Matrix Partitions 111

7 Conclusion 114

7.1 Comparison to other Models 114

7.2 Future Work 116

7.3 Contributions 116

A Proof of Theorems 2-3 118

A.1 Direct parts 121

A.2 Converse parts 131

B Proof of Theorems 4-5 135

B.1 Direct parts 135

B.2 Converse parts 146

C Proof of Theorems 6-7 150

C.1 Direct parts 150

C.2 Converse parts 161

Bibliography 166

List of Figures

2.1 Diagram showing general point-to-point communication system [1] 10

2.2 Feedback source network with one encoder [2] 13

2.3 Feedback source network with two encoders [2] 13

2.4 Yamamoto's development of the Shannon Cipher System 15

2.5 Vinck's [3] equivalent wiretap model 19

3.1 Venn diagram illustrating Shannon's information measures 23

3.2 Markov model for X,Y and Z 25

3.3 Correlated data streams 26

3.4 Diagram showing rate allocation for correlated sources X and Y 30

3.5 Slepian-Wolf encoding: the jointly typical pairs are described by the product bins [4] 31

3.6 Diagram showing achievable region for the Slepian-Wolf theorem [2] . . . 34

3.7 Shannon cipher system [5] 35

3.8 Wiretap Channel II concept [6] 36

3.9 Diagram showing the set-up of the Wire-tap Channel II 37

3.10 General representation of Ozarow's method 38

3.11 Security curve as developed by Wei [7] 39

4.1 Extended generalized model 47

4.2 Correlated source coding for two sources 50

4.3 The relation between private and common information 50

4.4 Shannon cipher system for two correlated sources 68

4.5 Wiretapped parity bits for maximum and minimum information leakage . 76

4.6 The information leakage on (X^K, Y^K) when (T_X, T_Y) has been wiretapped 77

4.7 The information leakage on (X^K, Y^K) when T_X or T_Y has been wiretapped 78

5.1 Correlated source coding for two sources with a more powerful adversary . 80

5.2 Shannon cipher system for two correlated sources with wiretapped source symbols 89

5.3 The information leakage on X^K when Y^{K_2} has been wiretapped 95

5.4 The information leakage on Y^K when Y^{K_2} has been wiretapped 96

5.5 The information leakage on (X^K, Y^K) when Y^{K_2} has been wiretapped . . 96

6.1 Correlated source coding for three sources with X and Y transmitting compressed information 98

6.2 The relation between private and common information 98

6.3 Shannon cipher system for three correlated sources 107

6.4 The information leakage on (X^K, Y^K) when Z^μ has been wiretapped . . . 113

Chapter 1

Introduction

The introduction addresses the field of security in communication networks, gives an overview of the objective of the thesis, includes an outline of the thesis and provides a list of publications for this research project. The field of research is broadly introduced here to provide a holistic view of the importance and significance of this research as there are many applications for which it can be used. The thesis objectives cover the aim of the thesis and hypothesis, and the thesis outline describes the chapters that lie ahead. The list of publications lists the papers published, submitted and that are to be submitted for this research project, which also provides an indication that this research is indeed significant.

This document is a PhD thesis for research in the field of telecommunications. The research focuses on the security aspects of correlated sources across a wiretap network. The field is largely information theory based, however in the latter part of this work there is an interesting link highlighted between information theory and coding theory. The problem statement, concepts, methodologies and solutions that the research has focused on is provided herein.

Practical communication systems make use of correlated sources. The communication nodes adhere to certain protocols and this means that certain information (e.g. date, area, etc.) in the header files will be the same for various nodes. From the receiver's (or an eavesdropper's) perspective, it appears as common information shared between the nodes. This is therefore pre-existing or known information for an eavesdropper. Thus, correlated sources are common in systems transmitting information, e.g. smart grid meter systems, wireless sensor networks and broadcast channels. This implies that the theory used for correlated sources may also be applied to this type of system. These networks can use the methodologies described in this research to secure the system or to determine the information leakage.

The research focuses on two and more correlated sources that transmit information to a receiver. This system is useful for wireless architectures. In wireless networks, physical links connecting nodes to one another are not present and the transmission medium is air. These networks have a security risk as the transmitted information may easily be intercepted. Wireless networks have thus in recent decades gained much exposure. Mobility, a result of wireless communications, supports productivity in a workplace because users are able to access information wherever wireless communication is available and can thus work while moving around [8]. Working while traveling increases worker productivity [8], which is favourable for businesses. Wireless communication has applications in many systems for example mobile cellular phones, WLANs (Wireless local access networks), satellite systems and wireless ad hoc networks. Hoebekeet *et al.* [9] maintain that the cellular phone is the strongest motivator for the increase in wireless communications. WLANs host a local access network, which support high speed data transmission [10]. Satellite communication makes it possible to have voice transmission from remote areas (for example journalists reporting live from a remote war zone) [10]. In wireless ad hoc networks wireless mobile nodes self-configure and form a network without any established infrastructure [10].

Wireless technology has been chosen for the research; this well-established technology has been chosen because of the vast range of applications for which it may be used. It is noted that each of these applications mentioned may have correlated sources depending on the communication protocols. Further applications for wirelesss communications are in embedded computing applications (where embedded devices communicate in a wireless manner with one another) and emergency services (informing authorities of an emergency so the necessary aid can be dispatched). If the protocol has common information (e.g. the date, time or location in a header file) then the transmitter will receive information correlated with other nodes/sources. It is also important to note that correlation is generalized in the sense that no correlation means zero correlation, hence this research also caters for many other communication scenarios.

An interesting wireless application is smart grids. The application is mentioned to show the potential of the research topic, however the scope of the research project is not limited to this single application. It is a type of electrical grid that functions to predict and intelligently respond to the behaviour of the users connected to it [11]. It is capable of making the conventional grid work more efficiently, securely and reliably through bidirectional flows of power and communication [12]. The two-way communication may be implemented using AMR (automatic meter reading), where the smart meter is an important component. Xia and Wang [12] define a smart meter as a device that usually has a processing chip and a non-volatile storage so that it can perform smart functions; for example being able to report periodic usage updates to the end-users and the generation facilities at the power company, and interact directly with smart appliances at home to control them. The information received by the end users may have correlated information depending on where the meters are located or what time the information was sent. It could also be related to the communication protocols to which the meters adhere.

Other applications for this work are broadcast channels and social media networks. In broadcast channels there is one sender and multiple receivers, for example satellite systems. Social media networks transmit information internationally in the form of images, video, voice and text. For both these applications there may be common information transmitted via the network. With the existence of common information, the sources are thus correlated and the principles that apply to correlated sources can also apply to these systems.

Correlated sources have the ability to decrease the bandwidth required to transmit and receive messages. A syndrome (compressed form of the original message) is transmitted instead of the original message. It is also interesting that this correlated source approach has the ability to provide a more secure communication system. The research focuses on the security aspect in an eavesdropped network that makes use of correlated sources.

Correlated sources possess a security risk as common information provides information about more than one source. Correlated source coding is the method that has come about to reduce this security issue. A compressed message has more information per bit, and therefore has a higher entropy because the transmitted information is more unpredictable. The unpredictability of the compressed message is also beneficial for the information security.

One of the security aspects focused on is the amount of information leakaed to an eavesdropper. The information leakage that has been considered is not that associated with cryptography, as discussed by Sun and Rane [13] but rather that associated with information theory. The scheme incorporating information leakage by Sun and Rane [13] deals with allowing for some information to be leaked such that the receiver is able to retrieve the original message even if it has been corrupted. The leaked information (which satisfies a lower bound so that it does not compromise the system) serves the purpose of making the system more secure, and it is related to the field of cryptography. Thus, one aspect of the information leakage that this research deals with is that where certain transmitted bits are analysed to determine how much of information about the source message has been retrieved.

The other security aspect investigated is providing perfect secrecy through the use of the Shannon cipher system approach. Shannon's secrecy model is an interesting avenue for this work. Merhav [14] investigated similarly, for a model using the additional parameters of the distortion of the source reconstruction at the legitimate receiver, the bandwidth expansion factor of the coded channels, and the average transmission cost. In this research, Shannon's cipher system approach is used to indicate bounds for transmission and key rates to achieve perfect secrecy.

Considering the applications that have been put forth, these correlated sources may be prone to information leakage in the presence of an eavesdropper. In order to practically determine the amount of information that an eavesdropper has access to an analysis of the information leakage for various encoding methods is presented herein. The practical analysis makes use of coding theory techniques to show how the information leakage is quantified.

A source message is passed through an encoder before it is transmitted across a channel. There are various encoding methods that exist; for example encryption, error correction, compression, message transmission in plaintext. In this work, the encoding method that has been explored is compression and transmitting messages in plaintext. The network compression is achieved through use of the Slepian-Wolf coding method. Chapters 4 and 5 employ this encoding scheme for use in systems where an eavesdropper has access to channel information only and where the eavesdropper has access to channel information and some source data symbols (i.e. some predetermined information) respectively. Since there is a single encoding method this can be described as homogeneous. In Chapter 6, network compression and the plaintext transmission of messages are used to cater for a scenario where an eavesdropper has easy access to a source. Since there are two encoding methods used, it can be described as a heterogeneous method.

This research incorporates these encoding methods for correlated sources across wiretapped links in order to determine and minimize the information leakage for such a scenario and to provide a Shannon cipher approach for perfect secrecy. Initially, a generalized case for multiple correlated sources is considered followed by specialized cases, which employ the concept of a multiple-access channel. These are networks that consist of one receiver and two or more sources (as defined by Cover and Thomas [4]). The wiretap network is characterized when an eavesdropper is present in this multiple-access channel, with noiseless conditions.

1.1 Objective of Research

The hypothesis for this research is as follows: A generalized model for correlated sources and a wiretap network will be developed. The purpose of the generalized model is to quantify the information leakage for this communication scenario. Furthermore, a masking method will be proposed to minimize/reduce the information leakage of the proposed model. Therefore, the major contribution is to develop the generalized model for this specific communication scenario and the minor contribution is to develop a method to minimize the information leakage for the generalized model.

In this work, the novel aspect covers a generalized model for multiple correlated sources that transmit messages to a single receiver followed by three specific novel scenarios in which the information leakage is quantified. Further, the Shannon cipher approach has been presented for the specific scenarios, which explores the security aspect further. The research is indeed significant and this can be gathered from the applications for which this research may be used.

1.2 Outline of Thesis

The thesis begins with a view of the methodologies and tools used and thereafter the various models that have been developed are considered. The first chapter is an introduction that introduces the research field, topic and the thesis structure. The list of publications pertaining to this research are thereafter presented.

In Chapter 2, the background of this research project and where this research fits into the sphere of information theory and coding theory is described. Related work and examples are described to give a further understanding of the significance of the research. The literature survey is comprehensive in detailing similar work that has been done. Investigations conducted in security for correlated sources, Slepian-Wolf coding and wiretap channels have been detailed. Coding schemes that relate to the field of information theory are introduced in this chapter.

In Chapter 3, the various methodologies and techniques that have been used in this research are described. These techniques include Slepian-Wolf's theorem, typical sequences, wiretap channels, Hamming weights, Shannon's cipher system approach and a matrix partition method for coding implementation. The fundamental aspects that are used to prove the Slepain-Wolf theorem are discussed to present this important theorem. Methods used to determine the equivocation of a source are also presented here. The coding implementation aspect describes the methodology used to provide a link between the fields of information theory and coding theory.

In Chapter 4, the multiple correlated source model and a two correlated source model are developed. Here, multiple correlated sources across a wiretap network is initially described in terms of the information leakage and thereafter in terms of Shannon's cipher system where transmission rates for perfect secrecy are developed. The information leakage is quantified using traditional information theory concepts of entropy and mutual information. The two correlated source model is also analyzed in the same way. In order to show the link with coding theory an implementation to determine the equivocation is done using a matrix partition method.

In Chapter 5, the focus is on a more specific two correlated source scenario to quantify the information leakage and to provide the Shannon cipher system approach. Here, the sources are split into two partitions and certain source symbols and syndromes are wiretapped. The information leakage is quantified for this model and Shannon's cipher system used to determine the transmission rates for perfect secrecy. As with the previous chapter this chapter ends with the matrix partition implementation for the model.

In Chapter 6, the information leakage for a correlated source model with heterogeneous encoding in which an eavesdropper has easy access to one source is considered. As before the information leakage is quantified and the model is thereafter analyzed in terms of Shannon's cipher system, followed by the coding implementation.

To the best of the author's knowledge these models described in Chapter 4-6 are novel and their information leakage characterization unique.

Chapter 7 concludes the thesis. The future work for this research and a list of contributions have also been provided.

1.3 List of Publications

This section lists the publications for this research project, the submitted research papers and the papers to be submitted based on this research. The sections or chapters of the thesis that contain the content of these papers have been indicated.

The following is a list of publications for this research project:

1) R Balmahoon and L Cheng, "Bandwidth Reduction using Correlated Source Compression for Smart Grid Meters with Feedback" in Proceedings of Southern Africa Telecommunication Networks and Applications Conference, Port Elizabeth, South Africa, August 30 – September 3, 2014.

2) R Balmahoon, H Vinck and L Cheng, "Information Leakage for Correlated Sources with Compromised Source Symbols over Wiretap Channel II" in 52nd Annual Allerton Conference on Communication, Control and Computing, Monticello, USA, October 1 – October 3, 2014. (Detailed in Section 5.1)

3) R Balmahoon and L Cheng, "Information Leakage of Heterogeneous Encoded Correlated Sequences over an Eavesdropped Channel" IEEE International Symposium on

Information Theory, Hong Kong, China, 14-19 June, 2015. (Detailed in Section 6.1 and Section 6.3)

The following is a list of journal papers to be submitted for this research project:

1) R Balmahoon and L Cheng, "Information Leakage of Correlated Source Coded Sequences over a Channel with an Eavesdropper" to submit to IEEE Transactions on Information Theory. (revised version for re-submission) (Detailed in Chapter 4)

2) R Balmahoon and L Cheng, "Information Leakage for Two Correlated Sources with Partially Predetermined Information" to submit to IEEE Transactions on Information Theory. (Detailed in Chapter 5)

This chapter has introduced the research project field and identified the importance of such a project. The hypothesis and aim of the research has been provided to clarify the research project goal. The thesis has been outlined to give an indication of the arrangement of the presentation for this research project. The publications have also been listed here.

Chapter 2

Background

The literature survey or background related to the research project is presented in this chapter. Initially the significant and novel work documented by Shannon that led to the introduction of the field of information theory is detailed. This forms the basis for the information theory aspects discussed further into the thesis. The concept of correlated sources forms an important aspect as all the novel models developed in this research consist of correlated sources. One of the security aspects analyzed is the Shannon cipher system approach; related literature is detailed in this chapter. The models also contain a wiretapper, and this chapter incorporates the research conducted in wiretapped networks to compare the similarity to the models developed during this research project. The coding implementation for wiretap networks has been researched and the related work is presented here. This forms a basis for bridging the gap between coding theory and information theory.

Communication systems enable us to transmit information from a source to a receiver. Here, a general communication system that is depicted in Figure 2.1, which laid the foundation for information theory and was introduced by Shannon [15] is shown.

This model by Shannon introduced the components involved in communication when transmitting digital information (i.e. the information is transmitted as a stream of 0's and 1's) from a source to a receiver. The transmitter is responsible for converting the message into a suitable form for the particular communication architecture. Thereafter, the receiver estimates the correct message and sends the information to the destination.

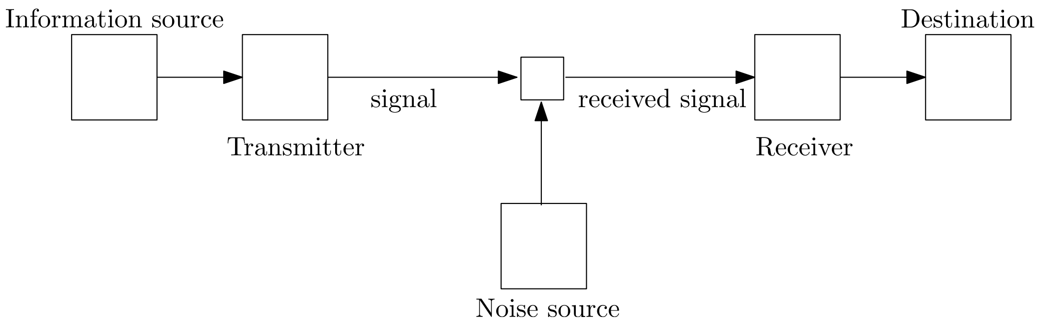

FIGURE 2.1: Diagram showing general point-to-point communication system [1]

While the information is transmitted it could encounter noise, which results in the received signal looking different to the transmitted signal.

To provide an analogy for transmitting and receiving information, an example described by Yeung [1] of a secretary sending a fax (i.e. trying to convey information from one point to another by fitting as much information as possible on a sheet of paper) is used. The page could have large fonts or smaller fonts to try to squeeze more characters on the page, however the page has a finite resolution so if the font is made too small it may not be readable by the receiver and also there may be noise through transmission resulting in incorrect characters appearing at the receiver. Even though some characters are not recognizable the receiver may still be able to determine the information on the page based on the context. This brings on the idea of finding the maximum amount of information that can fit on one page while the receiver can accurately determine the information at the receiver. The concept described here illustrates a fundamental question about communication systems.

The channel coding theorem was also presented in the work by Shannon [15], which formed the basis for correlated source coding. Here the entropy is used to characterize the minimum rate such that the source produces messages that are error free, hence the entropy has been termed by Cover and Thomas [4] as the ultimate data compression. The channel coding theorem was another result from this important paper by Shannon [15].

The important concept of uncertainty (known as the entropy) was introduced in the paper by Shannon [15] as pointed out by Yeung [1]; it shows that information is naturally random and probability distributions are used to develop the theory of information. There are various information measures that are developed from the entropy (and are explained in greater detail in Chapter 3) for two sources.

2.1 Correlated Sources

2.1.1 Correlated Source Compression

The Slepian-Wolf code has been defined by Lu *et al.* [16] as a code that uses incremental transmission of coded bits to achieve multiple coding rates. It is built on using typical set encoding and decoding, which has been described in Chapter 3. Slepian-Wolf [17], in 1973 initially described coding for correlated sources such that the Slepain-Wolf bound is achieved, which ahowed the use of Slepian-Wolf codes for correlated sources. Thereafter, there have been many applications of Slepain-Wolf codes. Two such examples are the use of streaming codes, where the Slepian-Wolf bound is met for streaming data that incorporates a random binning procedure [18] and the use of Slepian-Wolf codes for storing fingerprint biometrics [19].

In work by Prabhakaran *et al.* [20] the rate regions for Slepian-Wolf have been analyzed for a secrecy model where there is an eavesdropper present. For the models presented herein the Slepian-Wolf theorem is employed to ensure accurate reconstruction of the transmitted message at the receiver.

According to Wolf and Kurkoski [21], an important aspect of the Slepian-Wolf theorem is that the encoders can achieve better compression rates by exploiting the correlation in the transmitted data streams. The result is that Slepian-Wolf coding can achieve the same compression rate as an optimal single encoder that has all correlated data streams as inputs [21]. Thereafter, Slepian-Wolf coding has also been used in applications for security [22][16], showing that security is indeed a concern. In the research contained herein, security aspects are also explored, different to that already done as the information leakage across links is quantified and minimized. The correlated source approach contributes to information leakage as a source is able to provide common information for every other source with which it is correlated. Correlated source coding, which incorporates the Slepian-Wolf theorem is a method to alleviate this issue as compressed forms of the original messages are transmitted.

2.1.2 Side Information and Multiple Correlated Sources

Any extra information that the eavesdropper has access to can be considered as side information to assist with decoding. This side information can be viewed as a separate source and when the side information is correlated then it can be generalized to represent a correlated source. Villard *et al.* [23] have explored this side information concept further where security using side information at the receiver and eavesdropper is investigated. Side information is generally used to assist the decoder to determine the transmitted message. An earlier work involving side information was done by Yang *et al.* [2]. In Chapter 5, a specific model is introduced where there are data symbols transmitted directly to the receiver; this is considered as correlated side information.

The common side information concept is extended when there are common random keys available at the sender and the receiver. This is correlated side information available at the terminals and has been investigated by Ahlswede and Csiszar [24].

In work done by Johnson *et al.* [25] the field of side information and compressed information was investigated. Side information was thereafter looked at by Villard and Piantanida [26]: A source sends information to the receiver and an eavesdropper has access to information correlated to the source, which is used as side information. There is a second encoder that sends a compressed version of its own correlation observation of the source privately to the receiver. Here, the authors show that the use of correlation decreases the required communication rate and increases secrecy.

There has been work done by Maurer [27] that describes security aspects for common information between multiple sources. This work entails building a cryptographic system that satisfies perfect secrecy conditions with a key that has an entropy less than the message entropy.

2.1.3 Feedback Applications

To show that correlated sources exist in a range of models, it is noted that correlated sources have been implemented with feedback. Correlated sources with feedback are investigated by Yang *et al.* [2] for the case of one and two encoders, as depicted in Figure 2.2 and 2.3.

The scheme proposes a block coding algorithm for the case in Figure 2.2. It is proven that:

$$c \to H(X|Y) \tag{2.1}$$

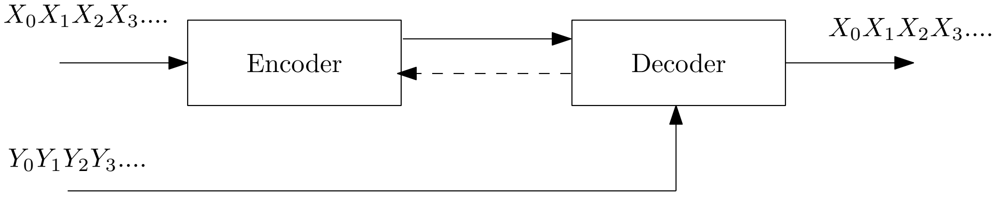

FIGURE 2.2: Feedback source network with one encoder [2]

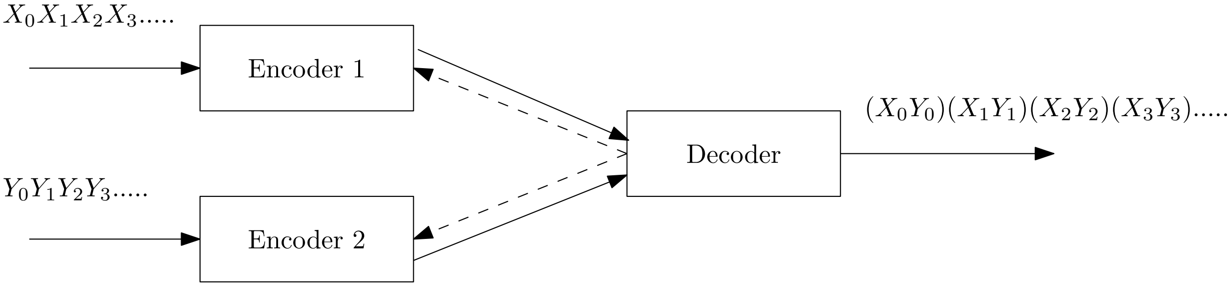

FIGURE 2.3: Feedback source network with two encoders [2]

where c is the compression rate (*i.e* the number of bits transmitted from the encoder to the decoder) and $H(X|Y)$ is the conditional entropy of the source X given Y, both of which are correlated. The authors also prove that the feedback rate approaches zero as the number of transmissions become very large. For Figure 2.3 the same analysis results are extended and the authors present a universal decoding algorithm for a feedback scenario. More recently, Yang *et al.* [2] also considered feedback and presented a model that uses typical set encoding and decoding to achieve the Slepian-Wolf bound for a feedback scenario.

2.1.4 Security and Other Applications

The use of correlated sources has various applications, for example the field of network coding (which is the use of coded data blocks during communication). Ho *et al.* [28] introduced network coding for correlated sources. Thereafter, the flow of information that incorporated multiple correlated sources was investigated by Barros and Servetto [29]. Other interesting work then dealt with the extraction of correlations between sources, such that the joint distributions may be determined [30]. A few years later, building on the extraction of correlation was work by Bogdanov and Mossel [31], where common bits are extracted without communication occurring. Thereafter some importance is placed on the work conducted by Prasad *et al.* [32] where the use of correlated sources is made for security needs. Here, the compression ability for correlated sources is exploited. This research contained herein also used the compression ability for correlated sources to provide security.

Dai *et al.* [33] point out that their correlated source approach can be used as an application in broadcast channels. Since we present fundamental research for correlated sources, it may be used with these applications as well. Research prior to Dai *et al.* [33] that incorporate Slepian-Wolf coding and broadcast channels as an application are those by Ahlswede and Korner [34] and Grokop *et al.* [35]. A network incorporating wiretappers that access noisy information can be called a wiretap channel. A detailed explanation of these channels is contained in Chapter 3. Villard and Piantanida [26] have looked at correlated sources and wiretap networks. In their work, there is a second encoder that sends a compressed version of its own correlated observation of the source privately to the receiver. Here, the authors show that the use of correlation decreases the required communication rate and increases secrecy.

Villard *et al.* [23] explore this side information concept further where security using side information at the receiver and eavesdropper is investigated. Side information is generally used to assist the decoder to determine the transmitted message. An earlier work involving side information is that by Yang *et al.* [2]. The concept can be considered to be generalised in that the side information could represent a source. It is an interesting problem when one source is more important and Hayashi and Yamamoto [36] consider it in another scheme, where only X is secure against wiretappers and Y must be transmitted to a legitimate receiver. They develop a security criterion based on the number of correct guesses of a wiretapper to retrieve a message. In an extension of the Shannon cipher system, Yamamoto [37] investigated the secret sharing communication system.

2.2 Shannon's Cipher System and Wiretap Channels

2.2.1 Shannon's Cipher System

Keeping information secure has become a major concern with the advancement in technology. This research incorporates some traditional ideas surrounding cryptography, namely Shannon's cipher system and adversarial attackers in the form of eavesdroppers. In cryptographic systems, there is usually a message in plaintext that needs to be sent to a receiver. In order to secure it, the plaintext is encrypted so as to prevent eavesdroppers from reading its contents, and is termed the ciphertext. Shannon's cipher system (mentioned by Yamamoto [5]) incorporates this idea. Apart from the Shannon cipher system, there is another well known cipher model i.e. the secret sharing communication system described by Yamamoto [38], which is an extension of Shannon's cipher system.

The definition of Shannon's cipher system has been discussed by Hanawal and Sundaresan [39]. In Yamamoto's [5] development on this model, a correlated source approach is introduced. This gives an interesting view of the problem, and is depicted in Figure 2.4. Correlated source coding incorporates the lossless compression of two or more correlated data streams. Correlated sources have the ability to decrease the bandwidth required to transmit and receive messages because a syndrome (compressed form of the original message) is sent across the communication links instead of the original message. A compressed message has more information per bit, and therefore has a higher entropy because the transmitted information is more unpredictable. The unpredictability of the compressed message is also beneficial in terms of securing the information.

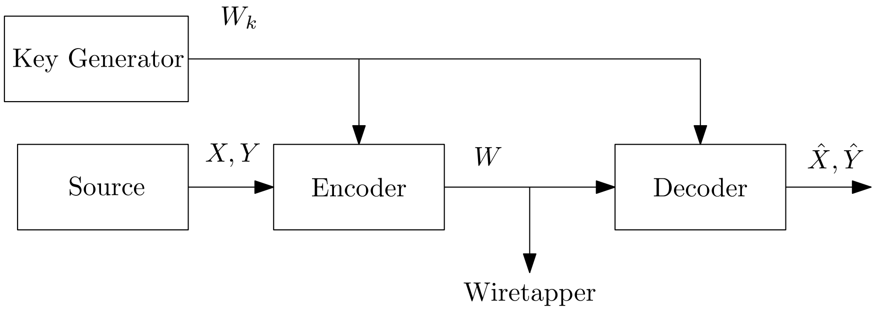

Figure 2.4: Yamamoto's development of the Shannon Cipher System

With reference to Figure 2.4, the source sends information for the correlated sources, X and Y along the main transmission channel. A key W_k, is produced and used by the encoder when producing the ciphertext. The wiretapper has access to the transmitted codeword, W. The decoded codewords are represented by $\widehat{X}$ and $\widehat{Y}$. In Yamamoto's scheme the security level was also focused on and found to be $\frac{1}{K}H(X^K, Y^K|W)$ (i.e. the joint entropy of X and Y given W, where K is the length of X and Y) when X and Y have equal importance. This is in accordance with traditional Shannon systems where the security is measured by the equivocation. When one source is more important than the other then the security level is measured by the pair of the individual uncertainties $(\frac{1}{K}H(X^K|W), \frac{1}{K}H(Y^K|W))$. An investigation into the rate distortion theory has been conducted in more recent research by Yamamoto [40]. This research project also incorporates Shannon's cipher system to determine the transmission rate for perfect secrecy for two or more correlated sources that transmit information to a receiver via separate links.

2.2.2 Wiretap Channels and Wiretap Channel II

Whether many links are considered or a single link as Yamamoto [5] had, there may be a wiretapper present that can access information across the link/s. The signals are more susceptible to eavesdropping in wireless networks compared to the traditional wired networks, as it is easier to attack the former. Other concerns in wireless communication are path loss, interference and fading. Being able to keep messages secure and user identities private thus becomes a concern. Furthermore, since eavesdropping is a major security risk in wireless networks, it is in the interest of producing a secure system to ensure that there is as less information as possible leaked to an eavesdropper. In work by Aggarwal *et al.* [41] active eavesdroppers are described. These eavesdroppers are able to erase/modify wiretapped bits. They develop a perfect secrecy model for this scenario. The eavesdropper investigated in the work contained herein is a passive wiretapper, who cannot modify information.

Since AMR (automatic meter reading) is an application of wireless networks, it has the same concerns as that mentioned for wireless networks, namely eavesdropping. A wiretap network is generally one that allows for eavesdropping across a noisy channel. Wiretap networks have been presented by Cai and Yeung [42] and incorporate network coding and information security. Bloch *et al.* [43] also develop research on wiretap networks further. They show how the wiretap network is related to the client-server architecture and thereafter implement wiretap codes on the network scenario. Wiretap networks have also been studied by Grokop *et al.* [35], where they incorporate source coding, using the Slepian-Wolf rate on a broadcast channel that is wiretapped. It has later been looked at via rank-metric codes for security [44]. Thereafter security of the wiretap channel was investigated by Cai *et al.* [42].

An interesting development for the conventional wiretap network is the Wiretap Channel II, introduced by Ozarow and Wyner [45] with a coset coding scheme. A characteristic that makes the Wiretap Channel II different from the original wiretap channel is that the former is error-free, which is why it can be incorporated into the network layer in the 7 layer ISO model. The mathematical model for this wiretap channel II has been given by Rouayheb *et al.* [6], and can be explained as follows: the channel between a transmitter and receiver is error-free and can transmit n symbols of which μ can be observed by the eavesdropper and the maximum secure rate can be shown to equal $n-\mu$ symbols. This wiretap channel can also be looked at from a Gaussian approach and a variation of this Gaussian wiretap channel has been investigated by Mitrpant *et al.* [46].

Security for the wiretap channel II has been spurred on by research by Luo *et al.* [47], where the equivocation for a wiretap channel II that leaks certain source data symbols to an eavesdropper was investigated. There has also been some work done on the Wiretap Channel II that focuses on network coding, by Cai and Yeung [42] and Rouayheb *et al.* [6]. Zhang [48] quantified the uncertainty of obtaining a source message after wiretapping certain bits on a link in a Wiretap Channel II. Secrecy in the Wiretap Channel II was looked at by Cheng *et al.* [49], where messages are encoded with some random key.

In an interesting application of the wiretap channel and wiretap channel of type II, Dai *et al.* [50] presented a model that incorporates compromised encoded bits and wiretapped bits from a noisy channel. The concept of a noiseless transmission gives rise to an ideal situation in terms of noise when analyzing the model. In chapter 5, a scenario where an eavesdropper has access to more than just the bits from the communication links is considered.

Luo *et al.* [47], in some previous work, have described this sort of adversary as more powerful because in addition to the eavesdropped bits from the communication links, the eavesdropper also has access to some data symbols from the source. In other previous work [51], the information leakage for two correlated sources when some channel information from the communication links had been wiretapped was investigated. Intuitively from this work, it is seen that there is indeed more information gained by the more powerful eavesdropper, not just in terms of the data symbols but in terms of the alternate source, which results from the fact that the sources are correlated. This concept is similar to that employed in the correlated source model developed Chapter 5. This makes it easier for the eavesdropper to determine the transmitted message and information about another correlated source. Recently, security aspects of the wiretap channel II has been researched by Rouayheb *et al.* [6], emphasizing that this area of security for the wiretap channel II has room for growth.

2.3 Coding and Security Aspects for Correlated Sources

In this research project information theory is primarily used, however the interesting relation between information theory and coding theory has also been explored. There has been work done on wiretap channels for a coding approach. The first was done by Wei [7] who presented the generalized Hamming weight to describe the minimum uncertainty that an eavesdropper has access to. This uncertainty has been termed the equivocation. The generalized Hamming weight uses the parity matrix rank to determine the equivocation when various transmitted bits are eavesdropped. An extension of this work was performed by Ngai *et al.* [52] to describe generalized Hamming weights for a network scenario. Thereafter characteristics on this channel were introduced by Luo *et al.* [47]. The characteristics focused on were those pertaining to Hamming weights and Hamming distances in order to determine the equivocation of a wiretapper. Thereafter, the security aspect of wiretap networks has been looked at in various ways by Cheng *et al.* [49], and Cai and Yeung [42], emphasizing that it is of concern to secure this type of channel.

The concern in this research in terms of coding theory is to find a link to information theory so as to quantify the information leakage across links in a practical manner. The work by Luo *et al.* [47] assists in achieving this goal.

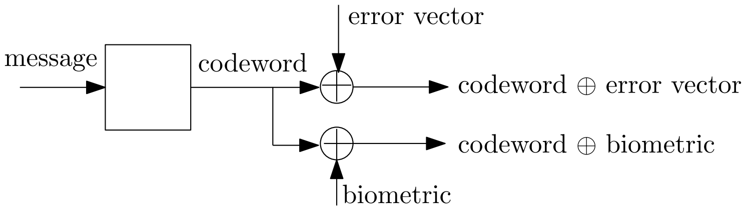

FIGURE 2.5: Vinck's [3] equivalent wiretap model

2.3.1 Matrix Partitions

The transmission of messages needs to satisfy the Slepian-Wolf bound in order for correct decoding to occur at the receiver. Slepian-Wolf coding enables the transmission of separately encoded messages and the joint decoding of them. The coset codes that have been used by Wyner (used in many applications, e.g. by Wei [7] and Luo *et al.* [47]) have been used by Pradhan and Ramachandran [53]. In this research project, the analogy for a generator matrix to represent the equivocation presented by Luo *et al.* [47] to determine the amount of leaked information is used. There have been many practical syndrome based schemes (Yang *et al.* [54], Pradhan and Ramchandran [55] and Liveris *et al.* [56]), one such example is that by Ma and Cheng [57], where partitions of the generator matrix is also employed. We use the method supplied by Stankovic *et al.* [58] in order to partition the matrices to make use of the matrix partition method, which is optimal for Slepian-Wolf coding.

2.3.2 Coding for Wiretap Channels

Wiretap networks/representations have been looked at by Ozarow and Wyner [45] where a coset coding scheme is employed with a wiretap channel of type II. There has also been work for coding along wiretap channels in other instances, for example by Vinck [3]. Here, the connection between biometrics, information theory and coding techniques is explored. A wiretap representation is used to consider two new situations for the wiretap channel.

In Figure 2.5, the message is a random vector satisfying a fixed length that is generated at enrollment, to construct the codeword. The fingerprint biometric study has also been done by Draper *et al.* [19] where Slepian-Wolf codes are incorporated, which relates very closely to Vinck's [3]. A similar link between information theory and coding theory has been provided by Luo *et al.* [47], which is also explored in this research.

This chapter gives a background of the field that has been researched. The novel work documented by Shannon starts the chapter and thereafter the concept of correlated sources, Shannon's cipher system and wiretapped networks are broadly focused on. These are important aspects of this research project as the models developed incorporate correlated sources and wiretappers, and one security aspect focused on is the Shannon's cipher system. The implementation based on coding techniques and the related research have also been mentioned as it forms an aspect of this research project.

Chapter 3

Techniques

This chapter includes a description of the methodologies and techniques used for the research project. The technical aspects of these techniques are contained here to show how the models in the chapters that follow have been developed and analyzed. The various techniques are also required to quantify the information leakage and incorporate the Shannon cipher approach for the models. Techniques such as the Slepian-Wolf theorem that describes transmission rates for correlated sources and typical set encoding and decoding, which is used to prove the Slepian-Wolf theorem and gives a method to encode and decode messages using very small typical subsets are among the necessary techniques for this work. Wiretap networks and the associated method used to analyze the wiretapped links are thereafter included. The coding approaches used that make use of generalized Hamming weights and a matrix partition method are described towards the end of the chapter, as these techniques are used to form the link between information theory and coding theory. These techniques and various others are described in this chapter.

For the alphabets $\mathcal{X}$ and $\mathcal{Y}$ we define the discrete random variables X and Y having length k each, where the symbols that belong to $\mathcal{X}$ and $\mathcal{Y}$ are represented by x and y respectively. The probability distribution is given by $p(x)$ for X and $p(y)$ for Y. For a collective set of these random variables, we can represent them as $X_1, X_2, \ldots, X_k$, having probability distributions $p(x_1, x_2, \ldots, x_k)$, and $Y_1, Y_2, \ldots, Y_k$, having probability distributions $p(y_1, y_2, \ldots, y_k)$.

3.1 Shannon's Information Measures

As mentioned in Chapter 2, the concept of entropy was introduced by Shannon [15]. Here, an explanation of the various Shannon information measures developed as a result of Shannon's work are provided.

Entropy: For a random variable X, the entropy is defined as

$$H(X) = -\sum_{x} p(x) \log p(x) \tag{3.1}$$

where $p(x)$ is the probability distribution of X.

The base of the logarithm can be chosen to be any convenient real number greater than one [1]. The entropy represents the level of uncertainty in a message as it is a function of the probability distribution of X, which is the average amount of uncertainty removed when the outcome of X is revealed [1].

For pairs of random variables, there are information measures in terms of the joint and conditional entropies.

Joint entropy: For a pair of random variables X and Y, the joint entropy is defined as

$$H(X,Y) = -\sum_{x,y} p(x,y) \log p(x,y) \tag{3.2}$$

where $p(x,y)$ is the joint probability distribution of X and Y.

Similarly, using the conditional probability distribution for two random variables X and Y, i.e. $p(x,y)$ the conditional entropy definition follows.

Conditional entropy: For a pair of random variables X and Y, the conditional entropy is defined as

$$H(X|Y) = -\sum_{x,y} p(x,y) \log p(x|y) \tag{3.3}$$

An important relation between these information measures can be considered as follows: $H(X,Y) = H(Y) + H(X|Y)$ or $H(X,Y) = H(X) + H(Y|X)$.

The mutual information between sources is also of interest in determining the dependence of sources and has been described in fundamental information theory literature [1][4].

Mutual information: For a pair of random variables X and Y, the mutual information between X and Y is defined as

$$I(X;Y) = \sum_{x,y} p(x,y) \log \frac{p(x|y)}{p(x)p(y)} \tag{3.4}$$

The relations between the joint entropies, conditional entropies and mutual information is given as follows: $I(X;Y) = H(X) + H(Y) - H(X,Y)$. Yeung [1] showed that all these Shannon information measures are special cases of the conditional mutual information. The Venn diagram in Figure 3.1 shows the visual representation of these information measures.

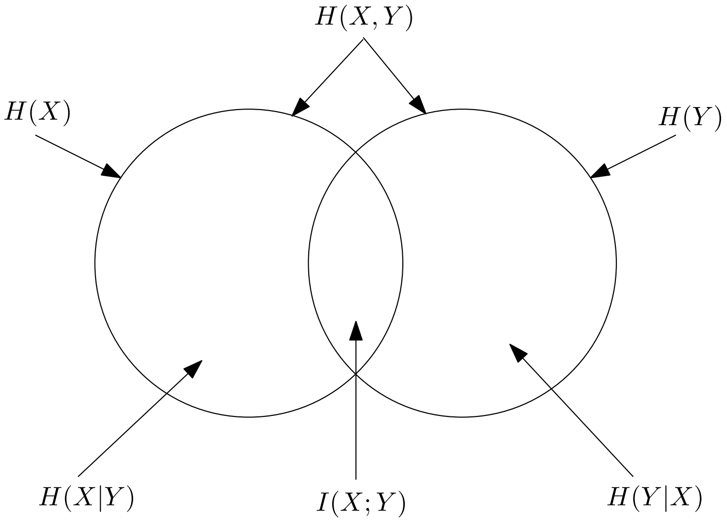

FIGURE 3.1: Venn diagram illustrating Shannon's information measures

After Shannon's work, there has been research to find the transmission rates for various other models. These techniques mentioned below and the information leakage bounds result from the Slepian-Wolf coding scenario, which is a method of coding that utilizes two compressed correlated sources.

3.1.1 *I*-Measure

The I-measure has been developed to assist in establishing a one-to-one correspondence between Shannon's information measures and set theory in full generality [1]. This allows for set operations to be used with certain forms of Shannon information measures, which brings in some more diversity to the operations used in information theory.

Let X_1 and X_2 be random variables and $\tilde{X_1}$ and $\tilde{X_2}$ be sets corresponding to X_1 and X_2, respectively. An information diagram is used to represent these sets, which is actually a conventional Venn diagram. The universal set, which is the union of $\tilde{X_1}$ and $\tilde{X_2}$, does not need to be shown explicitly just as in a usual Venn diagram [1]. Writing $A \cap B^c$ (i.e. the complement of B) as $A - B$, Yeung [1] has defined a signed measure μ^* (the I-measure) by

$$\begin{aligned} \mu^*(\tilde{X_1} - \tilde{X_2}) &= H(X_1|X_2) \\ \mu^*(\tilde{X_2} - \tilde{X_1}) &= H(X_2|X_1) \\ \text{and } \mu^*(\tilde{X_1} \cap \tilde{X_2}) &= I(X_1; X_2) \end{aligned} \tag{3.5}$$

The entropies of X and Y are given by $\mu^*(\tilde{X_1}) = H(X_1)$ and $\mu^*(\tilde{X_2}) = H(X_2)$ respectively.

The remaining set can be obtained via set-additivity, in order to achieve the Shannon information measure of $H(X,Y)$. This is done as follows:

$$\begin{aligned} & \mu^*(\tilde{X_1} \cup \tilde{X_2}) \\ = \;& \mu^*(\tilde{X_1} - \tilde{X_2}) + \mu^*(\tilde{X_2} - \tilde{X_1}) + \mu^*(\tilde{X_1} \cap \tilde{X_2}) \\ = \;& H(X_1|X_2) + H(X_2|X_1) + I(X_1; X_2) \\ = \;& H(X_1, X_2) \end{aligned} \tag{3.6}$$

Hence, all Shannon information measures for this scenario for 2 sources can be represented by the I-measure. Upon realizing this I-measure the set operations may be used in information theory.

3.1.2 Markov Model

The properties and concepts from Section 3.2 onward deal with i.i.d processes, however when the processes are dependent then the Markov model concept may be used. More specifically the Markov model focuses on processes that are stochastic where the random variables only depend on the variable preceding it and is conditionally independent of all the other preceding random variables [4].

Markov Chain: A markov chain is one where, for the stochastic processes $X_1, X_2, \ldots, X_n$ for $n = 1, 2, \ldots,$:

$$\begin{aligned} & \Pr(X_{n+1} = x_{n+1} | X_n = x_n, X_{n-1} = x_{n-1}, \ldots, X_1 = x_1) \\ = \ & \Pr(X_{n+1} = x_{n+1} | X_n = x_n) \end{aligned} \tag{3.7}$$

for all $x_1, x_2, \ldots, x_n, x_{n+1} \in \mathcal{X}$.

This means that if $X \rightarrow Y \rightarrow Z$ form a Markov chain (as depicted in Figure 3.2) then X and Y are dependent, and so are Y and Z, but there is no dependence between X and Z.

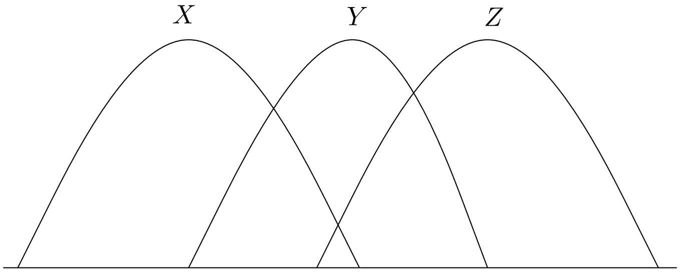

FIGURE 3.2: Markov model for X,Y and Z

This technique is used to prove certain information theory relations: e.g. the data processing theorem, the relation $I(X;Y;Z) \geq I(X;Y)$ [1] and Markov fields [4].

3.2 Correlated Source Coding

The messages from correlated sources have some similarity (measure of correlation) between them. Correlated source coding incorporates the lossless compression of two or more correlated data streams. Each of the correlated streams is encoded separately and the compressed data from each of the encoders are jointly decoded by a single decoder as shown in Figure 3.3, for two correlated streams. The work described in this research project incorporates multiple correlated sources, however two sources are illustrated here to show the concept. This idea of transmitting compressed information came about as a result of the threat posed by correlated sources. Correlated sources are a security risk when the correlated bits are known as an eavesdropper is able to gain additional information about the source. The correlated bits that have not been transmitted become additional information that the eavesdropper has access to. Hence, the need for correlated source coding.

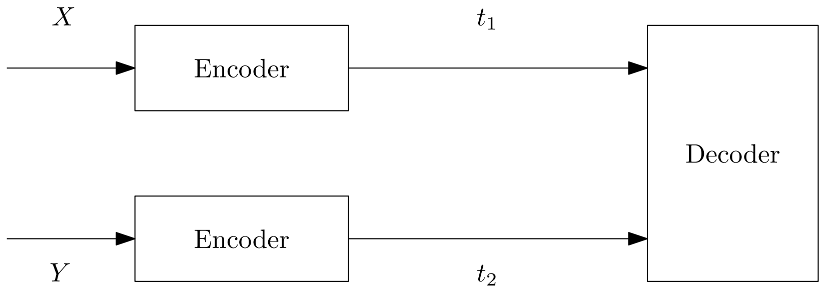

FIGURE 3.3: Correlated data streams

Here, X and Y are the correlated sources and t_1 and t_2 are the syndromes (compressed form of the original message) transmitted by X and Y respectively. The correlation is an advantage because less information needs to be transmitted across the channel (i.e. t_1 and t_2 are shorter in length than the messages at X and Y respectively), as it is not necessary to transmit the correlated information. Correlated sources thus have the ability to decrease the bandwidth required to transmit and receive messages because a syndrome is sent across the communication links instead of the original message. As mentioned in Chapter 1, the compressed message has more information per bit and therefore has a higher entropy. This is because the transmitted information is more unpredictable as there is no redundancy in this case. The unpredictability of the compressed message is also beneficial in terms of securing the information.

In order to encode correlated sources symbols, we need to ensure that the transmission rates satisfy certain transmission bounds. This is done through the use of Slepian-Wolf coding. In order to understand the Slepian-Wolf theorem the asymptotic equipartition property through the concept of typical sequences needs to be described as the Slepian-Wolf theorem uses it as a fundamental building block.

3.2.1 Typical Sequences

An ϵ-typical set of X, $A_\epsilon^{(n)}(X)$ is a small subset of the set $\mathcal{X}$ having certain properties that will be described in this section. It is seen that the size of the typical set when compared to the entire set approaches zero for large n [1]. The typical sequence is important because even though it is insignificant in terms of size when compared to the entire set it contains almost all the probability.

Typical sequences can either be strongly typical (difference between frequency of possible outcomes and corresponding probability is very small) or weakly typical (difference between empirical entropy and true entropy is very small). Strong typicality can be used for proving memoryless theorems, shown by Yeung [1] and is built on from the strong AEP (asymptotic equipartition property). The limitation for strong typicality is that it can only be used for random variables with finite alphabets, however there has been recent work on making strong typicality work for instances of infinite alphabets [59]. When a sequence or set is strongly typical then it implies weak typicality [1]. Weak typicality is commonly used in relation to the source coding theorem and is related to the Shannon-McMillan-Breiman Theorem by Yeung [1]. The weak AEP is used to interpret weakly typical sequences.

The weak AEP law specifies that the probability for a symbol x as it approaches $H(X)$ when n is large. This law is an application of the weak law of large numbers.

Weak AEP Law:

$$Pr\{|-\frac{1}{n}\log p(x) - H(X)| \leq \epsilon\} > 1 - \epsilon \tag{3.8}$$

The quantity $-\frac{1}{n}\log p(x)$ is the empirical entropy of X, which is close to the true entropy for a weakly typical sequence. If a sequence $X = \{x_1, x_2, \ldots x_n\}$ is drawn the weak AEP specifies that the probability of the sequence drawn is $2^{-nH(X)}$ with a high probability, i.e. a weakly typical sequence has probability $2^{-nH(X)}$. For large n we can therefore imagine x as been obtained directly from the weakly typical set.

Here, we use weakly typical sequences that are jointly typical. The concept of jointly typical sequences extends from the joint AEP (proved by Cover and Thomas [4]). For joint AEP we consider two variables $(X^n, Y^n) \in \mathcal{X}$ and $\mathcal{Y}$ respectively, having probabilities $(p(x), p(y))$. The following properties exist:

- The probability that (X^n, Y^n) belong to the a typical set approaches one as n becomes large

- The size of the typicality set is $2^{n(H(X,Y)+\epsilon)}$
- If there exists two independent variables (X', Y') that have the same probability distribution as $(p(x), p(y))$, then the probability that (X', Y') are part of the typical set is upper bounded by $2^{n(I(X;Y)-3\epsilon)}$.

The first property is proven using the weak law of large numbers. For the second property the probability is summed over the entire typical set, which has a probability of $2^{-n(H(X,Y)+\epsilon)}$ by definition, resulting in a size of $2^{n(H(X,Y)+\epsilon)}$. The third property results from the fact that the probability distributions $(p(x), p(y))$ summed over the typical sequence is upper bounded by $2^{\text{-}nH(X)}$ and $2^{\text{-}nH(Y)}$ subtracted from $2^{\text{-}nH(X,Y)}$. Using the Shannon's information theoretic relation here, $H(X,Y) - H(X) - H(Y) = I(X;Y)$ and collection of the ϵ, we obtain the result for the third property.

It is seen that in the jointly typical set there are $2^{nH(X)}$ and $2^{nH(Y)}$ typical sequences for X and Y respectively. However as pointed out by Cover and Thomas [4] there are only $2^{nH(X,Y)}$ jointly typical sequences so not all pairs of typical X^n and typical Y^n are also jointly typical; in fact there is a probability of $2^{-nI(X;Y)}$ that any randomly chosen pair is jointly typical.

For typical sequences, there are three important properties:

- the probability that a typical sequence belongs to the typical set approaches one when n is large
- the probability distribution for a typical sequence is given by $2^{n(H(S)\pm\epsilon)}$
- the size of the typical sequence is $2^{n(H(S)\pm 2\epsilon)}$

Here the set of S, $A_\epsilon^{(n)}(S)$, which is a small subset of the set $\mathcal{S}$ is used. The first property is a result of the law of large numbers. The second property follows from the definition of a typical sequence, as we know the following:

$$-\frac{1}{n}\log p(s) < H(S) - \epsilon \tag{3.9}$$

The third property follows from this second property where the probability distribution is summed over all $s \in A_\epsilon^{(n)}$, which has a result of 1. When we assume n is sufficiently large we are able to use the probability distribution $2^{-n(H(S)-\epsilon)}$ for the probability of $1-\epsilon$, thus providing both bounds.

For jointly typical sequences, there exists a set that is jointly typical to variables in $\mathcal{X}$, denoted by $A_\epsilon^{(n)}(S)$ where $S = (X_1, X_2)$. The joint probability distribution for (x_1, x_2) can be approximated by $H(X_1, X_2)$ when n is very large. Thus, the following property for the conditional probability distribution for jointly typical sequences is developed:

$$p(s_1|s_2) = 2^{n(H(S_1|S_2)\pm 2\epsilon)} \tag{3.10}$$

for $(S_1, S_2) \in \{X_1, X_2, \ldots, X_k\}$ where $(s_1, s_2) \in A_\epsilon^{(n)}(S_1, S_2)$. To prove this property the following relation is used:

$$p(s_2|s_1) = \frac{p(s_1, s_2)}{p(s1)} \tag{3.11}$$

where $p(s_1, s_2) = 2^{-n(H(S_1,S_2)\pm\epsilon)}$ and $p(s_1) = 2^{-n(H(S_1)\pm\epsilon)}$. Substituting these into equation (3.11) and using the relation $H(S_1, S_2) - H(S_1) = H(S_2|S_1)$ we obtain the desired result as shown in (3.10).

Just as joint typicality can be defined for typical sequences, so can conditional typicality. This concept is not used for this work, however descriptions of such sequences can be found in Cover and Thomas [4].

3.2.2 Slepian-Wolf Coding

The Slepian-Wolf theorem gives a bound on the minimum number of bits per character required for the encoded message streams in order to ensure accurate reconstruction (with an arbitrarily small error probability) at the decoder. The system efficiency is measured by the rates that the encoder outputs the encoded bits per character. Slepian and Wolf [17] produced the following result:

Slepian-Wolf Theorem: For two correlated sources X and Y transmitting messages to a destination node T (depicted in Figure 3.4), the transmission rates (R_X, R_Y) satisfy the following inequalities:

$$\begin{aligned} R_X &\geq H(X|Y) \\ R_Y &\geq H(Y|X) \\ R_X + R_Y &\geq H(X,Y) \end{aligned} \tag{3.12}$$

where R_X and R_Y represent the rate allocation for the correlated sources X and Y respectively. This means that X and Y need to have a rate allocation of $H(X,Y)$ to ensure that the received messages can be decoded correctly.

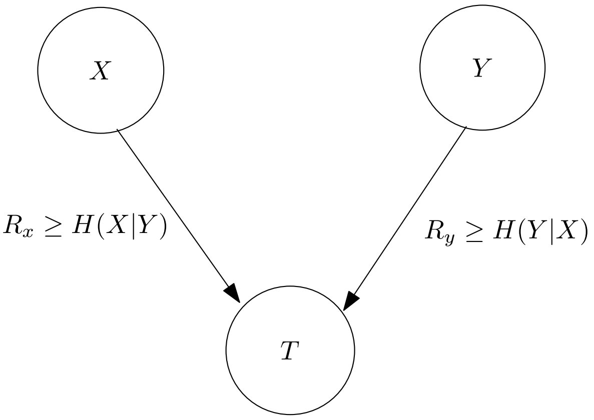

FIGURE 3.4: Diagram showing rate allocation for correlated sources X and Y

The Slepian-Wolf theorem is described using the concept of typical sequences and binning. Here, $\mathcal{X}$ is partitioned into 2^{nR_1} bins and $\mathcal{Y}$ is partitioned into 2^{nR_2} bins. The idea of random bins is that we choose a large random index for each source sequence and since the typical sequence is small, there is a different index for different source sequences with high probability. The code is generated by assigning all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ into one of 2^{nR_1} bins for X and 2^{nR_2} bins for Y. For X and Y the assignment to bins is independent according to the uniform distribution on $\{1, 2, \ldots, 2^{nR_1}\}$ and $\{1, 2, \ldots, 2^{nR_2}\}$ respectively.

The encoding and decoding is done as follows:
Encoding: For X, the index of the bin where X belongs is transmitted. For Y, the index of the bin where Y belongs is transmitted.
Decoding: There are one of two options. Firstly, if there is only one typical sequence

belonging to the bin then declare the typical sequence to be the result of X and Y, i.e. if there is only one pair (x, y) such that $f_1(x) = i_0$, $f_2(y) = j_0$ and $(x, y) \in A_\epsilon^{(n)}$. Here, f_1 and f_2 are the assignments to the bins for X and Y respectively. Otherwise, declare an error. During decoding, the pair of indices that have been transmitted specifies a product bin, as depicted in Figure 3.5. Here, we note that the binning scheme need not be characterized at the transmitter, just at the receiver. According to Cover and Thomas [4] it is this property that allows this code to function for distributed sources.

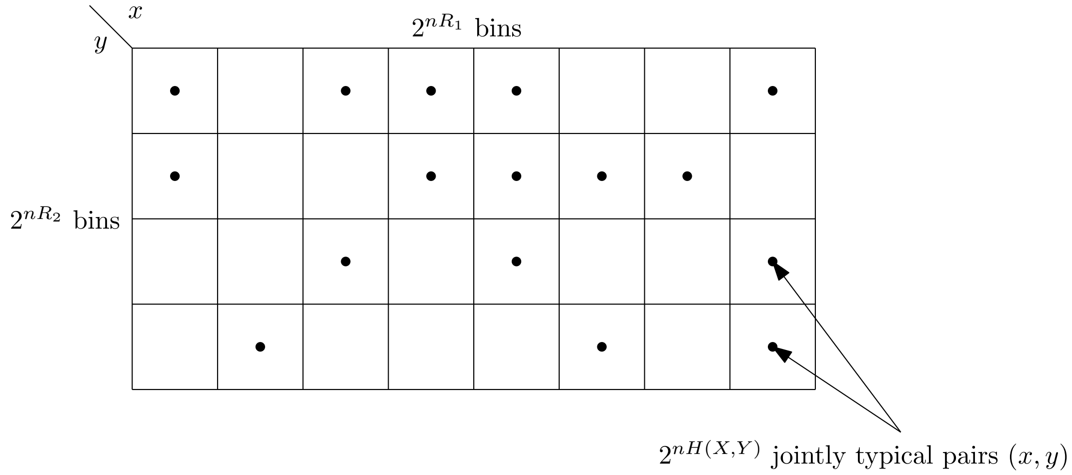

FIGURE 3.5: Slepian-Wolf encoding: the jointly typical pairs are described by the product bins [4]

Proof of Slepian-Wolf theorem. In order to prove that the Slepian-Wolf theorem is achievable, it is shown that the error probability is calculated to be bounded by 4ϵ. Four error events are defined:

- P_{e0}: the received sequence does not belong to the typical set
- P_{e1}: there exists another x, i.e. x' in the bin that is jointly typical with Y
- P_{e2}: there exists another y, i.e. y' in the bin that is jointly typical with X
- P_{e3}: there exists another (x, y) in the bin that belongs to the jointly typical set.

where $(P_{e0}, P_{e1}, P_{e2}, P_{e3})$ indicate the probabilities of the error events described above. The union of these error event probabilities provide the upper bound for the error probability.

From the joint AEP, we know that the probability the sequence does not belong to the jointly typical sequence is small, and as n becomes large this error is bounded by ϵ. Therefore $P_{e_0} \leq \epsilon$.

For P_{e1}, we use the fact that the error probability is upper bounded by the joint probability distribution summed over all (x, y) (which is 1) and the probability that there exists an x' in the same bin summed over the typical sequence (which is the size of the typical sequence times 2^{nR1}). This is shown in equation form below:

$$\begin{aligned} & \sum_{(x,y)} p(x,y) \sum_{(x',y)} \in A_{\epsilon}^{(n)} P(f_1(x') = f_1(x)) \\ = & \sum_{(x',y)} |A_{\epsilon}(X|y)| 2^{-nR_1} \\ \leq & \ 2^{n(H(X|Y)+\epsilon)} 2^{-nR_1} \end{aligned} \tag{3.13}$$

We can see that if $R_1 > H(X|Y)$ then for sufficiently large n (3.13) tends to 0, hence the error probability is upper bounded by ϵ. This means $P_{e_1} \leq \epsilon$. Similarly the third and fourth events can be shown to be upper bounded by ϵ each when $R_2 > H(Y|X)$ and $R_1 + R_2 > H(X, Y)$. The combination of these upper bounds results in an error probability of 4ϵ. This is shown by equations (3.14) and as follows.

$$\begin{aligned} & \sum_{(x,y)} p(x,y) \sum_{(x,y')} \in A_{\epsilon}^{(n)} P(f_2(y) = f_2(y')) \\ = & \sum_{(x,y')} |A_{\epsilon}(x|Y)| 2^{-nR_1} \\ \leq & \ 2^{n(H(Y|X)+\epsilon)} 2^{-nR_2} \end{aligned} \tag{3.14}$$

For P_{e2}, the fact that the error probability is upper bounded by the joint probability distribution summed over all (x, y) (which is 1) and the probability that there exists an y' in the same bin summed over the typical sequence (which is the size of the typical sequence times 2^{nR2} is used to determine the probability. It is seen that as $R_2 > H(Y|X)$ then for sufficiently large n (3.14) tends to 0, hence the error probability is upper bounded by ϵ. This implies that $P_{e_2} \leq \epsilon$.

For the remaining probability P_{e_3} we use the following as a result for there existence of another typical sequence in the same bin.

$$\begin{aligned} & \sum_{(x,y)} p(x,y) \sum_{(x,y)} \in A_\epsilon^{(n)} P(f_2(y) = f_2(y')) \\ = & \sum_{(x,y)} |A_\epsilon(X|Y)| 2^{-nR_1} 2^{-nR_2} \\ \leq & \; 2^{n(H(X,Y)+\epsilon)} 2^{-nR_1} 2^{-nR_2} \end{aligned} \tag{3.15}$$

From the result of (3.15) it is seen that as $R_1 + R_2 > H(X,Y)$ then for sufficiently large n, (3.15) tends to 0, hence the error probability is also upper bounded by ϵ. This implies that $P_{e_3} \leq \epsilon$. The combination of probabilities for these four error events, $(P_{e_0}, P_{e_1}, P_{e_2}, P_{e_3})$ is therefore upper bounded by 4ϵ. This proof shows the achievability of the Slepain-Wolf theorem, which has a major impact for correlated sources. □

There has been important work that makes use of the Slepian-Wolf theorem, for example that by Yamamoto [5] and Villard *et al.* [60]. These schemes use the Slepian-Wolf theorem to provide models for applications on broadcast channels, linking digital and analogue schemes [61] and binary erasure channels [60]. These therefore form the building blocks for systems of such applications. This points out that the research presented herein may also be used for these applications and in these ways to better the security of the system.

Optimizing the transmission rate regions is an aspect of Slepian-Wolf coding. As the rate increases the security decreases, which comes from the deduction that the error entropy is proportional to the information rate. Thus, in order to achieve optimal security, the rate should decrease.

Yang *et al.* [2] incorporate the Slepian-Wolf theorem into their study and give an indication of the achievable region for Slepian-Wolf codes (Figure 3.6).

The shaded region indicated in Figure 3.6 is that where the decoder can recover X and Y with arbitrarily small error (*i.e* the achievable region). The compression rate in bits is given by R_X and R_Y to encode X and Y respectively. When transmission occurs in this region then decoding can occur correctly.

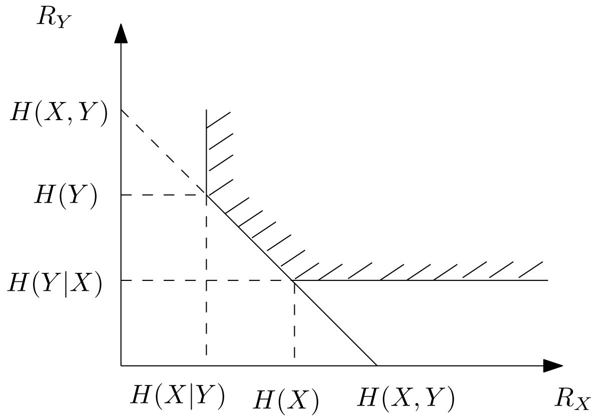

FIGURE 3.6: Diagram showing achievable region for the Slepian-Wolf theorem [2]

3.2.3 Shannon's Cipher System

The Shannon cipher system was the first information-theoretically secure communication system [42], and operates based on the following protocol:

For sources X and Y, sending a message m to the destination T:

- Generate e (secret key)
- Send $m + e \pmod p$ over the public channel, where m is the message intended for the receiver
- Send e over the private channel

After transmission, the receiver has access to both $m+e$ and e and can therefore retrieve m. The main idea is that the sender must randomize the message to protect it from the wiretapper. However, it is important to note that randomization decreases throughput as more bandwidth is necessary to transmit the various randomized versions of the source message.

Yamamoto [5] used Shannon's cipher system for correlated sources that transmit information across a common link (depicted in Figure 3.7). A key is used at the encoder to encode the messages and the same key is provided at the decoder in order to decode the messages. The encoding and decoding functions therefore include a key. The security of the system largely depends on the key security. The security levels are defined and described by Yamamoto [5] to characterize the security for each source X and Y by

(h_X, h_Y) and their combined security h_{XY}. Later in this work the same notation is used for describing the security levels. The purpose of incorporating Shannon's cipher system for Yamamoto [5] was to determine the transmission and key rates necessary for obtaining perfect secrecy.

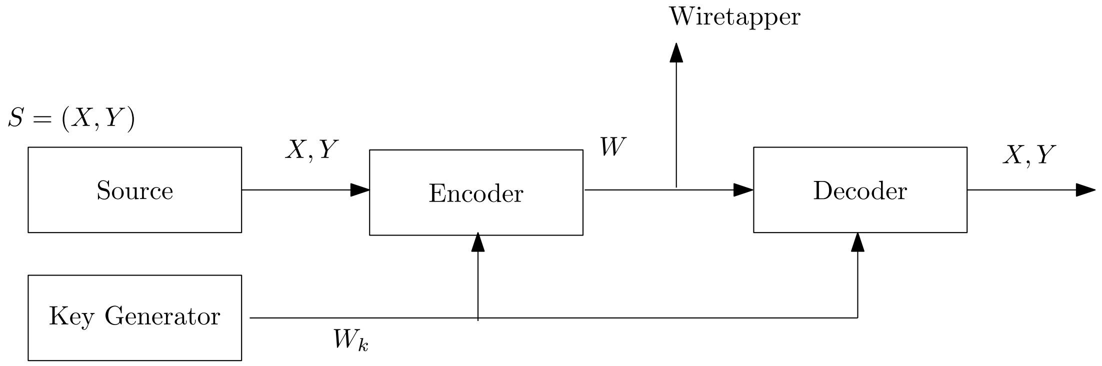

FIGURE 3.7: Shannon cipher system [5]

In Figure 3.7, the correlated sources are represented by X and Y, W is the cryptogram and W_k is the key. In Yamamoto's study in [5], the correlated sources are focused on and the key rate for a certain level is defined. In the study in [40], certain parameters (admissible region of cryptogram rate, key rate, legitimate receiver's distortion, wiretapper's uncertainty) for the Shannon cipher system with a noisy channel are determined. In an extension of the Shannon cipher system, Yamamoto [37] investigated the secret sharing communication system.

3.3 Wiretap Networks

The wiretapped network concept comes from the need to model a scenario where there is an eavesdropper present. The concept of wiretap network is best explained as a communication network and a collection of subsets of wiretap channels, where a wiretapper can eavesdrop on the packets on a limited number of network edges of its choice. There are models developed for the wiretap channel of type I and type II. The wiretap channel type II is an error-free version of the type I channel.

The mathematical model for Wiretap Channel II is given by Rouayheb *et al.* [6], and can be explained as follows: the channel between a transmitter and receiver is error-free and can transmit n symbols $Y = (y_1, \ldots, y_n)$ from which μ bits can be observed by the eavesdropper and the maximum secure rate can be shown to equal $n - \mu$ bits.

Here, μ is therefore the upper bound of information that can be leaked. This Wiretap Channel II concept is depicted diagrammatically in Figure 3.8.

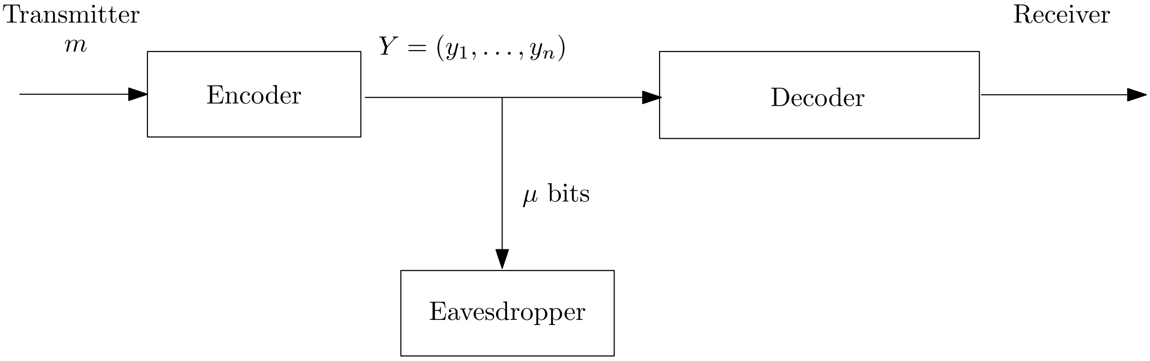

Figure 3.8: Wiretap Channel II concept [6]

In Figure 3.8, m is the source output, $Y = (y_1, \ldots, y_n)$ are the transmitted codewords and μ is the wiretapped information. The components of a wiretap network are as follows:

- Directed multigraph $G = (V, E)$, where G is acyclic, V is a node set and E is the edge set for the directed multigraph
- Source node, S
- Collection of a set of wiretapped edges (A), which is a collection of the subsets of edges, E (*i.e.* $A \subseteq E$). More than one element of A may be accessed by a wiretapper
- Set of user nodes, U (*i.e.* the users that are meant to receive the message m)

The quadruple (G, S, U, A) is referred to as a wiretap network [42]. In terms of the wiretap network, it is of concern to transmit messages across the network, while a wiretapper can access any set of the edges in A.

The wiretapped concept is also used in the Shannon cipher system, which has been investigated by Yamamoto [5] [40].

3.3.1 Ozarow and Wyner's Method

The method for information hiding across a wiretap channel was introduced by Ozarow and Wyner [45], which hereafter is referred to as Ozarow's and Wyner's method. The linear code is represented as a $(n, n - K)$ code, where $n > K$. The wiretapper is able to access their choice of $\mu < n$ bits. The scheme involves coset coding.

Ozarow and Wyner [45] define the Wiretap Channel II as follows:

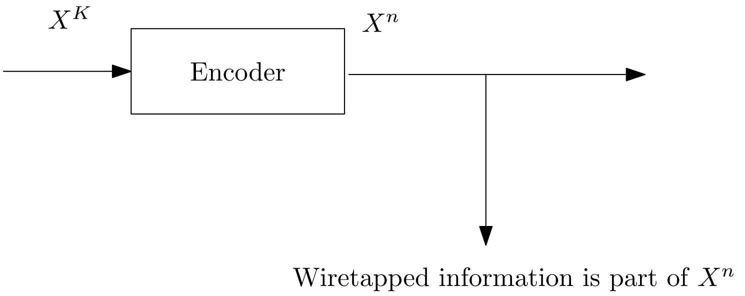

Figure 3.9: Diagram showing the set-up of the Wire-tap Channel II

where X^K is the source output and X^n is the n bit binary transmitted sequence across an error-free channel.

The uniqueness in this method lies in two considerations:

- a one to one relationship between the error patterns of length n and message of length K, that is to be received by the decoder, and
- the difficulty in determining the required error pattern if only one link is wiretapped.

This scheme is able to transmit K bits of information, using n bits, and is defined for a peer to peer scenario. Each message m is uniquely mapped to an error pattern $e(m)$, and the receiver is required to determine this $e(m)$ in order to find m.

Here, x has length n and is randomly chosen from the generated codebook, based on the codeword, and the transmitted sequence also has a length n. This sequence is a linear representation of x and an error pattern as indicated in (3.16).

$$x \oplus e(m) \tag{3.16}$$

where $e(m)$ is the error pattern corresponding to the information. This is illustrated diagrammatically in Figure 3.10.

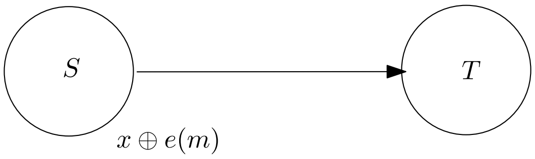

Figure 3.10: General representation of Ozarow's method

There is a unique mapping between the 2^K error patterns and messages that are to be transmitted. The decoder, T in Figure 3.10 receives $x \oplus e(m)$ and at a later time obtains/receives x. Thereafter, the exclusive-or of $x \oplus e(m)$ and x is performed, which results in the error message, $e(m)$ and due to the one to one mapping of the message with the error patterns, the original message m can easily be obtained. Here, the value of x acts as a mask in order to hide the error pattern that is being transmitted.

The advantage of this method in terms of secrecy is that if the link in Figure 3.10 is wiretapped then it is not possible to determine the error pattern that corresponds to the information being transmitted, hence the information remains secure.

This method is extended by Silva and Kschischang [44] where a proposed coset coding scheme is defined over an extension field.

3.3.2 Generalized Hamming Weight

The generalized Hamming weight concept is illustrated initially using the Ozarow and Wyner coding scheme presented above, by Wei [7]. Here, the generalized Hamming weight concept is presented for linear codes that completely characterize the performance of a linear code when it is used in a Wiretap Channel II. Based on using the minimum Hamming weight as a certain minimum property of one-dimensional sub codes, the authors obtain a generalized concept of higher-dimensional Hamming weights. A 'security curve' depicting the level of security for a (15,11) Hamming code is developed [7], and this shows the variation in the amount of information a wiretapper gains when having access to $\mu = \{0, 1, \ldots, 15\}$ bits of the message. The 'security curve' is shown below:

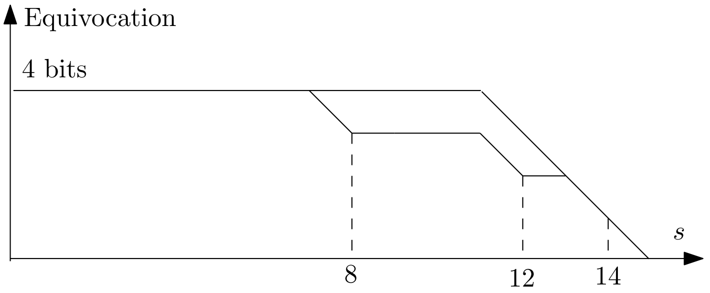

FIGURE 3.11: Security curve as developed by Wei [7]

The wiretapper is able to listen to any s bits, and the corresponding equivocation (*i.e.* the wiretapper's uncertainty in the message) is depicted in Figure 3.11. The equivocation is calculated based on equation (3.17) as follows:

$$min_{|I|=n-s} rank(< H_i : i \in I >) \tag{3.17}$$

where n is the number of bits of the source message, s is the number of bits that are wiretapped and H is the parity-check matrix for the codewords.

In order to determine the level of security, the minimum rank of the parity-check matrix H (using the column vectors) is calculated for each possibility of the number of leaked bits. This gives an indication of how much of uncertainty the wiretapper has in reconstructing the source message; the more the uncertainty, the more secure the system. The information leakage is therefore determined by the number of independent columns in H, *i.e.* the rank of the parity-check matrix. The drops for the curve depicted in Figure 3.11 occur at the generalized Hamming weights of the codeword matrix [7].

An interesting study based on the equivocation of data symbols is done by Luo *et al.* [47], where the user is split into multiple parties who are coordinated in coding their data symbols by using the same encoder. The wiretapper is able to tap partial transmitted symbols (i.e. Z^{μ}) and partial data symbols (i.e. S_2, as the source S is divided into two portions, S_1 and S_2). The generalized Hamming weight concept explained above is extended in the study, and shown to be useful for designing a perfect secrecy coding scheme for many parties. Here, the equivocation is investigated by analysing the difference between the ranks of a matrix (one that is constructed such that it can be used to calculate the received data bits) and a sub matrix of it.

The idea of equivocation and matrix partitions are used to determine how much of information the eavesdropper has access to. The generator matrix is split to represent the data symbols and a sub matrix is subtracted from the generator matrix in order to determine the equivocation. Luo *et al.* [47] proved the following:

$$\text{rank } G - \text{rank } G_2 = \min[H(S_1, S_2|Z^{\mu}) - H(S_2|Z^{\mu})] \tag{3.18}$$

where G_2 is the sub matrix of G, the generator matrix corresponding to the eavesdropped data symbols. For Luo *et al.* [47] the G matrix is divided into two portions, G_1 and G_2. Equation (3.18) shows that these ranks may be used to determine certain equivocations. The overall result is the equivocation on S_1, given Z^{μ} and S_2. This result is essential in providing the link between coding theory and information theory and has been used accordingly for this research project.

3.4 Coding Techniques for Correlated Sources

The coding technique that this research uses to show the link between information theory and coding theory is termed the matrix partition method and is described in this section.

This concept of matrix partition has been used to show practical implementation of certain techniques or coding theories. Here, a method that incorporates a partitioned generator matrix is described, and as mentioned in Chapter II there have been other such techniques that partition generator matrices; namely those developed by Yang *et al.* [54], Pradhan and Ramchandran [55], Liveris *et al.* [56] and Ma and Cheng [57].

Stankovic *et al.* [58] mention one of the basic techniques used for source correlation; a matrix partition approach is adopted. The general Slepian-Wolf code pair $(\mathcal{C}, m)$ is defined in [17], where $\mathcal{C}$ is an (n, k) linear code, which has a generator matrix $G_{k\times n}$ and m is a set of integers $\{m_1, m_2, \ldots, m_L\}$. Here, L is the number of partitions of the G

matrix. The codebook $\mathcal{C}$, which is the product of the message, m (of length k bits) and the generator matrix is represented below:

$$c = m \times G \tag{3.19}$$

The two correlated sources are X and Y and can produce codewords c (where $c \in \mathcal{C}$) of length n; x and y are the source messages. The correlated sources satisfy the Slepian-Wolf theorem given in equation (3.19). Sub matrices for the generator and parity-check matrices, G and H respectively, are initially constructed. Thereafter the syndromes $s_i = (s_1, \ldots, s_L)$ (where L is the number of partitions of the G matrix) are constructed and transmitted. The decoder is then responsible for reconstructing the source messages from the transmitted syndrome.

The partition of G and resultant partitions in H are calculated as per the partitions specified by the matrix partition method [58]:

$$G = \begin{bmatrix} I_k & P_{k \times (n-k)} \end{bmatrix} \tag{3.20}$$

$$G_i = \begin{bmatrix} O_{m_i \times m_{i-}} & I_{m_i} & O_{m_i \times m_{i+}} & P_{i_{m_i \times (n-k)}} \end{bmatrix} \tag{3.21}$$

$$H_i = \begin{bmatrix} I_{m_{i-}} & O_{m_{i-} \times m_i} & O_{m_{i-} \times m_{i+}} & O_{m_{i-} \times (n-k)} \\ O_{m_{i+} \times m_{i-}} & O_{m_{i+} \times m_i} & I_{m_{i+}} & O_{m_{i+} \times (n-k)} \\ O_{(n-k) \times m_{i+}} & P^T_{m_i} & O_{(n-k) \times m_{i+}} & I_{n-k} \end{bmatrix} \tag{3.22}$$

Where O_i is a zero matrix, of size defined by the subscript i and I_j is an identity matrix, of size defined by the subscript j. Here, P_k and P_i make up the $P_{k \times (n-k)}$ component of a particular G matrix, as defined in equation (3.20).

After these partitions are formed the syndromes are calculated by multiplying the source message $x_i = \begin{bmatrix} u_i & a_i & v_i & q_i \end{bmatrix}$, (which has length m_{i-}, m_i, m_{i+} and $n-k$ respectively) with the parity-check matrix H to result in:

$$s_i = \begin{bmatrix} u_i^T \\ v_i^T \\ q_i^T \oplus P_i^T a_i^T \end{bmatrix} \tag{3.23}$$

The source messages are compressed into syndromes of length $n - m_i$ bits in this step. At the decoder, the first step is to decompress the syndromes. This is done as indicated below:

$$t_i = \begin{bmatrix} u_i^T \\ O_{m_i \times 1} \\ v_i^T \\ q_i^T \oplus P_i^T a_i^T \end{bmatrix} \tag{3.24}$$

The results of $t_1 \oplus t_2, \ldots, \oplus t_L$ are calculated. The codeword satisfying the following is found:

$$d_{min}(t_1 \oplus t_2, c) \tag{3.25}$$

where d_{min} is the minimum Hamming distance and $c \in \mathcal{C}$, where $\mathcal{C}$ is the codebook.

For example, for a (7, 4) Hamming code where two rows of G are used to calculate the subcode for each encoder, the G and H matrices take the following form (this also gives an indication of matrix dimensions):

$$G_1 = \begin{bmatrix} O_{2\times2} & I_2 & O_{2\times2} & P_{1_{2\times3}} \end{bmatrix} \tag{3.26}$$

$$G_2 = \begin{bmatrix} O_{2\times 2} & I_2 & O_{2\times 2} & P_{2_{2\times 3}} \end{bmatrix} \tag{3.27}$$

$$H_1 = \begin{bmatrix} I_2 & O_{2\times 2} & O_{2\times 2} & O_{2\times 3} \\ O_{2\times 2} & O_{2\times 2} & I_2 & O_{2\times 3} \\ O_{3\times 2} & P_1^T & O_{3\times 2} & I_3 \end{bmatrix} \tag{3.28}$$

$$H_2 = \begin{bmatrix} I_2 & O_{2\times 2} & O_{2\times 2} & O_{2\times 3} \\ O_{2\times 2} & O_{2\times 2} & I_2 & O_{2\times 3} \\ O_{3\times 2} & P_2^T & O_{3\times 2} & I_3 \end{bmatrix} \tag{3.29}$$

In order to encode, the n length (in this case $n = 7$) vector $x_i = \begin{bmatrix} u_i & a_i & v_i & q_i \end{bmatrix}$ is multiplied by the parity-check matrix, H. In this way the syndromes are formed as follows:

$$s_1 = \begin{bmatrix} v_1^T \\ q_1^T \oplus P_1^T a_1^T \end{bmatrix} \tag{3.30}$$

$$s_2 = \begin{bmatrix} u_2^T \\ q_2^T \oplus P_2^T a_2^T \end{bmatrix} \tag{3.31}$$

In order to assist with decoding, n-length row vectors t_1 and t_2 are defined as:

$$t_1 = \begin{bmatrix} O_{2\times 1} \\ v_1^T \\ q_1^T \oplus P_1^T a_1^T \end{bmatrix} \tag{3.32}$$

$$t_2 = \begin{bmatrix} u_2^T \\ O_{2\times 1} \\ q_2^T \oplus P_2^T a_2^T \end{bmatrix} \tag{3.33}$$

Stankovic *et al.* [58] make the conclusion that $x_i \oplus t_i = a_i G_i$ is a valid codeword of $\mathcal{C}_i$ (the codeword sub matrix) and thus $\mathcal{C}$ (the codeword matrix). At the decoder, both syndromes are collected and $t_1 \oplus t_2$ is calculated. The decoder is then tasked with finding a codeword that is closest (in Hamming distance) to the result of $t_1 \oplus t_2$, as per the representation in (3.25). The sources are recovered as:

$$x_1 = a_1 G_1 \oplus t_1 \tag{3.34}$$

and

$$x_2 = a_2 G_2 \oplus t_2 \tag{3.35}$$

where a_1 and a_2 are the decoded systematic parts of the codeword. It is thus possible to retrieve X and Y using the systematic part of the codeword, the generator matrix and the received syndrome.

This method is one of the methods that partition the generator matrix in order to transmit information effectively for correlated sources. In work by Ma and Cheng [57], the generator matrix is also similarly split so that each portion can be used to determine the resultant message for a particular source. There has also been similar partition methods provided by Yang *et al.* [54], Pradhan and Ramchandran [55] and Liveris *et al.* [56], where each examines a particular coding method for these partitions.

This chapter contained the descriptions of the techniques that have been used in this research project. The techniques used to analyze the security aspects have been presented; namely Slepian-Wolf theorem and Shannon's cipher system, together with the associated methodologies involved in proving these theorems or methods. Wiretap networks have also been explored followed by descriptions of the coding techniques involved in analyzing the models that have been developed.

Chapter 4

Information Leakage for Multiple Correlated Sources using Slepian-Wolf Coding

This chapter initially details a generalized correlated source model, which is an extension of the novel two correlated source model described later in this chapter and the correlated source models described in the following chapters. One of the main contributions is the development of the two correlated source model (there is reference made during the chapter to the difference between this model and the others from the literature reviewed, emphasizing the novelty). There are initially two avenues explored to investigate the information leakage in this chapter; one quantifying the information leakage for the Slepian-Wolf scenario and the other incorporating Shannon's cipher system where key lengths are minimized and a masking method to save on keys is presented. The security aspects of the two correlated source model is also a contribution. An important contribution thereafter is the coding approach for the two correlated source model. There are details describing the coding approach contained in this chapter, which show practical implementation for the novel model developed and provides an important link between the information theory and coding theory fields.

4.1 A Generalized Model for Multiple Correlated Sources

Consider multiple correlated sources transmitting information to a single receiver. There is common and private information transmitted along the links, which in the presence of a wiretapper may be compromised. Here, the multiple correlated sources transmit compressed information across multiple links, which are wiretapped. Figure 4.1 gives a pictorial view of the model for multiple correlated sources. The notation used in this figure is explained below.

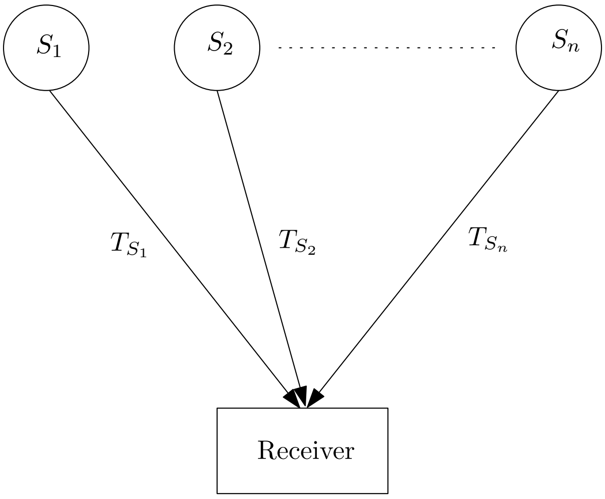

Figure 4.1: Extended generalized model

Consider a situation where there are many sources, which are part of the set $\mathbf{S}$:

$$\mathbf{S} = \{S_1, S_2, \ldots, S_n\}$$

where i represents the i^{th} source ($i = 1, \ldots, n$) and there are n sources in total. Each source may have some correlation with another source and all sources are part of a binary alphabet. There is one receiver that is responsible for performing decoding. The syndrome for a source S_i is represented by T_{S_i}, which is part of the same alphabet as the sources. The entropy of a source is given by a combination of a specific conditional entropy and mutual information. In order to present the entropy we first define the following sets:

- The set, $\mathbf{S}$ that contains all sources: $\mathbf{S} = \{S_1, S_2, \ldots, S_n\}$.

- The set, $\mathbf{S}_t$ that contains t unique elements from $\mathbf{S}$ and $\mathbf{S}_t \subseteq \mathbf{S}$, $S_i \in \mathbf{S}_t$, $\mathbf{S}_t \cup \mathbf{S}_t^c$ $= \mathbf{S}$ and $|\mathbf{S}_t| = t$

Here, $H(S_i)$ is obtained as follows:

$$H(S_i) = H(S_i|\mathbf{S}_{\setminus S_i}) + \sum_{t=2}^{n}(-1)^{t-1} \sum_{\text{all possible } \mathbf{S}_t} I(\mathbf{S}_t|\mathbf{S}_t^c) \tag{4.1}$$

where n is the number of sources, $H(S_i|\mathbf{S}_{\setminus S_i})$ denotes the conditional entropy of the source S_i given S_i subtracted from the set $\mathbf{S}$ and $I(\mathbf{S}_t|\mathbf{S}_t^c)$ denotes the mutual information between all sources in the subset $\mathbf{S}_t$ given the complement of $\mathbf{S}_t$. It is possible to decode the source message for source S_i by receiving all components related to S_i. This gives rise to the following inequality for $H(S_i)$ in terms of the sources:

$$\begin{aligned} H(S_i|\mathbf{S}_{\setminus S_i}) \quad &+ \quad \sum_{t=2}^{n}(-1)^{t-1} \sum_{\text{all possible } \mathbf{S}_t} I(\mathbf{S}_t|\mathbf{S}_t^c) \\ &\leq \quad H(S_i) + \delta \end{aligned} \tag{4.2}$$

In this type of model information from multiple links may need to be gathered in order to determine the transmitted information for one source because common information may be transmitted by other links. Here, the common information between sources is represented by the $I(\mathbf{S}_t|\mathbf{S}_t^c)$ term. The portions of common information sent by each source can be determined upfront and is arbitrarily allocated.

The information leakage for this multiple source model is indicated in (4.3) and (4.4).

Remark 1: The leaked information for a source S_i given the transmitted codewords T_{S_i}, is given by:

$$L_{T_{S_i}}^{S_i} = I(S_i; T_{S_i}) \tag{4.3}$$

Since the notion that the information leakage is the conditional entropy of the source given the transmitted information subtracted from the source's uncertainty (i.e $H(S_i) - H(S_i|T_{S_i})$), the proof for (4.3) is trivial. Here, the common information is the minimum amount of information leaked. Each source is responsible for transmitting its own private information and there is a possibility that this private information may also be leaked. The maximum leakage for this case is thus the uncertainty of the source itself, $H(S_i)$.

We also consider the information leakage for a source S_i when another source $S_{j(j \neq i)}$ has transmitted information. This gives rise to Remark 2.

Remark 2: The leaked information for a source S_i given the transmitted codewords T_{S_j}, where $i \neq j$ is:

$$\begin{aligned} L^{S_i}_{T_{S_j}} &= H(S_i) - H(S_i|T_{S_j}) \\ &= H(S_i) - [H(S_i) - I(S_i;T_{S_j})] \\ &= I(S_i;T_{S_j}) \end{aligned} \tag{4.4}$$

The information leakage for a source is determined based on the information transmitted from any other channel using the common information between them. The private information is not considered as it is transmitted by each source itself and can therefore not be obtained from an alternate channel. Remark 2 therefore gives an indication of the maximum amount of information leaked for source S_i, with knowledge of the syndrome T_{S_j}.

The common information provides information for more than one source and is therefore important to secure as it leaks information about more than one source. This section gives an indication of the information leakage for the multiple correlated sources model.

4.2 Two Correlated Source Model

A special case of multiple correlated sources is now investigated. The independent, identically distributed (i.i.d.) sources X and Y are mutually correlated random variables, depicted in Figure 4.2. The alphabet sets for sources X and Y are represented by $\mathcal{X}$ and $\mathcal{Y}$ respectively. Assume that (X^K, Y^K) are encoded into two syndromes (T_X and T_Y). The compressed representation is as follows: $T_X = (V_X, V_{CX})$ and $T_Y = (V_Y, V_{CY})$ where T_X and T_Y are the syndromes of X and Y. Here, T_X and T_Y are characterized by (V_X, V_{CX}) and (V_Y, V_{CY}) respectively. The Venn diagram in Figure 4.3 easily illustrates this idea where it is shown that V_X and V_Y represent the private information of sources X^K and Y^K respectively and V_{CX} and V_{CY} represent the common information between X^K and Y^K generated by X^K and Y^K respectively.

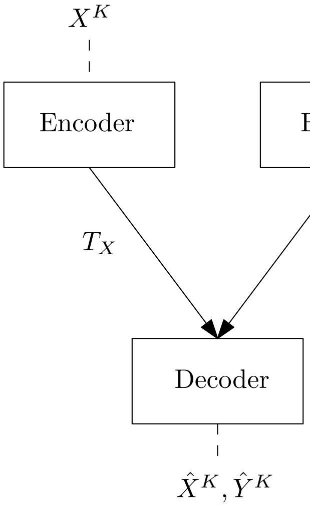

FIGURE 4.2: Correlated source coding for two sources

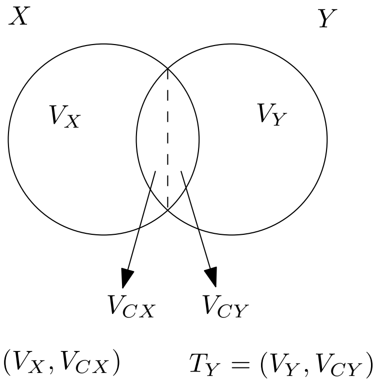

FIGURE 4.3: The relation between private and common information

The correlated sources X and Y transmit messages (in the form of syndromes) to the receiver along wiretapped links. The decoder determines X and Y only after receiving all of T_X and T_Y. The common information between the sources are transmitted through the portions V_{CX} and V_{CY}. In order to determine a transmitted message, a source's private information and a common information portion are necessary.

Here, the Slepian-Wolf bound is reached. The lengths of T_X and T_Y are not fixed as it depends on the encoding process and nature of the Slepian-Wolf codes. The process is therefore not ideally one-to-one and reversible and is another difference between this model and Yamamoto's [5] model.

The code described in this section satisfies the following inequalities for $\delta > 0$ and sufficiently large K.

$$Pr\{X^K \neq G(V_X, V_{CX}, V_{CY})\} \leq \delta \tag{4.5}$$

$$Pr\{Y^K \neq G(V_Y, V_{CX}, V_{CY})\} \leq \delta \tag{4.6}$$

$$H(V_X, V_{CX}) \leq H(X^K) + \delta \tag{4.7}$$

$$H(V_Y, V_{CY}) \leq H(Y^K) + \delta \tag{4.8}$$

$$H(V_X, V_Y, V_{CY}) \leq H(X^K, Y^K) + \delta \tag{4.9}$$

$$H(X^K|V_X, V_Y) \geq H(V_{CX}) - \delta \tag{4.10}$$

$$H(X^K|V_{CX}, V_{CY}) \geq H(V_X) - \delta \tag{4.11}$$

$$H(X^K|V_{CX}, V_{CY}, V_Y) \geq H(V_X) - \delta \tag{4.12}$$

$$\begin{aligned} H(V_{CX}) + H(V_X) - \delta \leq H(X^K|V_{CY}, V_Y) \\ \leq H(X^K) - H(V_{CY}) + \delta \end{aligned} \tag{4.13}$$

where G is a function to define the decoding process at the receiver. It can intuitively be seen from (4.7) and (4.8) that X and Y are recovered from the corresponding private information and the common information produced by X^K and Y^K. Equations (4.7) - (4.9) show that the private information and common information produced by each source should contain no redundancy. It is also seen from (4.11) and (4.12) that V_Y is independent of X^K asymptotically. Here, (V_X, V_Y) and V_{CX} or V_{CY} are asymptotically disjoint, which ensures that no redundant information is sent to the decoder.

Yamamoto [5] proved that a common information between X^K and Y^K is represented by the mutual information $I(X;Y)$. Yamamoto [5] also defined two kinds of common information. The first common information is defined as the rate of the attainable minimum core by removing each private information, which is independent of the other information, from (X^K, Y^K) as much as possible. The second common information is defined as the rate of the attainable maximum core such that if we lose this quantity then the uncertainty of X and Y becomes the entropy of the common information between the sources. Here, the common information that V_{CX} and V_{CY} represent is considered.

The relationship between the common information portions is now demonstrated by constructing the prototype code (W_X, W_Y, W_{CX}, W_{CY}) as per Lemma 1.

Lemma 1: For any $\epsilon_0 \geq 0$ and sufficiently large K, there exits a code $W_X = F_X(X^K)$, $W_Y = F_Y(Y^K)$, $W_{CX} = F_{CX}(X^K)$, $W_{CY} = F_{CY}(Y^K)$, $\widehat{X}^K, \widehat{Y}^K = G(W_X, W_Y, W_{CX}, W_{CY})$, where $W_X \in I_{M_X}$, $W_Y \in I_{M_Y}$, $W_{CX} \in I_{M_{CX}}$, $W_{CY} \in I_{M_{CY}}$ for I_{M_α}, which is defined as $\{0, 1, \ldots, M_\alpha - 1\}$, that satisfies,

$$Pr\{\widehat{X}^K, \widehat{Y}^K \neq X^K, Y^K\} \leq \epsilon \tag{4.14}$$

$$H(X|Y) - \epsilon_0 \leq \frac{1}{K} H(W_X) \leq \frac{1}{K} \log M_X \leq H(X|Y) + \epsilon_0 \tag{4.15}$$

$$H(Y|X) - \epsilon_0 \leq \frac{1}{K} H(W_Y) \leq \frac{1}{K} \log M_Y \leq H(Y|X) + \epsilon_0 \tag{4.16}$$

$$\begin{aligned} I(X;Y) - \epsilon_0 &\leq \frac{1}{K}(H(W_{CX}) + H(W_{CY})) \\ \leq & \frac{1}{K}(\log M_{CX} + \log M_{CY}) \leq I(X;Y) + \epsilon_0 \end{aligned} \tag{4.17}$$

$$\frac{1}{K} H(X^K|W_Y) \geq H(X) - \epsilon_0 \tag{4.18}$$

$$\frac{1}{K} H(Y^K|W_X) \geq H(Y) - \epsilon_0 \tag{4.19}$$

We can see that (4.15) - (4.17) mean

$$\begin{aligned} & H(X,Y) - 3\epsilon_0 \leq \frac{1}{K}(H(W_X) + H(W_Y) + H(W_{CX}) \\ + \quad & H(W_{CY})) \\ \leq \quad & H(X,Y) + 3\epsilon_0 \end{aligned} \tag{4.20}$$

Hence from (4.14), (4.20) and the ordinary source coding theorem, (W_X, W_Y, W_{CX}, W_{CY}) have no redundancy for sufficiently small $\epsilon_0 \geq 0$. It can also be seen that W_X and W_Y are independent of Y^K and X^K respectively.

Proof of Lemma 1. As seen by Slepian and Wolf, mentioned by Yamamoto [5] there exist M_X codes for the $P_{Y|X}(y|x)$ DMC (discrete memoryless channel) and M_Y codes for the $P_{X|Y}(x|y)$ DMC. The codeword sets exist as C_i^X and C_j^Y, where C_i^X is a subset of the typical sequence of X^K and C_j^Y is a subset of the typical sequence of Y^K. The encoding functions are similar, and here one decoding function has been created as there is one decoder at the receiver:

$$f_{Xi} : I_{M_{CX}} \to C_i^X \tag{4.21}$$

$$f_{Yj} : I_{M_{CY}} \to C_j^Y \tag{4.22}$$

$$g : X^K, Y^K \to I_{M_{CX}} \times I_{M_{CY}} \tag{4.23}$$

The relations for (M_X, M_Y) and the common information remains the same as per Yamamoto's and will therefore not be proven here.

In this scheme, the average (V_{CX}, V_{CY}) transmitted is used for many codewords from X and Y. Thus, at any time either V_{CX} or V_{CY} is transmitted. Over time, the split between which common information portion is transmitted is determined and the protocol is prearranged accordingly. Therefore all the common information is either transmitted as l or m, and as such Yamamoto's encoding and decoding method may be used.

As per Yamamoto's method the code does exist and W_X and W_Y are asymptotically independent of Y and X respectively, as shown by Yamamoto [5]. □

The common information is important in this model as the sum of V_{CX} and V_{CY} represent a common information between the sources. The following theorem holds for this common information:

Theorem 1:

$$\frac{1}{K}[H(V_{CX}) + H(V_{CY})] = I(X;Y) \tag{4.24}$$

where V_{CX} is the common portion between X^K and Y^K produced by X^K and V_{CY} is the common portion between X^K and Y^K produced by Y^K. It is noted that the (4.24) holds asymptotically, and does not hold with equality when K is finite. Here, we show the approximation when K is infinitely large. The private portions for X^K and Y^K are represented as V_X and V_Y respectively. As explained in Yamamoto's [5] Theorem 1, two types of common information exist (the first is represented by $I(X;Y)$ and the second by $\min(H(X^K), H(Y^K))$. Here part of this idea is developed to show that the sum of the common information portions produced by X^K and Y^K in this new model is represented by the mutual information between the sources.

Proof of Theorem 1. The first part is to prove that $H(V_{CX}) + H(V_{CY}) \geq I(X;Y)$. The conditions (4.5) and (4.6) are weakened to the following:

$$\Pr\,\{X^K, Y^K \neq G_{XY}(V_X, V_Y, V_{CX}, V_{CY}\}) \leq \delta_1 \tag{4.25}$$

For any (V_X,V_Y, V_{CX}, V_{CY}) $\in C(3\epsilon_0)$ (which can be seen from (4.20)), from (4.25) and the ordinary source coding theorem that the following results:

$$\begin{aligned} H(X^K, Y^K) - \delta_1 &\leq \frac{1}{K}H(V_X, V_Y, V_{CX}, V_{CY}) \\ &\leq \frac{1}{K}[H(V_X) + H(V_Y) + H(V_{CX}) \\ &+ H(V_{CY})] \end{aligned} \tag{4.26}$$

where $\delta_1 \to 0$ as $\delta \to 0$. From Lemma 1,

$$\frac{1}{K}H(V_Y|X^K) \geq \frac{1}{K}H(V_Y) - \delta \tag{4.27}$$

$$\frac{1}{K}H(V_X|Y^K) \geq \frac{1}{K}H(V_X) - \delta \tag{4.28}$$

From (4.26) - (4.28),

$$\begin{aligned}\frac{1}{K}[H(V_{CX})+H(V_{CY})] &\geq H(X,Y)-\frac{1}{K}H(V_X)\\ &- \frac{1}{K}H(V_Y)-\delta_1\\ &\geq H(X,Y)-\frac{1}{K}H(V_X|Y^K)\\ &- \frac{1}{K}H(V_Y|X^K)-\delta_1-2\delta \end{aligned} \tag{4.29}$$

On the other hand, we can see that

$$\frac{1}{K}H(X^K,V_Y) \leq H(X,Y)+\delta \tag{4.30}$$

This implies that

$$\frac{1}{K}H(V_Y|X^K) \leq H(Y|X)+\delta \tag{4.31}$$

and

$$\frac{1}{K}H(V_X|Y^K) \leq H(X|Y)+\delta \tag{4.32}$$

From (4.29), (4.31) and (4.32) we get

$$\begin{aligned}\frac{1}{K}[H(V_{CX})+H(V_{CY})] &\geq H(X,Y)-H(X|Y)-H(Y|X)\\ &- \delta_1-4\delta\\ &= I(X;Y)-\delta_1-4\delta \end{aligned} \tag{4.33}$$

It is possible to see from (4.17) that $H(V_{CX})+H(V_{CY}) \leq I(X;Y)$. From this result, (4.23) and (4.33), and as $\delta_1 \to 0$ and $\delta \to 0$ it can be seen that

$$\frac{1}{K}[H(V_{CX}+H(V_{CY})] = I(X;Y) \tag{4.34}$$

□

This model can cater for a scenario where a particular source, say X needs to be more secure than Y (possibly because of eavesdropping on the X channel). In such a case, the $\frac{1}{K}H(V_{CX})$ term in (4.33) needs to be as high as possible. When this uncertainty is increased then the security of X increases.

In order to determine the security of the system, a measure for the amount of information leaked has been developed. This is a new notation and quantification, which contributes to the novelty of this work. The obtained information and total uncertainty are used to determine the leaked information. Information leakage is indicated by $L^{\mathcal{P}}_{\mathcal{Q}}$, where $\mathcal{P}$ indicates the source/s for which information leakage is being quantified and $\mathcal{Q}$ indicates the sequence that has been wiretapped.

The information leakage bounds for the following cases are indicated in (4.35) - (4.38):

- Leakage on X when (V_X, V_Y) is wiretapped
- Leakage on X when (V_{CX}, V_{CY}) is wiretapped
- Leakage on X when (V_{CX}, V_{CY}, V_Y) is wiretapped

$$L^{X^K}_{V_X,V_Y} \leq H(X^K) - H(V_{CX}) - H(V_{CY}) + \delta \tag{4.35}$$

$$L^{X^K}_{V_{CX},V_{CY}} \leq H(X^K) - H(V_X) - H(V_{CY}) + \delta \tag{4.36}$$

$$L^{X^K}_{V_{CX},V_{CY},V_Y} \leq H(X^K) - H(V_X) - H(V_{CY}) + \delta \tag{4.37}$$

$$\begin{aligned} H(V_{CY}) - \delta \leq L^{X^K}_{V_Y,V_{CY}} & \\ \leq \quad H(X^K) - H(V_{CX}) - H(V_X) + \delta & \end{aligned} \tag{4.38}$$

Here, V_Y is private information of source Y^K and is independent of X^K and therefore does not leak any information about X^K, shown in (4.36) and (4.37). Equation (4.38) gives an indication of the minimum and maximum amount of leaked information for the interesting case where a syndrome has been wiretapped and the information leakage quantification on the alternate source is considered. The outstanding common information component is the maximum information that can be leaked. For this case, the common information V_{CX} and V_{CY} can thus consist of added protection to reduce the amount of information leaked. These bounds developed in (4.35) - (4.38) are proven in the next section.

The proofs for the above mentioned information leakage inequalities are now detailed. First, the inequalities in (4.10) - (4.13) will be proven, so as to prove that the information leakage equations hold.

Proof for (4.10):

$$\begin{aligned}
& \frac{1}{K}H(X^K|V_X, V_Y) \\
= \; & \frac{1}{K}[H(X^K, V_X, V_Y) - H(V_X, V_Y)] \\
= \; & \frac{1}{K}[H(X^K, V_Y) - H(V_X, V_Y)] && (4.39) \\
= \; & \frac{1}{K}[H(X^K|V_Y) + I(X^K; V_Y) + H(V_Y|X^K)] \\
& -\frac{1}{K}[H(V_X|V_Y) + I(V_X; V_Y) + H(V_Y|V_X)] \\
= \; & \frac{1}{K}[H(X^K|V_Y) + H(V_Y|X^K) - H(V_X|V_Y) \\
& -H(V_Y|V_X)] \\
= \; & \frac{1}{K}[H(X^K) + H(V_Y) - H(V_X) - H(V_Y)] && (4.40) \\
= \; & \frac{1}{K}[H(X^K) - H(V_X)] \\
\geq \; & \frac{1}{K}[H(V_X) + H(V_{CX}) + H(V_{CY}) - H(V_X)] - \delta \\
= \; & \frac{1}{K}[H(V_{CX}) + H(V_{CY})] - \delta && (4.41)
\end{aligned}$$

where (4.39) holds because V_X is a function of X and (4.40) holds because X is independent of V_Y asymptotically and V_X is independent of V_Y asymptotically.

For the proofs of (4.11) and (4.12), the following simplification for $H(X|V_{CY})$ is used:

$$\begin{aligned} H(X^K|V_{CY}) &= H(X^K, Y^K) - H(V_{CY}) \\ &= H(X^K) + H(V_{CY}) - I(X; V_{CY}) - H(V_{CY}) \\ &= H(X^K) + H(V_{CY}) - H(V_{CY}) - H(V_{CY}) \\ &+ \delta_1 \qquad (4.42) \\ &= H(X^K) - H(V_{CY}) + \delta_1 \qquad (4.43) \end{aligned}$$

where $I(X; V_{CY})$ approximately equal to $H(V_{CY})$ in (4.42) can be seen intuitively from the Venn diagram in Figure 4.3. Since it is an approximation, δ_1, which is smaller than δ in the proofs below has been added to cater for the tolerance.

Proof for (4.11):

$$\begin{aligned} & \frac{1}{K} H(X^K|V_{CX}, V_{CY}) \\ = & \frac{1}{K}[H(X^K, V_{CX}, V_{CY}) - H(V_{CX}, V_{CY})] \\ = & \frac{1}{K}[H(X^K, V_{CY}) - H(V_{CX}, V_{CY})] \qquad (4.44) \\ = & \frac{1}{K}[H(X^K) - H(V_{CY}) + I(X; V_{CY}) \\ + & H(V_{CY}|X^K)] - \frac{1}{K}[H(V_{CX}|V_{CY}) \\ + & I(V_{CX}; V_{CY}) + H(V_{CY}|V_{CX})] + \delta_1 \\ = & \frac{1}{K}[H(X^K) - H(V_{CY}) + H(V_{CY}) - H(V_{CX}) \\ - & H(V_{CY})] + \delta_1 \qquad (4.45) \\ = & \frac{1}{K}[H(X^K) - H(V_{CY}) - H(V_{CX})] + \delta_1 \\ \geq & \frac{1}{K}[H(V_X) + H(V_{CX}) + H(V_{CY}) - H(V_{CY}) \\ - & H(V_{CX})] - \delta \\ = & \frac{1}{K} H(V_X) + \delta_1 - \delta \qquad (4.46) \end{aligned}$$

where (4.44) holds because V_{CX} is a function of X^K and (4.45) holds because X is independent of V_{CY} asymptotically and V_{CX} is independent of V_{CY} asymptotically.

The proof for $H(X|V_{CX}, V_{CY}, V_Y)$ is similar to that for $H(X|V_{CX}, V_{CY})$, because V_Y is independent of X.

Proof for (4.12):

$$\begin{aligned}
& \frac{1}{K}H(X^K|V_{CX}, V_{CY}, V_Y) \\
= & \frac{1}{K}H(X^K|V_{CX}, V_{CY}) && (4.47) \\
= & \frac{1}{K}[H(X^K, V_{CX}, V_{CY}) - H(V_{CX}, V_{CY})] \\
= & \frac{1}{K}[H(X^K, V_{CY}) - H(V_{CX}, V_{CY})] && (4.48) \\
= & \frac{1}{K}[H(X^K) - H(V_{CY}) + I(X; V_{CY}) + H(V_{CY}|X^K)] \\
& -\frac{1}{K}[H(V_{CX}|V_{CY}) + I(V_{CX}; V_{CY}) + H(V_{CY}|V_{CX})] \\
+ & \delta_1 \\
= & \frac{1}{K}[H(X^K) - H(V_{CY}) + H(V_{CY}) - H(V_{CX}) \\
- & H(V_{CY})] + \delta_1 && (4.49) \\
= & \frac{1}{K}[H(X^K) - H(V_{CY}) - H(V_{CX})] + \delta_1 \\
\geq & \frac{1}{K}[H(V_X) + H(V_{CX}) + H(V_{CY}) - H(V_{CY}) \\
- & -H(V_{CX})] - \delta + \delta_1 \\
= & \frac{1}{K}H(V_X) - \delta + \delta_1 && (4.50)
\end{aligned}$$

where (4.48) holds because V_{CX} is a function of X^K and (4.49) holds because X^K is independent of V_{CY} asymptotically and V_{CX} is independent of V_{CY} asymptotically.

For the proof of (4.13), the following probabilities are considered:

$$\Pr\{V_X, V_{CX} \neq G(T_X)\} \leq \delta \tag{4.51}$$

$$\Pr\{V_Y, V_{CY} \neq G(T_Y)\} \leq \delta \tag{4.52}$$

$$
\begin{aligned}
& \frac{1}{K}H(X^K|T_Y) \\
\leq\ & \frac{1}{K}H(X^K, V_{CY}, V_Y)] + \delta && (4.53)\\
=\ & \frac{1}{K}[H(X^K, V_{CY}, V_Y) - H(V_{CY}, V_Y)] + \delta \\
=\ & \frac{1}{K}[H(X^K, V_Y) - H(V_{CY}, V_Y)] + \delta && (4.54)\\
=\ & \frac{1}{K}[H(X^K|V_Y) + I(X^K; V_Y) + H(V_Y|X^K)] \\
& -\frac{1}{K}[H(V_{CY}|V_Y) + I(V_{CY}; V_Y) + H(V_Y|V_{CY})] + \delta \\
=\ & \frac{1}{K}[H(X^K) + H(V_Y) - H(V_{CY}) - H(V_Y)] + \delta && (4.55)\\
=\ & \frac{1}{K}[H(X^K) - H(V_{CY})] + \delta && (4.56)
\end{aligned}
$$

where (4.53) holds from (4.52), (4.54) holds because V_{CY} and V_Y are asymptotically independent. Furthermore, (4.55) holds because V_{CY} and V_Y are asymptotically independent and X^K and V_Y are asymptotically independent.

Following a similar proof to those done above in this section, another bound for $H(X^K|V_{CY}, V_Y)$ can be found as follows:

$$
\begin{aligned}
& \frac{1}{K}H(X^K|V_{CY}, V_Y) \\
=\ & \frac{1}{K}[H(X^K, V_{CY}, V_Y) - H(V_{CY}, V_Y)] \\
=\ & \frac{1}{K}[H(X^K, V_Y) - H(V_{CY}, V_Y)] && (4.57)\\
=\ & \frac{1}{K}[H(X^K|V_Y) + I(X^K; V_Y) + H(V_Y|X^K)] \\
& -\frac{1}{K}[H(V_{CY}|V_Y) + I(V_{CY}; V_Y) + H(V_Y|V_{CY})] \\
=\ & \frac{1}{K}[H(X^K) + H(V_Y) - H(V_{CY}) - H(V_Y)] && (4.58)\\
=\ & \frac{1}{K}[H(X^K) - H(V_{CY})] \\
\geq\ & \frac{1}{K}[H(V_X) + H(V_{CX}) + H(V_{CY}) - H(V_{CY})] - \delta \\
=\ & \frac{1}{K}[H(V_X) + H(V_{CX})] - \delta && (4.59)
\end{aligned}
$$

where (4.57) holds because V_{CY} and V_Y are asymptotically independent and (4.58) holds because V_{CY} and V_Y are asymptotically independent.

Since the information leakage is considered as the total information obtained subtracted from the total uncertainty, the following holds for the four cases considered in this section:

$$\begin{aligned} L_{V_X,V_Y}^{X^K} &= H(X^K) - H(X^K|V_X,V_Y) \\ &\leq H(X^K) - H(V_{CX}) - H(V_{CY}) + \delta \end{aligned} \tag{4.60}$$

which proves (4.35).

$$\begin{aligned} L_{V_{CX},V_{CY}}^{X^K} &= H(X^K) - H(X^K|V_{CX},V_{CY}) \\ &\leq H(X^K) - H(V_X) + \delta \end{aligned} \tag{4.61}$$

which proves (4.36).

$$\begin{aligned} L_{V_{CX},V_{CY},V_Y}^{X^K} &= H(X^K) - H(X^K|V_{CX},V_{CY},V_Y) \\ &\leq H(X^K) - H(V_X) + \delta \end{aligned} \tag{4.62}$$

which proves (4.37).

The two bounds for $H(V_{CY},V_Y)$ are given by (4.56) and (4.59). From (4.56):

$$\begin{aligned} L_{V_Y,V_{CY}}^{X^K} &\geq H(X^K) - [H(X) - H(V_{CY}) + \delta] \\ &\geq H(V_{CY}) - \delta \end{aligned} \tag{4.63}$$

and from (4.59):

$$\begin{aligned} L_{V_Y,V_{CY}}^{X^K} &\leq H(X^K) - (H(V_X) + H(V_{CX}) - \delta) \\ &\leq H(X^K) - H(V_X) - H(V_{CX}) + \delta \end{aligned} \tag{4.64}$$

Combining these results from (4.63) and (4.64) gives (4.38).

This section details one method for analyzing the security of the system. The Shannon cipher system, which is used to determine transmission and key rate bounds for perfect secrecy is another avenue explored and the approach follows in the next section.

4.3 Shannon's Cipher System Approach For Multiple Correlated Sources

This section details a novel masking method to minimize the key length and thereafter incorporates Shannon's cipher system with the multiple correlated source model.

The masking method encompasses masking the conditional entropy portion with a mutual information portion. By masking, certain information is hidden and it becomes more difficult to obtain the information that has been masked. Masking can typically be done using random numbers, however the need for random numbers that represent keys is eliminated. Here a common information is used to mask with.

The following assumptions are made:

- The capacity of each link cannot be exhausted using this method.
- A common information is used to mask certain private information. Further, private information that needs to be masked always exists in this method.

The allocation of common information for transmission is done on an arbitrary basis. The objective of this subsection is to minimize the key lengths while achieving perfect secrecy.

The private information for source i is given by $H(S_i|\mathbf{S}_{\setminus S_i})$ according to (4.1), which is called W_{S_i} and the common information associated with source S_i is given by W_{CS_i}. First, choose a common information with which to mask. Then take a part of W_{S_i}, i.e. ${W_{S_i}}'$, that has entropy equal to $H(W_{CS_i})$ and mask as follows:

$$W_{S_i}^{'} \oplus W_{CS_i} \tag{4.65}$$

When the exclusive-or of the two sequences is performed the result is a single sequence that may look different to the original sequences. Thereafter the masked portion is transmitted instead of the $W_{S_i}^{'}$ portion when transmitting W_{S_i} thus providing added security. If Y is secure then this common information can be transmitted along Y's channel, which ensures the information is kept secure. The ability to mask using the common information is a unique and interesting feature of this new model for multiple correlated sources. The underlying principle is that the secure link should transmit more common information after transmitting the private information.

The lower bound for the channel rate when the masking approach is used is given by:

$$R_i^M \geq H(S_1, \ldots, S_n) - \sum_{t=2}^{n} \sum_{\text{all possible } \mathbf{S}_t} (t-1) I(\mathbf{S}_t | \mathbf{S}_t^c) \tag{4.66}$$

where R_i^M is the ith channel rate when masking is used.

The method works theoretically but may result in some concern practically as there may be a security compromise when common information is sent across non secure links. If the W_{CS_i} component used for masking has been compromised then the private portion it masked will also be compromised. A method to overcome this involves using two common information parts for masking. Equation (4.65) representing the masking would become:

$$W_{S_i}^{'} \oplus W_{CS_i} \oplus W_{CS_j} \tag{4.67}$$

where $i \neq j$ and both W_{CS_i} and W_{CS_j} are common information associated with source S_i. This way, if only W_{CS_j} is compromised then W_{S_i} is not compromised as it is still protected by W_{CS_i}. Here, combinations of common information are used to increase the security.

The Shannon's cipher system for this multiple source model is now presented in order to determine the rate regions for perfect secrecy. The multiple sources each have their own encoder and there is a universal decoder. Each source has an encoder represented by:

$$\begin{aligned} E_i : \mathcal{S} \times I_{W_{S_i}} \quad \rightarrow \quad & I_{W_{CS_i}} = \{0, 1, \ldots, W_{S_i} - 1\} \\ & I_{W_{CS_i}} = \{0, 1, \ldots, W_{CS_i} - 1\} \end{aligned} \tag{4.68}$$

where $I_{W_{S_i}}$ is the alphabet representing the private portion for source S_i and $I_{W_{CS_i}}$ is the alphabet representing the common information for source S_i. The decoder at the receiver is defined as:

$$D : (I_{W_{S_i}}, I_{W_{CS_i}}) \quad \times \quad I_{Mk} \rightarrow \mathcal{S} \tag{4.69}$$

The encoder and decoder mappings are below:

$$W_i = F_{E_i}(S_i, W_{ki}) \tag{4.70}$$

$$\widehat{S}_i = F_{D_i}(W_i, W_{ki}, W_{\{kp\}}) \tag{4.71}$$

where $p = 1, \ldots, n$, $p \neq i$ and $W_{\{kp\}}$ represents the set of common information required to determine S_i, and $\widehat{S}_i$ is the decoded output.

The following conditions should be satisfied for the general cases:

$$\frac{1}{K} \log W_{S_i} \leq R_i + \epsilon \tag{4.72}$$

$$\frac{1}{K} \log M_{ki} \leq R_{ki} + \epsilon \tag{4.73}$$

$$\Pr\{\widehat{S}_i \neq S_i\} \leq \epsilon \tag{4.74}$$

$$\frac{1}{K}H(S_i|W_i) \leq h_i - \epsilon \tag{4.75}$$

$$\frac{1}{K}H(S_j|W_i) \leq h_j - \epsilon \tag{4.76}$$

where R_i is the the rate of source S_i's channel and R_{k_i} is the key rate of S_i. The security levels, for source i and any other source j are measured uncertainties h_i and h_j respectively.

The general cases considered are:

Case 1: When T_{S_i} is leaked and S_i needs to be kept secret.

Case 2: When T_{S_i} is leaked and S_j needs to be kept secret.

The admissible rate region for each case is defined as follows:

Definition 1a: (R_i, R_{ki}, h_i) is admissible for case 1 if there exists a code (F_{E_i}, F_D) such that (4.72) - (4.75) hold for any $\epsilon \to 0$ and sufficiently large K.

Definition 1b: (R_i, R_{ki}, R_j, R_{kj}, h_i, h_j) is admissible for case 2 if there exists a code (F_{E_i}, F_D) such that (4.72) - (4.74) and (4.76) hold for any $\epsilon \to 0$ and sufficiently large K.

Definition 2: The admissible rate regions are defined as:

$$\begin{aligned} \mathcal{R}(h_i) = \{&(R_i, R_{ki}) : \\ &(R_i, R_{ki}, h_i) \text{ is admissible for case 1}\} \end{aligned} \tag{4.77}$$

$$\begin{aligned} \mathcal{R}(h_i, h_j) = \{&(R_i, R_{ki}, R_j, R_{kj}) : \\ &(R_i, R_{ki}, R_j, R_{kj}, h_j) \text{ is admissible for case 2}\} \end{aligned} \tag{4.78}$$

The admissible regions give an indication of the rate regions for this scenario. The regions are derived for the more specific cases in Chapters 5-6, which are developed using this method. The information leakage described in the Slepian-Wolf aspect indicates the common information that should be secured to ensure less information leakage.

4.4 Shannon's Cipher System Approach for Two Correlated Sources

The Shannon's cipher system approach for two independent correlated sources (depicted in Figure 4.4) is detailed in this section. The source outputs are i.i.d random variables X and Y, taking on values in the finite sets $\mathcal{X}$ and $\mathcal{Y}$. Both the transmitter and receiver have access to the key, a random variable, independent of X^K and Y^K and taking values in $I_{M_k} = \{0, 1, 2, \ldots, M_k - 1\}$. The sources X^K and Y^K compute the ciphertexts W_1 and W_2, which are the result of specific encryption functions on the plaintext from X and Y respectively. The encryption functions are invertible, thus knowing W_1 and the corresponding key k_X, X can be retrieved. The key for Y is represented as k_Y.

The mutual information between the plaintext and ciphertext should be small so that the wiretapper cannot gain much information about the plaintext. For perfect secrecy, this mutual information should be zero, then the length of the key should be at least the length of the plaintext.

The encoder functions for X and Y, (E_X and E_Y respectively) are given as:

$$\begin{aligned} E_X : \mathcal{X}^K \times I_{M_{kX}} \quad \rightarrow \quad & I_{M'_X} = \{0, 1, \ldots, M'_X - 1\} \\ & I_{M'_{CX}} = \{0, 1, \ldots, M'_{CX} - 1\} \end{aligned} \tag{4.79}$$

$$\begin{aligned} E_Y : \mathcal{Y}^K \times I_{M_{kY}} \quad \rightarrow \quad & I_{M'_Y} = \{0, 1, \ldots, M'_Y - 1\} \\ & I_{M'_{CY}} = \{0, 1, \ldots, M'_{CY} - 1\} \end{aligned} \tag{4.80}$$

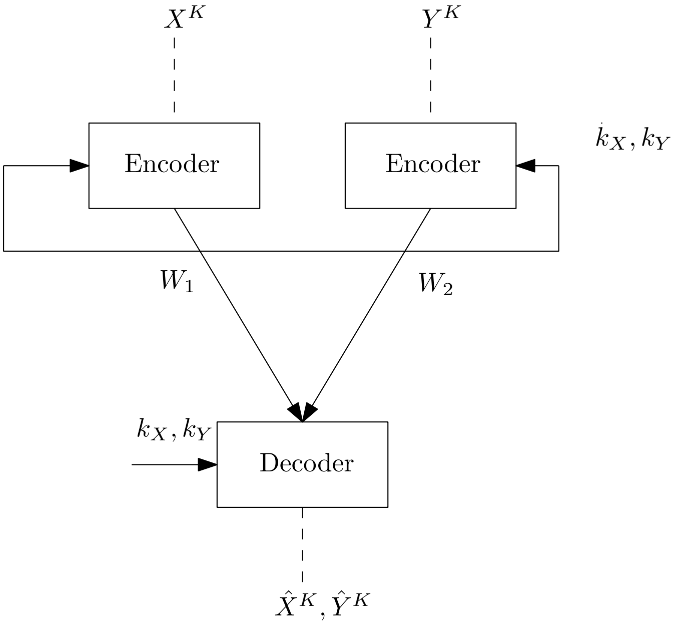

Figure 4.4: Shannon cipher system for two correlated sources

The decoder is defined as:

$$\begin{aligned} D_{XY} : (I_{M'_X}, I_{M'_Y}, I_{M'_{CX}}, I_{M'_{CY}}) &\times I_{M_{kX}}, I_{M_{kY}} \\ &\rightarrow \mathcal{X}^K \times \mathcal{Y}^K \end{aligned} \tag{4.81}$$

The encoder and decoder mappings are below:

$$W_1 = F_{E_X}(X^K, W_{kX}) \tag{4.82}$$

$$W_2 = F_{E_Y}(Y^K, W_{kY}) \tag{4.83}$$

$$\widehat{X}^K = F_{D_X}(W_1, W_2, W_{kX}) \tag{4.84}$$

$$\widehat{Y}^K = F_{D_Y}(W_1, W_2, W_{kY}) \tag{4.85}$$

or

$$(\widehat{X}^K, \widehat{Y}^K) = F_{D_{XY}}(W_1, W_2, W_{kX}, W_{kY}) \tag{4.86}$$

The following conditions should be satisfied for cases 1- 4:

$$\frac{1}{K} \log M_X \leq R_X + \epsilon \tag{4.87}$$

$$\frac{1}{K} \log M_Y \leq R_Y + \epsilon \tag{4.88}$$

$$\frac{1}{K} \log M_{kX} \leq R_{kX} + \epsilon \tag{4.89}$$

$$\frac{1}{K} \log M_{kY} \leq R_{kY} + \epsilon \tag{4.90}$$

$$\Pr\{\widehat{X}^K \neq X^K\} \leq \epsilon \tag{4.91}$$

$$\Pr\{\widehat{Y}^K \neq Y^K\} \leq \epsilon \tag{4.92}$$

$$\frac{1}{K}H(X^K|W_1) \leq h_X + \epsilon \tag{4.93}$$

$$\frac{1}{K}H(Y^K|W_2) \leq h_Y + \epsilon \tag{4.94}$$

$$\frac{1}{K}H(X^K, Y^K|W_1, W_2) \leq h_{XY} + \epsilon \tag{4.95}$$

where R_X is the rate of source X's channel and R_Y is the rate of source Y's channel. Here, (R_{kX}, R_{kY}) is the rate of the key channel when allocating a key to X and Y. The security level for X and Y are measured by the total and individual uncertainties, h_{XY} and (h_X, h_Y) respectively.

The cases 1 - 3 that are considered are as follows:
Case 1: When (W_1, W_2) is leaked and (X^K, Y^K) needs to be kept secret. The security level of concern is represented by $\frac{1}{K}H(X^K, Y^K|W_1, W_2)$.
Case 2: When (W_1, W_2) is leaked and (X^K, Y^K) needs to be kept secret. The security level of concern is represented by $(\frac{1}{K}H(X^K|W_1, W_2), \frac{1}{K}H(Y^K|W_1, W_2))$.
Case 3: When (W_1, W_2) is leaked and Y^K needs to be kept secret.The security level of concern is represented by $\frac{1}{K}H(Y^K|W_1, W_2)$.

The admissible rate region for each case is defined as follows:
Definition 1a: $(R_X,\ R_Y,\ R_{kX},\ R_{kY},\ h_{XY})$ is admissible for case 1 if there exists a code $(F_{E_X},\ F_{D_{XY}})$ and $(F_{E_Y},\ F_{D_{XY}})$ such that (4.87) - (4.92) and (4.95) hold for any $\epsilon \to 0$ and sufficiently large K.
Definition 1b: $(R_X,\ R_Y,\ R_{kX},\ R_{kY},\ h_X,\ h_Y)$ is admissible for case 2 if there exists a code $(F_{E_X},\ F_{D_{XY}})$ and $(F_{E_Y},\ F_{D_{XY}})$ such that (4.87) - (4.94) hold for any $\epsilon \to 0$ and sufficiently large K.
Definition 1c: $(R_X,\ R_Y,\ R_{kX},\ R_{kY},\ h_Y)$ is admissible for case 3 if there exists a code

$(F_{E_Y},\ F_{D_{XY}})$ such that (4.87) - (4.92) and (4.94) hold for any $\epsilon \to 0$ and sufficiently large K.

Definition 2: The admissible rate regions of $\mathcal{R}_j$ for case j are defined as:

$$\begin{aligned} \mathcal{R}_1(h_{XY}) = \{(R_X, R_Y, R_{kX}, R_{kY}) : \\ (R_X, R_Y, R_{kX}, R_{kY}, h_{XY}) \text{ is admissible for case } 1\} \end{aligned} \tag{4.96}$$

$$\begin{aligned} \mathcal{R}_2(h_X, h_Y) = \{(R_X, R_Y, R_{kX}, R_{kY}) : \\ (R_X, R_Y, R_{kX}, R_{kY}, h_X, h_Y) \text{ is admissible for case } 2\} \end{aligned} \tag{4.97}$$

$$\begin{aligned} \mathcal{R}_3(h_Y) = \{(R_X, R_Y, R_{kX}, R_{kY}) : \\ (R_X, R_Y, R_{kX}, R_{kY}, h_Y) \text{ is admissible for case } 3\} \end{aligned} \tag{4.98}$$

Theorems for these regions have been developed:

Theorem 2: For $0 \le h_{XY} \le H(X,Y)$,

$$\begin{aligned} &\mathcal{R}_1(h_{XY}) = \{(R_X, R_Y, R_{kX}, R_{kY}) : \\ &R_X \ge H(X|Y), \\ &R_Y \ge H(Y|X), \\ &R_X + R_Y \ge H(X,Y) \\ &R_{kX} + R_{kY} \ge h_{XY}\} \end{aligned} \tag{4.99}$$

Theorem 3: For $0 \leq h_X \leq H(X)$ and $0 \leq h_Y \leq H(Y)$,

$$\begin{aligned}
&\mathcal{R}_2(h_Y) = \{(R_X, R_Y, R_{kX}, R_{kY}) : \\
&R_X \geq H(X|Y), \\
&R_Y \geq H(Y|X), \\
&R_X + R_Y \geq H(X, Y) \\
&R_{kX} + R_{kY} \geq \max(h_X, h_Y)\}
\end{aligned} \tag{4.100}$$

When $h_X = 0$ then case 3 can be reduced to that depicted in (4.100). Hence, Corollary 1 follows:

Corollary 1: For $0 \leq h_Y \leq H(Y)$, $\mathcal{R}_3(h_Y) = \mathcal{R}_2(0, h_Y)$

The direct and converse parts of the proofs for (4.99) and (4.100) are contained in Appendix A.

4.5 Information Leakage for the System using Matrix Partitions

In this section the aim is to determine the equivocation (uncertainty) in retrieving a message from the transmitted channel information. The convention used by Stankovic *et al.* [58] is followed to present an example together with a method incorporating generator matrix ranks put forth by Luo *et al.* [47] to determine the equivocation. The Hamming distance is represented as follows: $d_H(X^K, Y^K) \leq 1$.

The following generator matrix G is used:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

The matrix takes the form: $G = [I_k P^T]$ and here I_k is the identity matrix of order k and P^T is made up of two 2×3 matrices in this case.

Suppose the messages to send across the channels for X and Y are given by: $x = [a_1\ v_1\ q_1] = [10\ 11\ 001]$ and $y = [u_2\ a_2\ q_2] = [10\ 11\ 011]$.

There is compression along X's and Y's channel. As per the matrix partition method the syndrome for X and Y is comprised of:

$$T_X = \begin{bmatrix} v_1^T \\ P_1^T a_1^T \oplus q_1^T \end{bmatrix}$$

$$T_Y = \begin{bmatrix} u_2^T \\ P_2^T a_2^T \oplus q_2^T \end{bmatrix}$$

where P_1^T is the G matrix transpose of rows 1-2 and columns 5-7 and P_2^T is the G matrix transpose of rows 3-4 and columns 5-7. The generator matrices used by X and Y to achieve these syndromes are G_X and G_Y respectively.

$$G_X = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$G_Y = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

This results in syndromes of [1 1 1 0 0] for X and [1 0 1 1 1] for Y.

Here, the equivocation for these cases can be found using the G matrix specified above and a sub matrix of G. This follows from Luo *et al.* [47], where the equivocation is given by: $\triangle_{Y|T_Y} = \text{rank}(G) - \text{rank}(G_Y)$. Here, $\triangle_{Y|T_Y}$ is the equivocation on Y given T_Y.

Next, the information leakage for each of the following cases is analyzed:

- The equivocation on (X^K, Y^K) when (T_X, T_Y) is leaked
- The equivocation on (X^K, Y^K) when T_X is leaked
- The equivocation on (X^K, Y^K) when T_Y is leaked

In order to show the most representative results for each of the cases the scenarios contributing to the minimum and maximum information leakage have been considered.

Before the information leakage method is described certain variables are introduced. Here, μ_{T_X} and μ_{T_Y} represent the number of wiretapped bits from T_X and T_Y respectively. The length of the information bits from each syndrome is represented as l_i^X and l_i^Y for X^K and Y^K respectively. The length of parity bits with respect to X^K or Y^K is denoted as l_p, and the following can be developed: $l_i^X + l_i^Y + 2l_p$ is the overall length of T_X and T_Y. Hence we have: $0 \leq \mu_{T_X} \leq l_i^X + l_p$ and $0 \leq \mu_{T_Y} \leq l_i^Y + l_p$.

Note that the leakage is determined using a combination of the information bits, parity bits and the parity matrix H rank. The H matrix rank is used to determine how much of information is leaked from the wiretapped bits when the columns corresponding to the wiretapped bits have been removed. Let H' denote the H matrix with the wiretapped columns removed.

The case for the leakage on (X^K, Y^K) when (T_X, T_Y) is leaked is now considered. Initially the maximum leakage is described. When $\mu_{T_X} \leq l_i^X$ and $\mu_{T_Y} \leq l_i^Y$, the maximum leakage is $\mu_{T_X} + \mu_{T_Y} + \text{rank}(H) - \text{rank}(H')$. This considers when the information bits (namely v_1 and u_2) have been leaked only.

For this example the syndromes can leak a maximum of two information bits each, and a combined leakage of four bits. For each information bit wiretapped there is one bit of information leaked about X^K and Y^K. Since the rank of H' remains as three for when each of these bits are wiretapped, the information leakage is determined by the information bits entirely. This can be seen in the maximum case in Figure 4.6 for the first four wiretapped bits.

Next, $\mu_{T_X} > l_i^X$ and $\mu_{T_Y} > l_i^Y$ is considered. This case considers when more than the information bits are wiretapped. For this case $\min(\mu_{T_X} - l_i^X, \mu_{T_Y} - l_i^Y)$ parity bits can be from the corresponding positions in $P_1^T a_1^T \oplus q_1^T$ and $P_2^T a_2^T \oplus q_2^T$. Therefore, the maximum leakage is as indicated in (4.101).

$$l_i^X + l_i^Y + \mu_{T_X} + \min(\mu_{T_X} - l_i^X, \mu_{T_Y} - l_i^Y) + \text{rank}(H) - \text{rank}(H') \tag{4.101}$$

If $\mu_{T_X} > l_i^X$ and $\mu_{T_Y} \leq l_i^Y$ the maximum leakage is $\mu_{T_Y} + l_i^X + \text{rank}(H) - \text{rank}(H')$; if $\mu_{T_X} \leq l_i^X$ and $\mu_{T_Y} > l_i^Y$, the maximum leakage is $\mu_{T_X} + l_i^Y + \text{rank}(H) - \text{rank}(H')$.

The parity bits only leak information about X^K and Y^K when the positions wiretapped correspond. If the last parity bit in T_X is wiretapped and the last parity bit in T_Y is wiretapped then since these wiretapped bits are in corresponding positions there will be one bit leaked about X^K and Y^K. As such, for the maximum leakage the parity bits should be placed in corresponding positions, as indicated by the 'x' positions in Figure 4.5. For this example the information leakage between 5 - 10 wiretapped bits increases by one bit for every two bits wiretapped. This is because these are the parity bits of concern and there is one bit of information leaked for every pair of corresponding parity bits wiretapped. The rank of H' also increases by one for every two bits wiretapped for these 5 - 10 wiretapped bits. Thus the information leakage increases by one for every pair of parity bits and by a further one for every pair of parities as there is a change at these points in the H' matrix rank.

Now the minimum leakage is considered. When $\mu_{T_X} \leq l_p$ and $\mu_{T_Y} \leq l_p$, the minimum leakage is $\max(0, \mu_{T_X} + \mu_{T_Y} - l_p) + \text{rank}(H) - \text{rank}(H')$. This considers when the parity bits (namely $P_1^T a_1^T \oplus q_1^T$ and $P_2^T a_2^T \oplus q_2^T$) have been leaked only. Otherwise, the minimum leakage is $\mu_{T_X} + \mu_{T_Y} - l_p + \text{rank}(H) - \text{rank}(H')$.

To achieve the minimum information leakage the wiretapped parity bits should not correspond, which is shown by the 'o' positions in Figure 4.5. This means that three bits may be wiretapped (all parity and not corresponding bits, for example all of T_X's

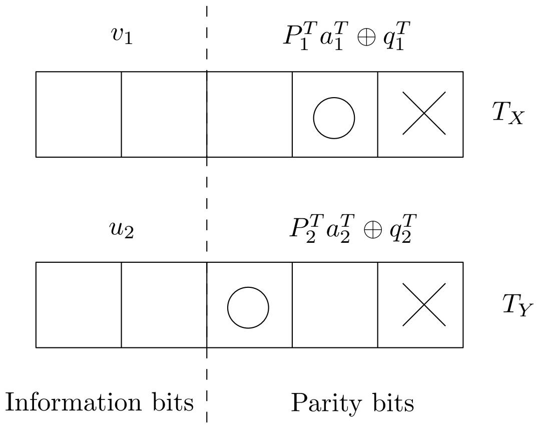

FIGURE 4.5: Wiretapped parity bits for maximum and minimum information leakage

parity bits) before the information leakage starts. The fourth wiretapped bit could match a corresponding parity bit or be an information bit; both of which will result in one bit of information leakage. The same follows for the fifth to seventh wiretapped bits. When the eighth bit is wiretapped the minimum case is where all the parity bits correspond (i.e. 6 bits) and there are two information bits wiretapped; at this point the information leakage rises by two bits. Until this point the rank of H' was three, hence it would not affect the information leakage. An additional one bit of information leakage when this eighth bit is wiretapped comes from the rank of H' changing by one. Thereafter there are two bits of information leakage for each wiretapped bit. This comes from the one information bit leaked and the rank of H' increasing by one for each of the ninth and tenth wiretapped bits. This is depicted as the minimum case in Figure 4.6.

Next the information leakage for the second and third cases are determined. The leakage for these cases reach the same limit for the minimum and maximum cases of information leakage, however the information leakage peak occurs at different points depending on which bits (information or parity) are leaked first. The leakage for the second and third cases respectively are as follows: $L_{T_X}^{X^K,Y^K} = l_i^X$ and $L_{T_Y}^{X^K,Y^K} = l_i^Y$. Using the numerical example for this section, the graphical representation is in Figure 4.7. If the parity bits of either T_X or T_Y are wiretapped, then there is no information leakage as there are no corresponding parity bits to match with and to allow for information leakage. This is shown in Figure 4.7 as the wiretapped bits 3-5 for the maximum case and the wiretapped bits 1-3 for the minimum case. When the information bits are wiretapped there is one bit of leakage for each information bit, thus resulting in two bits of leakage when both information bits from T_X or T_Y have been wiretapped. This is shown in Figure 4.7

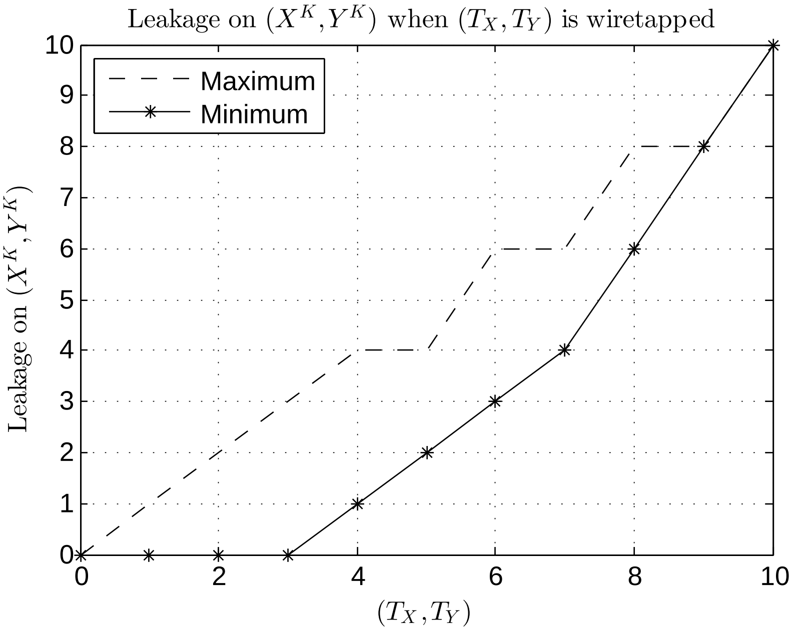

FIGURE 4.6: The information leakage on (X^K, Y^K) when (T_X, T_Y) has been wiretapped

as the wiretapped bits 1-2 for the maximum case and the wiretapped bits 4-5 for the minimum case. The maximum case depicted is when the information bits are initially wiretapped and the minimum case is where the parity bits are initially wiretapped.

In this example certain bits have more equivocation than others and as such which bits are wiretapped plays a role in making the system vulnerable at different times. For instance, following from the third case if only T_Y is wiretapped from the parity bits then for the first 3 bits there is no information leakage due to T_Y as the wiretapper would have encountered the masked bits. The information leakage occurs after the third bit, when u_2 is wiretapped. This therefore shows an upper and lower bound on the uncertainty, where the upper bound is given when bits u_2 is leaked first and the lower bound is given when the masked portion is first leaked. The parity bits are masked and are thus more difficult to be leaked to an adversary. Parity bits from both sources need to be wiretapped and in the same positions in order to leak information.

In general, for a systematic code the columns that have a weight of one would contribute

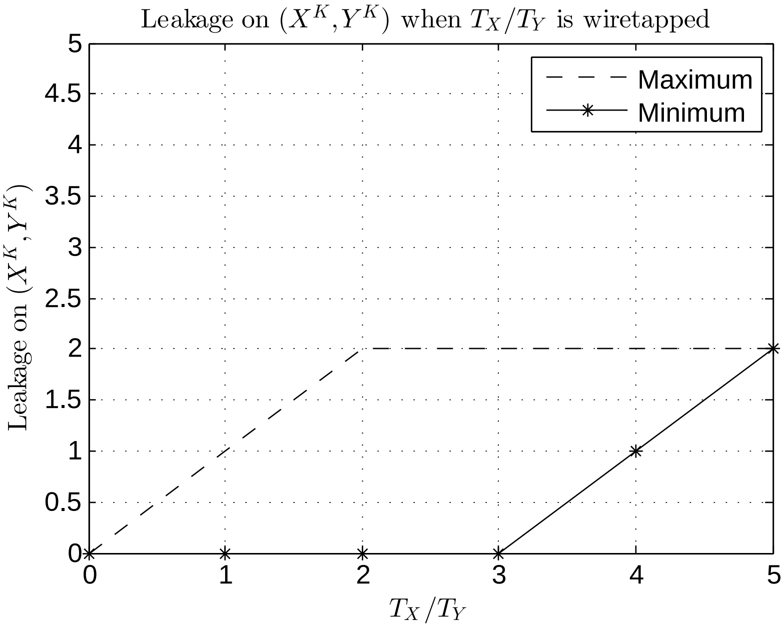

Figure 4.7: The information leakage on (X^K,Y^K) when T_X or T_Y has been wiretapped

one bit to the information leakage entirely. With use of the matrix partition approach, if the parity bits of both T_X and T_Y are wiretapped (and these bits are from the same columns in each generator matrix) then for every two parity bits wiretapped there is one bit of information leaked. The parity bits and the information bits can also be used to solve the parity matrix to determine the information leakage. If the wiretapped parity bits do not belong to the same columns then there is no information leakage at that point.

This chapter introduces a multiple correlated source model followed by a novel two correlated source model. The security aspects of the two correlated source model has been analyzed and a masking method to reduce on the length of keys required has been presented. The security aspects make use of existing techniques using the Slepian-Wolf scenario and Shannon's cipher system approach to show the information leakage bounds for the novel model and rate regions required to achieve perfect secrecy respectively. The chapter ends with an aspect showing the coding approach that demonstrates practical implementation for such a model.

Chapter 5

Information Leakage of Slepian-Wolf Encoded Sequences for Two Correlated Sources with Partially Predetermined Information

This chapter describes a novel two correlated source model where some source information has been leaked to a wiretapper. It caters for applications used in degraded broadcast channels and scenarios where there is pre-existing information available to an eavesdropper. This model is a variation of the two correlated source model investigated in the previous chapter. Here a main contribution is the development of the two correlated source model. The two approaches explored to investigate the information leakage have been used here; one quantifying the information leakage for the Slepian-Wolf scenario and the other incorporating Shannon's cipher system. These security aspects of the two correlated source model is also a contribution. The chapter again ends with a section showing the coding implementation for this model, which is an important contribution as it shows practical implementation for the novel model developed and provides an important link between the information theory and coding theory fields.

5.1 Two Correlated Source Model with Partially Predetermined Information

The independent, identically distributed (i.i.d.) sources X and Y are mutually correlated random variables, depicted in Figure 5.1. The alphabet sets for sources X and Y are represented by $\mathcal{X}$ and $\mathcal{Y}$ respectively. Assume that $(X^K,\ Y^K)$ are encoded into two syndromes (T_X and T_Y). The compressed representation is as follows: $T_X = (V_X, V_{CX})$ and $T_Y = (V_Y, V_{CY})$ where T_X and T_Y are the syndromes of X and Y. Here, T_X and T_Y are characterized by (V_X, V_{CX}) and (V_Y, V_{CY}) respectively. The Venn diagram in Figure 4.3 may again be used to illustrate this idea where it is shown that V_X and V_Y represent the private information of sources X and Y respectively and V_{CX} and V_{CY} represent the common information between X^K and Y^K generated by X^K and Y^K respectively. Each source is composed of two components; X^{K_1} and X^{K_2} for X^K and Y^{K_1} and Y^{K_2} for Y^K, of which one component is leaked to the eavesdropper. Here, the lengths K_1 and K_2 are related to K as follows: $K_1 + K_2 = K$. Due to the stationary nature of the sources, if Y^{K_2} is known by the wiretapper then it corresponds to X^{K_2} known about X^K as the wiretapper has access to certain common information between the sources.

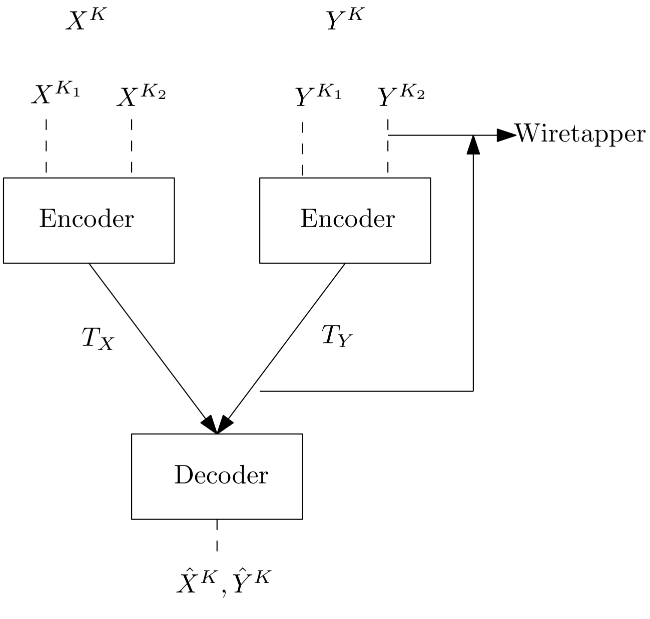

Figure 5.1: Correlated source coding for two sources with a more powerful adversary

In the same way as was described for the two correlated source model presented in Chapter 4, the correlated sources X and Y transmit messages (in the form of syndromes) to the receiver along the wiretapped links. The decoder determines X and Y only after receiving all of T_X and T_Y. The eavesdropper has access to either the common or private portion represented by (T_X, T_Y) and some data symbols from the corresponding source (Y^{K_2}). The effect is that the eavesdropper has access to some compressed information (that is transmitted across the communication link after encoding) and some uncompressed information (i.e. the source's data symbols). There is a mapping/function that describes the relation between the uncompressed information and the compressed information. This implies that certain source bits correspond to certain compressed bits transmitted as channel information. It is valuable to determine how much of information the eavesdropper has access to when wiretapping the private or common information portions (this is described in the next section).

Here, typical set encoding and decoding is used. We are able to determine bin indices for the jointly typical sequence from the indices passed over the communication channel. When common or private information from a particular link is wiretapped it gives an indication of which rows/columns in the specific look up table the sequence is contained within. With additional information the uncertainty of which row/column to look to for the codeword is reduced as it helps to narrow the number of possible codewords. In this way, all the codewords having the same sequence as the wiretapped source bits will be shortlisted codewords.

The code described in this section satisfies the following inequalities for $\delta > 0$ and sufficiently large K.

$$Pr\{X \neq G(V_X, V_{CX}, V_{CY})\} \leq \delta \tag{5.1}$$

$$Pr\{Y \neq G(V_Y, V_{CX}, V_{CY})\} \leq \delta \tag{5.2}$$

$$H(V_X, V_{CX}, V_{CY}) \leq H(X) + \delta \tag{5.3}$$

$$H(V_Y, V_{CX}, V_{CY}) \leq H(Y) + \delta \tag{5.4}$$

$$H(V_X, V_Y, V_{CX}, V_{CY}) \leq H(X, Y) + \delta \tag{5.5}$$

$$H(X^K|V_X, V_Y) \geq H(V_{CX}) + H(V_{CY}) - \delta \tag{5.6}$$

$$H(X^K|V_{CX}, V_{CY}) \geq H(V_X) + H(V_{CY}) - \delta \tag{5.7}$$

$$H(X^K|V_{CX}, V_{CY}, V_Y) \geq H(V_X) + H(V_{CY}) - \delta \tag{5.8}$$

$$\begin{aligned} H(V_{CX}) + H(V_X) - \delta &\leq H(X^K|V_{CY}, V_Y) \\ &\leq H(X^K) - H(V_{CY}) + \delta \end{aligned} \tag{5.9}$$

where G is a function to define the decoding process at the receiver. It can intuitively be seen from (5.3) and (5.4) that X and Y are recovered from the corresponding private information and the common information produced by X^K and Y^K. Equations (5.3), (5.4) and (5.5) show that the private information and common information produced by each source should contain no redundancy.

The prototype code described in Lemma 1 in Section 4.2 and the encoding and decoding methods are also applied in this section.

In order to determine the security of the system, the measure introduced in Section 4.2 for the amount of information leaked is used. The obtained information subtracted from the total uncertainty is used to determine the information leakage.

The information leakage bounds for the following cases are provided in (5.10) - (5.12):

- Leakage on Y when (V_Y, Y^{K_2}) is wiretapped
- Leakage on Y when (V_{CY}, Y^{K_2}) is wiretapped
- Leakage on X when (V_{CY}, Y^{K_2}) is wiretapped

$$\begin{aligned} L^{Y^K}_{V_Y,Y^{K_2}} &\leq H(Y^K|X^K) - H(V_Y) + I(V_Y;Y^K) \\ &+ H(Y^{K_2}|V_Y) + \delta \end{aligned} \tag{5.10}$$

$$\begin{aligned} L^{Y^K}_{V_{CY},Y^{K_2}} &\leq H(Y^K|X^K) - H(V_Y) + I(V_{CY};Y^K) \\ &+ H(Y^{K_2}|V_{CY}) + \delta \end{aligned} \tag{5.11}$$

$$\begin{aligned} L^{X^K}_{V_{CY},Y^{K_2}} &\leq H(X^K|Y^K) - H(V_X) \\ &+ I(X^K;Y^{K_2}|V_{CY}) + I(V_{CY};X^K) \\ &+ \delta \end{aligned} \tag{5.12}$$

As indicated in Figure 5.1, Y^{K_2} is used to represent the source bits that have been wiretapped. This could be common information that relates to X^K or private information of X^K. Equation (5.12) gives an indication of the minimum and maximum amount of leaked information for the interesting case where the channel information and data symbols have been wiretapped and its information leakage on the alternate source is quantified. This is interesting because intuitively it is known that there is some information that may be leaked by an alternate source. For this case, the common information V_{CX} and V_{CY} can thus be secured to reduce the amount of information leaked. The bounds developed in (5.10) - (5.12) are proven below. These are also described in [62].

The code (V_X, V_{CX}, V_{CY}, V_Y) that has been defined in Chapter 4 describing the model exists, and (5.1) - (5.5) satisfy (5.6) - (5.9), which have already been proven in Chapter 4, then the information leakage bounds for this scenario with a more powerful adversary is given by (5.10) - (5.12).

Proof for (5.10): First, $H(Y^K|V_Y, Y^{K_2})$ is determined.

$$\begin{aligned}
& H(Y^K|V_Y, Y^{K_2}) \\
= \; & H(Y^K, V_Y, Y^{K_2}) - H(V_Y, Y^{K_2}) \\
= \; & H(Y^K) + H(V_Y|Y^K) + H(Y^{K_2}|Y^K, V_Y) \\
- \; & H(V_Y, Y^{K_2}) \qquad (5.13) \\
= \; & H(Y^K) + H(V_Y) - I(V_Y; Y^K) + H(Y^{K_2}) \\
- \; & I(Y^{K_2}; Y^K|V_Y) - I(Y^{K_2}; V_Y) - H(V_Y|Y^{K_2}) \\
- \; & I(V_Y; Y^{K_2}) - H(Y^{K_2}|V_Y) \\
= \; & H(Y^K) + H(V_Y) - I(V_Y; Y^K) + H(Y^{K_2}) \\
- \; & H(Y^{K_2}|V_Y) - I(Y^{K_2}; V_Y) - H(V_Y) \\
+ \; & I(V_Y; Y^{K_2}) - I(V_Y; Y^{K_2}) - H(Y^{K_2}) \\
+ \; & H(Y^{K_2}|V_Y) \\
= \; & H(Y^K) - I(V_Y; Y^K) - I(Y^{K_2}; Y^K|V_Y) \\
\geq \; & H(V_Y) + H(V_{CX}) + H(V_{CY}) - I(V_Y; Y^K) \\
- \; & H(Y^{K_2}|V_Y) - \delta \qquad (5.14) \\
= \; & H(V_Y) + I(X^K; Y^K) - I(V_Y; Y^K) - H(Y^{K_2}|V_Y) \\
- \; & \delta \qquad (5.15)
\end{aligned}$$

where (5.13) holds from the entropy chain rule, (5.14) holds from (5.4), and (5.15) holds from Theorem 1.

The information leakage is thus:

$$\begin{aligned}
L^{Y^K}_{V_Y,Y^{K_2}} &= H(Y^K) - H(Y^K|V_Y,Y^{K_2}) \\
&\leq H(Y^K) - H(V_Y) - I(X^K;Y^K) + I(V_Y;Y^K) \\
&+ H(Y^{K_2}|V_Y) + \delta \\
&= H(Y^K|X^K) - H(V_Y) + I(V_Y;Y^K) \\
&+ H(Y^{K_2}|V_Y) + \delta \qquad (5.16)
\end{aligned}$$

which proves (5.10).

Proof for (5.11):

$$\begin{aligned}
& H(Y^K|V_{CY},Y^{K_2}) \\
=\ & H(Y^K,V_{CY},Y^{K_2}) - H(V_{CY},Y^{K_2}) \\
=\ & H(Y^K) + H(V_{CY}|Y^K) + H(Y^{K_2}|Y^K,V_{CY}) \\
-\ & [H(V_{CY}|Y^{K_2}) + I(V_{CY};Y^{K_2}) \\
+\ & H(Y^{K_2}|V_{CY})] \qquad (5.17) \\
=\ & H(Y^K) + H(V_{CY}) - I(V_{CY};Y^K) + H(Y^{K_2}) \\
-\ & I(Y^{K_2};Y^K|V_{CY}) - I(Y^{K_2};V_{CY}) \\
-\ & H(V_{CY}) + I(V_{CY};Y^{K_2}) - I(V_{CY};Y^{K_2}) \\
-\ & H(Y^{K_2}) + I(V_{CY};Y^{K_2}) \\
=\ & H(Y^K) - I(V_{CY};Y^K) - H(Y^{K_2}|V_{CY}) \\
\geq\ & H(V_Y) + H(V_{CX}) + H(V_{CY}) \\
-\ & I(V_{CY};Y^K) - H(Y^{K_2}|V_{CY}) - \delta \qquad (5.18) \\
=\ & H(V_Y) + I(X^K;Y^K) - I(V_{CY};Y^K) \\
-\ & H(Y^{K_2}|V_{CY}) - \delta \qquad (5.19)
\end{aligned}$$

where (5.17) holds from the entropy chain rule, (5.18) holds from (5.4) and (5.19) holds from Theorem 1.

The information leakage is thus:

$$\begin{aligned}
L^{Y^K}_{V_{CY},Y^{K_2}} &= H(Y^K) - H(Y^K|V_{CY},Y^{K_2}) \\
&\leq H(Y^K) - H(V_Y) - I(X^K;Y^K) \\
&+ I(V_{CY};Y^K) + H(Y^{K_2}|V_{CY}) + \delta \\
&= H(Y^K|X^K) - H(V_Y) + I(V_{CY};Y^K) \\
&+ H(Y^{K_2}|V_{CY}) + \delta \qquad (5.20)
\end{aligned}$$

which proves (5.11).

Following a similar proof to those done above in this section, a bound for $H(X^K|V_{CY},V_{Y2})$ can be found as follows:

$$\begin{aligned}
& H(X^K|V_{CY},Y^{K_2}) \\
= \; & H(X^K,V_{CY},Y^{K_2}) - H(V_{CY},Y^{K_2}) \\
= \; & H(X^K) + H(V_{CY}|X^K) + H(Y^{K_2}|V_{CY},X^K) \\
- \; & H(V_{CY},Y^{K_2}) \qquad (5.21) \\
= \; & H(X^K) + H(V_{CY}) - I(V_{CY};X^K) + H(Y^{K_2}) \\
- \; & I(X^K;Y^{K_2}|V_{CY}) - I(Y^{K_2};V_{CY}) \\
- \; & H(V_{CY}|Y^{K_2}) - I(V_{CY};Y^{K_2}) \\
- \; & H(Y^{K_2}|V_{CY}) \qquad (5.22) \\
= \; & H(X^K) + H(V_{CY}) - I(V_{CY};X^K) + H(Y^{K_2}) \\
- \; & I(X^K;Y^{K_2}|V_{CY}) - I(Y^{K_2};V_{CY}) - H(V_{CY}) \\
+ \; & I(V_{CY};Y^{K_2}) - H(Y^{K_2}) + I(V_{CY};Y^{K_2}) \\
- \; & I(V_{CY};Y^{K_2}) \\
= \; & H(X^K) - I(X^K;Y^{K_2}|V_{CY}) - I(V_{CY};X^K) \\
\geq \; & H(V_X) + H(V_{CX}) + H(V_{CY}) \\
- \; & I(X^K;Y^{K_2}|V_{CY}) - I(V_{CY};X^K) - \delta \qquad (5.23) \\
= \; & H(V_X) + I(X^K;Y^K) - I(X^K;Y^{K_2}|V_{CY}) \\
- \; & I(V_{CY};X^K) - \delta \qquad (5.24)
\end{aligned}$$

where (5.21) and (5.22) results from the chain rule, (5.24) holds from Theorem 1, and (5.23) holds from (5.3).

The information leakage is thus:

$$\begin{aligned} L^{X^K}_{V_{CY},Y^{K_2}} &= H(X^K) - H(X^K|V_{CY}, Y^{K_2}) \\ &\leq H(X^K) - H(V_X) - I(X^K;Y^K) \\ &+ I(X^K;Y^{K_2}|V_{CY}) + I(V_{CY};X^K) + \delta \\ &= H(X^K|Y^K) - H(V_X) + I(X^K;Y^{K_2}|V_{CY}) \\ &+ I(V_{CY};X^K) + \delta \end{aligned} \tag{5.25}$$

which proves (5.12).

This section shows the information leakage when various portions of the channel information and some source data symbols are leaked. It is evident that the eavesdropper has more information about a particular source as shown in (5.20)-(5.25), than if only the channel information was wiretapped. This can be drawn from a comparison with the previous chapter. The interesting case explored for (5.12) demonstrates that there is common information leaked about X from the wiretapped Y's source symbols or the syndrome T_Y, due to the correlation between the sources.

Equation (5.10) in effect means that the information leakage is upper bounded by the common information between V_Y and the eavesdropped source data symbols and $H(Y^{K_2}|V_Y)$. The security level is therefore dependent on these portions. If these are secured then the information leakage will be less.

For (5.11), the common portion between V_{CY} and the eavesdropped source data symbols together with $H(Y^{K_2}|V_{CY})$ form the upper bound for the information leakage. In the same way as (5.10), increasing the security for these information portions ensures more information can remain secure.

Again, in (5.12) V_{CY} and the eavesdropped source data symbols, together with $H(X^K|V_{CY})$ play a role in leaking information. Since V_{CY} is a common information portion it leaks at least some information but no more than $I(X;Y)$ about X.

Equations (5.10) - (5.12) can be verified graphically using Figure 4.3. The wiretapped information from the link may be redundant information if the source data symbols correspond to the same information, which could be less information leaked than if the source bits and the channel information corresponded to different information.

5.2 Shannon Cipher System Approach for Two Correlated Sources with Partially Predetermined Information

The independent, identically distributed (i.i.d.) sources X and Y are mutually correlated random variables, depicted in Figure 5.2. The alphabet sets for sources X and Y are represented by $\mathcal{X}$ and $\mathcal{Y}$ respectively. As in the previous section, assume that (X^K, Y^K) are encoded into two syndromes (T_X and T_Y). The compressed representation is as follows: $T_X = (V_X, V_{CX})$ and $T_Y = (V_Y, V_{CY})$ where T_X and T_Y are the syndromes of X and Y. The characterization of the syndromes remains the same as specified above. Both the transmitter and receiver have access to the key, a random variable, independent of X^K and Y^K and taking values in $I_{M_K} = \{0, 1, 2, \ldots, M_K - 1\}$. The sources X^K and Y^K compute the ciphertexts $X^{'}$ and $Y^{'}$, which are the result of specific encryption functions on the plaintext from X and Y respectively. As described in Chapter 4, the encryption functions are invertible, thus knowing $X^{'}$ and the key, X^K can be retrieved.

The eavesdropper has access to either the common or private portions given by T_Y and/or T_X and some data symbols from the corresponding source (Y^{K_2}). There is a mapping/function that describes the relation between the uncompressed information and the compressed information. This implies that certain source bits correspond to certain compressed bits transmitted as channel information. It is valuable to determine how much of information to transmit at a time such that the eavesdropper cannot retrieve the message (this is described in the next section).

The encoder functions for X and Y, (E_X and E_Y respectively) are given as:

$$\begin{aligned} E_X : (\mathcal{X}^{K_1}, \mathcal{X}^{K_2}) \times I_{M_{kX}} \quad \rightarrow \quad & I_{M'_X} = \{0, 1, \ldots, M'_X - 1\} \\ & I_{M'_{CX}} = \{0, 1, \ldots, \\ & M'_{CX} - 1\} \end{aligned} \tag{5.26}$$

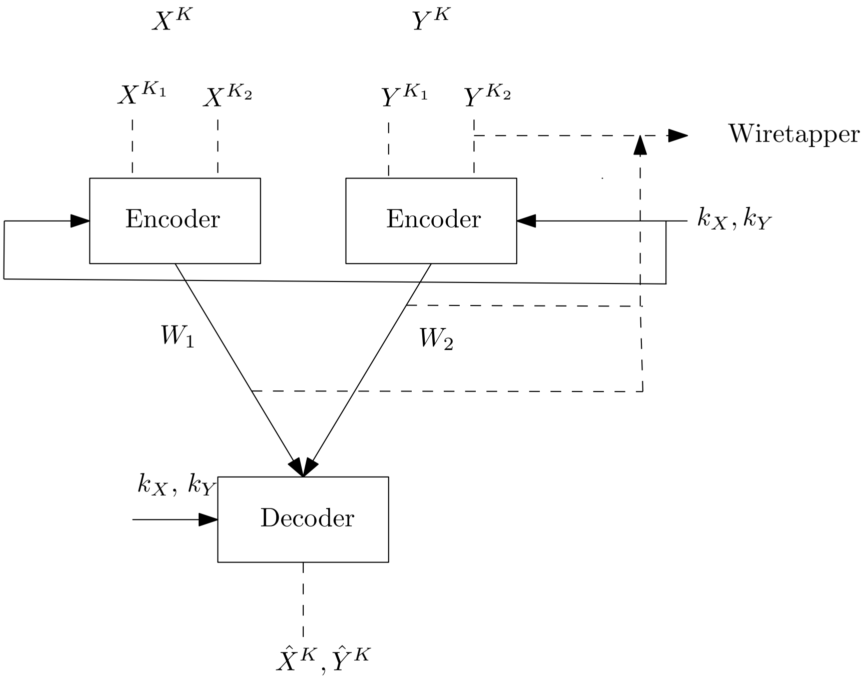

FIGURE 5.2: Shannon cipher system for two correlated sources with wiretapped source symbols

$$\begin{aligned} E_Y : (\mathcal{Y}^{K_1}, \mathcal{Y}^{K_2}) \times I_{M_{kY}} &\rightarrow I_{M'_Y} = \{0, 1, \ldots, M'_Y - 1\} \\ & I_{M'_{CY}} = \{0, 1, \ldots, \quad (5.27) \\ & M'_{CY} - 1\} \quad (5.28) \end{aligned}$$

The decoder is defined as:

$$\begin{aligned} D_{XY} : (I_{M'_X}, I_{M'_Y}, I_{M'_{CX}}, I_{M'_{CY}}) &\times I_{M_{kX}}, I_{M_{kY}} \\ &\rightarrow \mathcal{X}^K \times \mathcal{Y}^K \quad (5.29) \end{aligned}$$

The encoder and decoder mappings are below:

$$W_1 = F_{E_X}(X^{K_1}, X^{K_2}, W_{kX}) \tag{5.30}$$

$$W_2 = F_{E_Y}(Y^{K_1}, Y^{K_2}, W_{kY}) \tag{5.31}$$

$$\widehat{X}^K = F_{D_X}(W_1, W_2, W_{kX}) \tag{5.32}$$

$$\widehat{Y}^K = F_{D_Y}(W_1, W_2, W_{kY}) \tag{5.33}$$

or

$$(\widehat{X}^K, \widehat{Y}^K) = F_{D_{XY}}(W_1, W_2, W_{kX}, W_{kY}) \tag{5.34}$$

The following conditions should be satisfied for cases 1- 4:

$$\frac{1}{K}\log M_X \leq R_X + \epsilon \tag{5.35}$$

$$\frac{1}{K}\log M_Y \leq R_Y + \epsilon \tag{5.36}$$

$$\frac{1}{K}\log M_{kX} \leq R_X + \epsilon \tag{5.37}$$

$$\frac{1}{K}\log M_{kY} \leq R_{kY} + \epsilon \tag{5.38}$$

$$\Pr\{\widehat{X}^K \neq X^K\} \leq \epsilon \tag{5.39}$$

$$\Pr\{\widehat{Y}^K \neq Y^K\} \leq \epsilon \tag{5.40}$$

$$\frac{1}{K}H(X^K|W_1, W_2) \leq h_X + \epsilon \tag{5.41}$$

$$\frac{1}{K}H(Y^K|W_1, W_2) \leq h_Y + \epsilon \tag{5.42}$$

$$\frac{1}{K}H(X^K, Y^K|W_1, W_2) \leq h_{XY} + \epsilon \tag{5.43}$$

where R_X is the rate of source X's channel and R_Y is the rate of source Y's channel. Here, (R_{kX}, R_{kY}) is the rate of the key channel when allocating a key to X and Y. The security level for X and Y are measured by the total and individual uncertainties, (h_X, h_Y).

The cases 1 - 3 are:

Case 1: When (W_1, W_2, Y^{K_2}) is leaked and (X^K, Y^K) needs to be kept secret. The security level of concern is represented by $\frac{1}{K}H(X^K, Y^K|W_1, W_2, Y^{K_2})$.

Case 2: When (W_1, W_2, Y^{K_2}) is leaked and (X^K, Y^K) needs to be kept secret. The security level of concern is represented by $(\frac{1}{K}H(X^K|W_1, W_2, Y^{K_2}), \frac{1}{K}H(Y^K|W_1, W_2, Y^{K_2}))$.

Case 3: When (W_1, W_2, Y^{K_2}) is leaked and Y^K needs to be kept secret.The security level of concern is represented by $\frac{1}{K}H(Y^K|W_1, W_2, Y^{K_2})$.

The admissible rate region for each case is defined as follows:

Definition 1a: $(R_X,\ R_Y,\ R_{kX},\ R_{kY},\ h_{XY})$ is admissible for case 1 if there exists a code $(F_{E_X},\ F_{D_{XY}})$ such that (5.35) - (5.40) and (5.43) hold for any $\epsilon \to 0$ and sufficiently large K.

Definition 1b: $(R_X,\ R_Y,\ R_{kX},\ R_{kY},\ h_X,\ h_Y)$ is admissible for case 2 if there exists a code $(F_{E_Y},\ F_{D_{XY}})$ such that (5.35) - (5.42) hold for any $\epsilon \to 0$ and sufficiently large K.

Definition 1c: $(R_X,\ R_Y,\ R_{kX},\ R_{kY},\ h_Y)$ is admissible for case 3 if there exists a code $(F_{E_X},\ F_{D_{XY}})$ and $(F_{E_Y},\ F_{D_{XY}})$ such that (5.35) - (5.40) and (5.42) hold for any $\epsilon \to 0$ and sufficiently large K.

Definition 2: The admissible rate regions of $\mathcal{R}_j$ for case j are defined as:

$$\begin{aligned}\mathcal{R}_1(h_{XY}) = \{&(R_X, R_Y, R_{kX}, R_{kY}) : \\ &(R_X, R_Y, R_{kX}, R_{kY}, h_{XY}) \text{ is admissible for case 1}\}\end{aligned} \tag{5.44}$$

$$\begin{aligned}\mathcal{R}_2(h_X, h_Y) = \{&(R_X, R_Y, R_{kX}, R_{kY}) : \\ &(R_X, R_Y, R_{kX}, R_{kY}, h_X, h_Y) \text{ is admissible for case 2}\}\end{aligned} \tag{5.45}$$

$$\begin{aligned}\mathcal{R}_3(h_Y) = \{&(R_X, R_Y, R_{kX}, R_{kY}) : \\ &(R_X, R_Y, R_{kX}, R_{kY}, h_Y) \text{ is admissible for case 3}\}\end{aligned} \tag{5.46}$$

Theorems for these regions have been developed:

Theorem 4: For $0 \leq h_{XY} \leq H(X,Y) - \mu_C - \mu_Y$ and

$$\begin{aligned}
&\mathcal{R}_1(h_{XY}) = \{(R_X, R_Y, R_{kX}, R_{kY}) : \\
&R_X \geq H(X|Y), \\
&R_Y \geq H(Y|X), \\
&R_X + R_Y \geq H(X,Y) \text{ and} \\
&R_{kX} + R_{kY} \geq h_{XY}\}
\end{aligned} \tag{5.47}$$

Theorem 5: For $0 \leq h_X \leq H(X) - \mu_C$ and $0 \leq h_Y \leq H(Y) - \mu_C - \mu_Y$,

$$\begin{aligned}
&\mathcal{R}_2(h_X, h_Y) = \{(R_X, R_Y, R_{kX}, R_{kY}) : \\
&R_X \geq H(X|Y), \\
&R_Y \geq H(Y|X), \\
&R_X + R_Y \geq H(X,Y) \text{ and} \\
&R_{kX} + R_{kY} \geq \max(h_X, h_Y)\}
\end{aligned} \tag{5.48}$$

where $\mathcal{R}_1$ and $\mathcal{R}_2$ are the regions for cases 1 and 2 respectively.

Here, the wiretapped source symbols are indicated by the following entropy: $\frac{1}{K2}H(Y^{K_2}) = \mu_C + \mu_Y$, where μ_C and μ_Y are the common and private portions of the i.i.d source Y that are contained in Y^{K_2} per symbol. Here, Y_{K_2} is proportional to K. When $h_X = 0$ then case 3 can be reduced to that in (5.48). Hence Corollary 2 follows:
Corollary 2: For $0 \leq h_Y \leq H(Y) - \mu_C - \mu_Y$, $\mathcal{R}_3(h_Y) = \mathcal{R}_2(0, h_Y)$

The code achieving these bounds for case 2 allows for the key length of h_Y to be achieved across Y's channel in case 3. The security levels, which are measured by the individual uncertainties (h_X, h_Y) and total uncertainty h_{XY} give an indication of the level of uncertainty in knowing certain information. When the uncertainty increases then less information is known to an eavesdropper and there is a higher level of security. The direct and converse parts of the proofs for Theorem 4 (5.47) and Theorem 5 (5.48) are contained within Appendix B.

5.3 Information Leakage for the System using Matrix Partitions

The setup (G matrix, H matrix and syndromes) for this section is the same as that for the implementation for the two correlated source model presented in Section 4.5. Here K_2 has a length specified as $K_2 \leq K$. The Hamming distance is represented as follows: $d_H(X^K, Y^K) \leq 1$.

The method specified in Section 4.5 is applied here. The leakage due to (T_X, T_Y) has been detailed in Section 4.5 and here the leaked Y^{K_2} portion may be considered separately thereby forming a solution for the following cases:

- The equivocation on (X^K, Y^K) when (T_X, T_Y, Y^{K_2}) is leaked
- The equivocation on (X^K, Y^K) when (T_X, Y^{K_2}) is leaked
- The equivocation on (X^K, Y^K) when (T_Y, Y^{K_2}) is leaked

The information leakage on (X^K, Y^K) when K_2 bits of source Y is leaked is considered. First, since $d_H(X^K, Y^K) \leq 1$, if there are $0 < K_2 \leq K$ bits, the number of possible sequences including repeated sequences is $2^{K-K_2}(K+1)$. For each K_2 bits wiretapped, there are K_2+1 possible combinations that have a Hamming distance of one. Therefore, the information leakage due to Y^{K_2} with respect to X^K is detailed in (5.49).

$$L_{Y^{K_2}}^{X^K} = K_2 - \frac{K-K_2+1}{K+1} \log_2 \frac{K-K_2+1}{K+1} - \sum_{i=1}^{K_2} \frac{1}{K+1} \log_2 \frac{1}{K+1} \tag{5.49}$$

where $K = 7$.

The results obtained for this scenario in (5.49) are presented in Figure 5.3. It is seen that the maximum information leakage of Y_{K_2} on X^K is the four bits representing the common information between X^K and Y^K.

For the leakage of Y^{K_2} with respect to Y^K, it is given by K_2. This is depicted in Figure 5.4. The combination of this quantity (eliminating the common information) and that in (5.49) result in the information leakage on (X^K, Y^K) when Y^{K_2} has been leaked. With

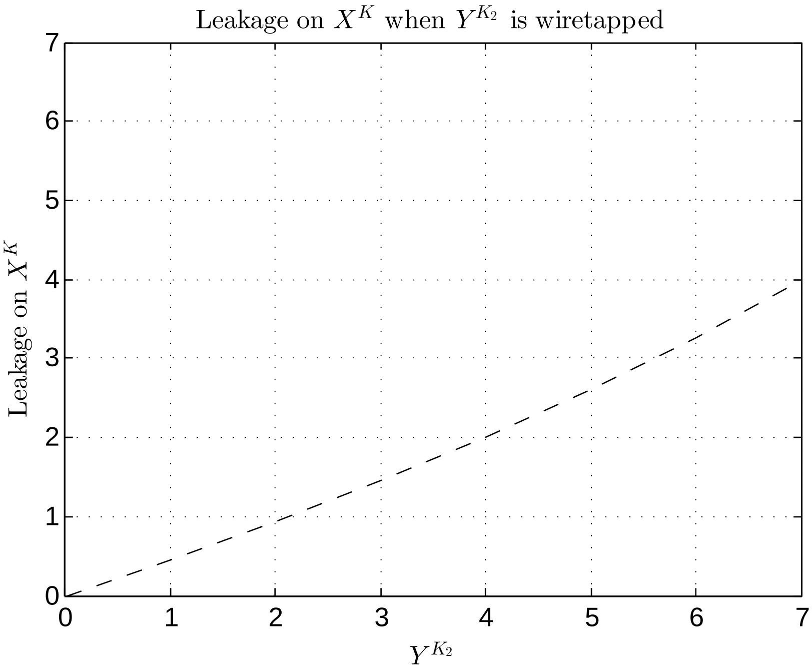

FIGURE 5.3: The information leakage on X^K when Y^{K_2} has been wiretapped

use of the Venn diagram above it is seen that the information leakage on (X^K, Y^K) reduces to Y^{K_2}. This means that for example, if Y^{K_2} is two bits then there are two bits known about (X^K, Y^K). Figure 5.5 shows the numerical results.

The information leakage represented here may be used in the cases specified in this section to separately determine the information leakage of Y^{K_2} on X^K and Y^K.

The chapter described a novel two correlated source model where some source information has been leaked to a wiretapper. The security aspects for this model have been analyzed in terms of the Slepian-Wolf scenario and Shannon's cipher system. The information leakage bounds and rate regions for perfect secrecy have been provided based on the analysis of the security aspects. The chapter ends with the coding implementation for the novel model presented here, which is an important contribution as highlighted at the beginning of this chapter.

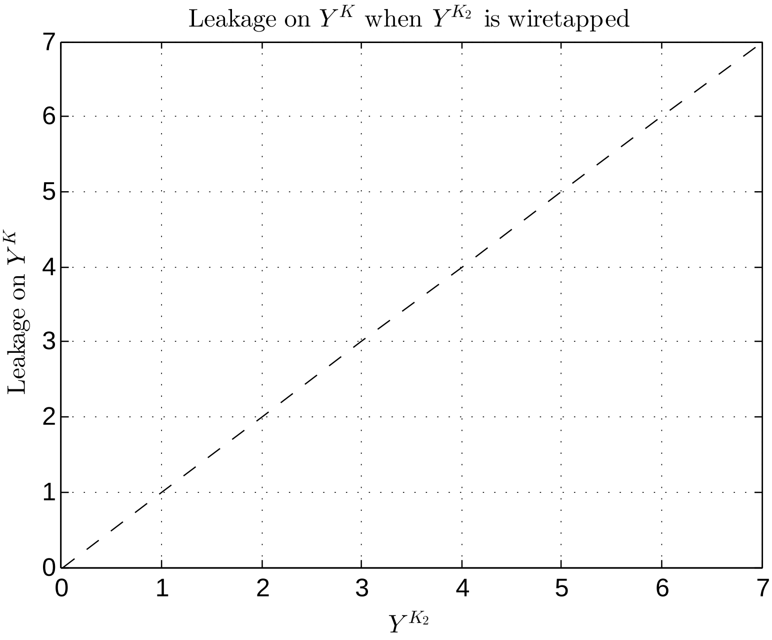

FIGURE 5.4: The information leakage on Y^K when Y^{K_2} has been wiretapped

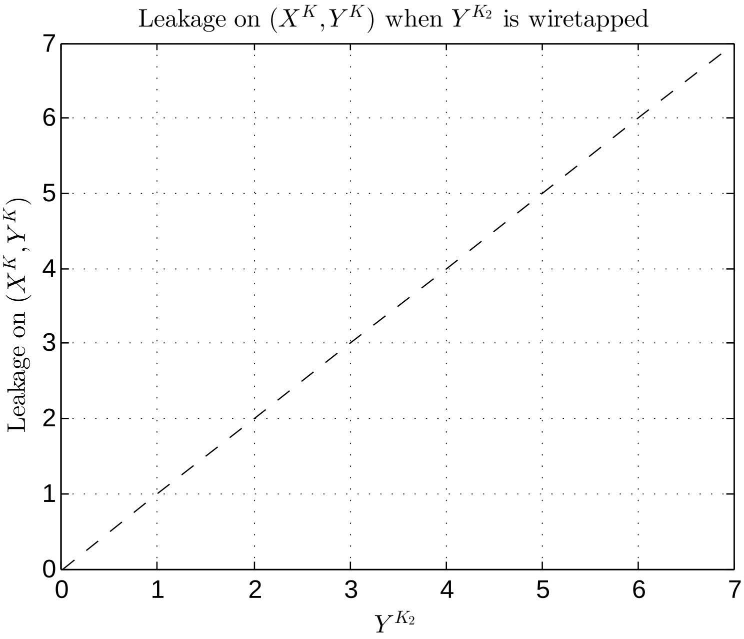

FIGURE 5.5: The information leakage on (X^K,Y^K) when Y^{K_2} has been wiretapped

Chapter 6

Information Leakage for Correlated Sources using Heterogeneous Encoding Method

This chapter describes a novel correlated source scenario in which two encoding methods are investigated; the novel model is referred to as a model with a heterogeneous encoded method. It caters for applications where a source has been leaked to a wiretapper. A main contribution is the development of the heterogeneous encoding correlated source model. The two approaches explored to investigate the information leakage have been used here; one quantifying the information leakage for the Slepian-Wolf scenario and the other incorporating Shannon's cipher system. These security aspects of the two correlated source model is also a contribution. The chapter again ends with a section showing the coding implementation for this model, which is an important contribution as it shows practical implementation for the novel model developed and provides an important link between the information theory and coding theory fields.

6.1 Correlated Source Model for Heterogeneous Encoding Method

The scenario has also been presented in terms of this model description and the implementation below [63]. The independent, identically distributed (i.i.d.) sources X, Y and

Z are mutually correlated random variables, depicted in Figure 6.1. The alphabet sets for sources X, Y and Z are represented by $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ respectively. Assume that X^K and Y^K are encoded into two channel information portions represented by their common and private information portions. Here, $T_X = (V_{CX}, V_X)$ and $T_Y = (V_{CY}, V_Y)$ where T_X and T_Y are the channel information of X and Y respectively. The Venn diagram in Figure 6.2 illustrates this idea. Each source is composed of K bits, and for source Z^K, μ of these symbols are considered as the wiretapped information and is leaked to the wiretapper ($\mu \leq K$).

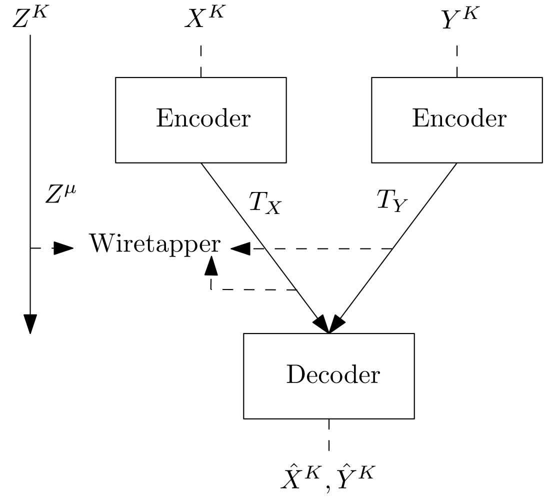

FIGURE 6.1: Correlated source coding for three sources with X and Y transmitting compressed information

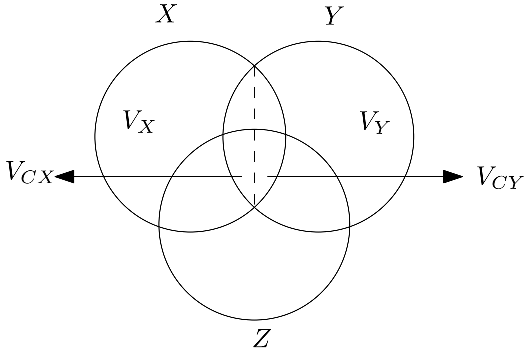

FIGURE 6.2: The relation between private and common information

The correlated sources X, Y and Z transmit messages (in the form of some channel information) to the receiver along the wiretapped links. The eavesdropper has access to either the common or private portions given by T_X and T_Y and the predetermined information from the source Z, i.e. Z^μ. As with the model in Chapter 5, the effect is that the eavesdropper has access to some compressed information (that is transmitted across the communication link after encoding) and some uncompressed information (i.e. the data symbols from source Z).

Here, for X^K and Y^K the typical set encoding and decoding described in Chapter 4 is used. As a summary, it is possible to determine bin indices for the typical sequence from the indices passed over the communication channel. When common or private information from the syndromes are wiretapped it gives an indication of which row/column in the specific look up table the sequence is contained within.

The code described in this section satisfies the following inequalities for $\delta > 0$ and sufficiently large K.

$$Pr\{X \neq G(V_X, V_{CX})\} \leq \delta \tag{6.1}$$

$$Pr\{Y \neq G(V_Y, V_{CY})\} \leq \delta \tag{6.2}$$

From the Venn diagram we see the private information and common information produced by each source should contain almost no redundancy. Here, (V_{CX}, V_X, V_Y, V_{CY}) are asymptotically disjoint, which ensures that there is almost no redundant information sent to the decoder.

Here, the nature of codes when there are three correlated sources is explored. The correlation occurs as follows: $d_H(X^K, Y^K) \leq 1$ and $d_H(Y^K, Z^K) \leq 1$. This means X and Y have a Hamming distance of one and Y and Z have a Hamming distance of one. There is therefore some sort of correlation between X and Z as they are both correlated to Y.

The prototype code is initially defined: for any $\epsilon_0 \geq 0$ and sufficiently large K, there exits a code $W_{CX} = F_{CX}(X^K)$, $W_{CY} = F_{CY}(Y^K)$, $\widehat{X}^K, \widehat{Y}^K$, where $W_X \in I_{M_X}$, $W_Y \in I_{M_Y}$, $W_{CX} \in I_{M_{CX}}$ and $W_{CY} \in I_{M_{CY}}$ for I_{M_α}, which is defined as $\{0, 1, \ldots, M_\alpha - 1\}$, that satisfies,

$$Pr\{\widehat{X}^K, \widehat{Y}^K, \widehat{Z}^K \neq X^K, Y^K, Z^K\} \leq \epsilon \tag{6.3}$$

$$H(X|Y,Z) - \epsilon_0 \leq \frac{1}{K} \log M_X \leq H(X|Y,Z) + \epsilon_0 \tag{6.4}$$

$$\begin{aligned} H(Y|X,Z) - \epsilon_0 &\leq \frac{1}{K} H(W_Y) \leq \frac{1}{K} \log M_Y \\ &\leq H(Y|X) + \epsilon_0 \end{aligned} \tag{6.5}$$

$$H(Z|X,Y) - \epsilon_0 \leq \frac{1}{K} \log M_Z \leq H(Z|X,Y) + \epsilon_0 \tag{6.6}$$

$$\begin{aligned} & I(X;Y) - \epsilon_0 \leq \frac{1}{K} \log[H(W_C X) + H(W_{CY})] \\ \leq \; & I(X;Y) + \epsilon_0 \end{aligned} \tag{6.7}$$

$$\frac{1}{K} H(X^K|V_Y, V_Z) \geq H(X) - \epsilon_0 \tag{6.8}$$

$$\frac{1}{K} H(Y^K|V_X, V_Z) \geq H(Y) - \epsilon_0 \tag{6.9}$$

$$\frac{1}{K} H(Z^K|V_Z, V_Y) \geq H(Z) - \epsilon_0 \tag{6.10}$$

We can see that (6.3) - (6.7) mean

$$\begin{aligned} & H(X,Y) - 3\epsilon_0 \leq \frac{1}{K}(H(V_X) + H(V_{CX}) + H(W_Y) \\ + \quad & H(W_{CY})) \leq H(X,Y) + 3\epsilon_0 \\ + \quad & 3\epsilon_0 \end{aligned} \tag{6.11}$$

Hence from (6.3), (6.11) and the ordinary source coding theorem, (W_X, W_Y, W_{CX} and W_{CY}) have almost no redundancy for sufficiently small $\epsilon_0 \geq 0$. The encoding and decoding defined by the existence of the prototype code provided by (6.3) - (6.11) have been proven in Chapter 4 for two sources.

This model can cater for a scenario where a particular source, say Y needs to be more secure than X (possibly because of more eavesdropping on the Y channel); we would need to secure the information that could be compromised. This masking approach is described in Chapter 4.

In order to determine the security of the system, a measure for the amount of information leaked has been developed. The obtained information and total uncertainty are used to determine the leaked information. Information leakage is indicated using the $L^{\mathcal{P}}_{\mathcal{Q}}$ notation described in Chapter 4.

The information leakage bound for the following two cases are considered:
Case 1: Leakage on Y when (T_X, T_Y, Z^μ) are wiretapped.
Case 2: Leakage on X when (T_X, T_Y, Z^μ) are wiretapped.

The information leakage for these cases is as follows:

$$\begin{aligned} L^{Y^K}_{T_X,T_Y,Z^\mu} \quad \leq \quad & I(T_Y;Y^K) + I(T_X;Y^K) \\ + \quad & I(T_Y;T_X|Y) + I(Y^K;Z^\mu) + I(T_Y;Z^\mu|Y^K) \\ + \quad & I(T_X;Z^\mu|Y^K,T_Y) - I(T_X;T_Y) - I(T_X;Z^\mu) \\ - \quad & I(T_Y;Z^\mu|T_X) + 2\delta \end{aligned} \tag{6.12}$$

$$\begin{aligned} L^{Y^K}_{T_X,T_Y,Z^\mu} \leq & \; I(T_Y;X)+I(X;T_X) \\ + & \; I(T_Y;T_X|X)+I(X;Z^\mu)+I(T_Y;Z^\mu|X) \\ + & \; I(T_X;Z^\mu|Y,T_Y)-I(T_X;T_Y)-I(Z^\mu;T_X) \\ - & \; I(T_Y;Z^\mu|T_X)+2\delta \end{aligned} \tag{6.13}$$

Here, T_X and T_Y are the compressed sequences and in terms of the information quantity they include either the private or common portion. Thus, we can see the above bound as a generalized result for wiretapping X's or Y's links, when μ bits of the source Z is leaked. The portion Z^μ could be leaked with respect to source X or Y.

This bound developed in (6.12) is proven below.

Proof for (6.12): First, $H(Y^K|T_Y,T_X,Z^\mu)$ is determined as the information leakage is found using $H(Y)-H(Y|T_Y,T_X,Z^\mu)$.

$$\begin{aligned}
& H(Y|T_Y, T_X, Z^\mu) \\
= \; & H(Y, T_Y, T_X, Z^\mu) - H(T_Y, T_X, Z^\mu) \\
\overset{(a)}{=} \; & H(Y^K) + H(T_Y|Y) + H(T_X|T_Y, Y) \\
+ \; & H(Z^\mu|Y^K, T_Y, T_X) - [H(T_Y) + H(T_X|T_Y) \\
+ \; & H(Z^\mu|T_Y, T_X)] \\
\overset{(b)}{=} \; & H(Y^K) + [H(T_Y) - I(T_Y; Y)] + [H(T_X - I(Y; T_X) \\
- \; & I(T_Y; T_X|Y)] + [H(Z^\mu) - I(Y; Z^\mu) \\
- \; & I(T_Y; Z^\mu|Y) - I(T_X; Z^\mu|Y, T_Y)] - H(T_Y) \\
- \; & [H(T_X) - I(T_X; T_Y)] - [H(Z^\mu) \\
- \; & I(Z^\mu; T_X) - I(T_Y; Z^\mu|T_X)] \\
\overset{(c)}{=} \; & H(Y) + H(T_Y) - I(T_Y; Y) + H(T_X) - I(Y; T_X)) \\
- \; & I(T_Y; T_X|Y) + H(Z^\mu) - I(Y; Z^\mu) \\
- \; & I(T_Y; Z^\mu|Y) - I(T_X; Z^\mu|Y, T_Y) - H(T_Y) \\
- \; & H(T_X) + I(T_X; T_Y) - H(Z^\mu) + I(Z^\mu; T_X) \\
+ \; & I(T_Y; Z^\mu|T_X) \\
= \; & H(Y^K) - I(T_Y; Y) - I(Y; T_X) \\
- \; & I(T_Y; T_X|Y) - I(Y; Z^\mu) - I(T_Y; Z^\mu|Y) \\
- \; & I(T_X; Z^\mu|Y, T_Y) + I(T_X; T_Y) \\
+ \; & I(Z^\mu; T_X) + I(T_Y; Z^\mu|T_X)
\end{aligned} \tag{6.14}$$

where (a) results from the chain rule expansion for $H(Y, T_Y, T_X, Z^\mu)$ and $H(T_Y, T_X, Z^\mu)$ and (b) results from the property that the conditional entropy is the same as the mutual information subtracted from the total uncertainty, i.e. $H(X|Y) = H(X) - I(X; Y)$. Here, (c) is arithmetic, where the terms $H(T_Y)$, $H(T_X)$ and $H(Z^\mu)$ cancel.

The information leakage is thus:

$$
\begin{aligned}
L^{Y^K}_{T_Y,T_X,Z^\mu} &= H(Y) - H(Y^K|T_Y,T_X,Z^\mu) \\
&\leq H(Y^K) - H(V_Y) - H(V_{CY}) - H(V_{CX}) \\
&- H(V_{CZ}) - H(Y^K) + I(T_Y;Y) + I(Y;T_X) \\
&+ I(T_Y;T_X|Y) + I(Y;Z^\mu) + I(T_Y;Z^\mu|Y) \\
&+ I(T_X;Z^\mu|Y,T_Y) - [I(T_X;T_Y) \\
&+ I(Z^\mu;T_X) + I(T_Y;Z^\mu|T_X)] + \delta \qquad (6.15) \\
&= I(T_Y;Y) + I(Y;T_X) + I(T_Y;T_X|Y) \\
&+ I(Y;Z^\mu) + I(T_Y;Z^\mu|Y) + I(T_X;Z^\mu|Y,T_Y) \\
&- I(T_X;T_Y) - I(Z^\mu;T_X) \\
&- I(T_Y;Z^\mu|T_X) + 2\delta \qquad (6.16)
\end{aligned}
$$

which proves (6.12). Here, (6.15) results from (6.2).

Proof for (6.13):

$$
\begin{aligned}
& H(X|T_Y, T_X, Z^\mu) \\
= \quad & H(X, T_Y, T_X, Z^\mu) - H(T_Y, T_X, Z^\mu) \\
\overset{(d)}{=} \quad & H(X) + H(T_Y|X^K) + H(T_X|T_Y, X) \\
+ \quad & H(Z^\mu|X^K, T_Y, T_X) - [H(T_Y) + H(T_X|T_Y) \\
+ \quad & H(Z^\mu|T_Y, T_X)] \\
\overset{(e)}{=} \quad & H(X) + [H(T_Y) - I(T_Y; X)] + [H(T_X - I(X; T_X) \\
- \quad & I(T_Y; T_X|X)] + [H(Z^\mu) - I(X; Z^\mu) \\
- \quad & I(T_Y; Z^\mu|X) - I(T_X; Z^\mu|X, T_Y)] - H(T_Y) \\
- \quad & [H(T_X) - I(T_X; T_Y)] - [H(Z^\mu) \\
- \quad & I(Z^\mu; T_X) - I(T_Y; Z^\mu|T_X)] \\
\overset{(f)}{=} \quad & H(X) + H(T_Y) - I(T_Y; X) + H(T_X) - I(X; T_X)) \\
- \quad & I(T_Y; T_X|X) + H(Z^\mu) - I(X; Z^\mu) \\
- \quad & I(T_Y; Z^\mu|X) - I(T_X; Z^\mu|X, T_Y) - H(T_Y) \\
- \quad & H(T_X) + I(T_X; T_Y) - H(Z^\mu) + I(Z^\mu; T_X) \\
+ \quad & I(T_Y; Z^\mu|T_X) \\
= \quad & H(X^K) - I(T_Y; X) - I(X; T_X) \\
- \quad & I(T_Y; T_X|X) - I(X; Z^\mu) - I(T_Y; Z^\mu|X) \\
- \quad & I(T_X; Z^\mu|X, T_Y) + I(T_X; T_Y) \\
+ \quad & I(Z^\mu; T_X) + I(T_Y; Z^\mu|T_X)
\end{aligned}
\tag{6.17}
$$

where (d) results from the chain rule expansion for $H(X, T_Y, T_X, Z^\mu)$ and $H(T_Y, T_X, Z^\mu)$ and (e) results from the property that the conditional entropy is the same as the mutual information subtracted from the total uncertainty, i.e. $H(X|Y) = H(X) - I(X; Y)$. Here, (f) is arithmetic, where the terms $H(T_Y)$, $H(T_X)$ and $H(Z^\mu)$ cancel.

The information leakage is thus:

$$
\begin{aligned}
L^{X}_{T_Y,T_X,Z^{\mu}} &= H(X) - H(X|T_Y,T_X,Z^{\mu}) \\
&\leq H(X) - H(V_X) - H(V_{CY}) - H(V_{CX}) \\
&- H(V_{CZ}) - H(X) + I(T_Y;X) + I(X;T_X) \\
&+ I(T_Y;T_X|X) + I(X;Z^{\mu}) + I(T_Y;Z^{\mu}|X) \\
&+ I(T_X;Z^{\mu}|X,T_Y) - [I(T_X;T_Y) \\
&+ I(Z^{\mu};T_X) + I(T_Y;Z^{\mu}|T_X)] + \delta \qquad (6.18) \\
&= I(T_Y;X) + I(X;T_X) + I(T_Y;T_X|X) \\
&+ I(X;Z^{\mu}) + I(T_Y;Z^{\mu}|X) + I(T_X;Z^{\mu}|Y,T_Y) \\
&- I(T_X;T_Y) - I(Z^{\mu};T_X) \\
&- I(T_Y;Z^{\mu}|T_X) + 2\delta \qquad (6.19)
\end{aligned}
$$

which proves (6.13). Here, (6.18) results from (6.1).

This section shows the information leakage for when various portions of the channel information and source data symbols from one source are leaked. The interesting cases explored for (6.12) and (6.13) demonstrate that the source Z contributes to leakage for X and Y; this is due to the common information shared between them.

Equations (6.12) and (6.13) indicate that the information leakage is upper bounded by the common information portions indicated. The information leakage in (6.12) and (6.13) can be reduced if the common information portions are secured. Equations (6.12) and (6.13) can be verified using the Venn diagram in Figure 6.2.

6.2 Shannon Cipher Approach for Correlated Sources using Heterogeneous Encoding Method

Here, Shannon's cipher system for the heterogeneous encoding method (depicted in Figure 6.3) is presented. The two source outputs are i.i.d random variables X and Y, taking on values in the finite sets $\mathcal{X}$ and $\mathcal{Y}$. Both the transmitter and receiver have access to the key, a random variable, independent of X^K and Y^K and taking values in $I_{M_k} = \{0, 1, 2, \ldots, M_k - 1\}$. As before, the sources X^K and Y^K compute the ciphertexts

W_1 and W_2, which are the result of specific encryption functions on the plaintext from X and Y respectively. The encryption functions are invertible, thus knowing W_1 and the key, k_X for X then X can be retrieved. The key for Y is represented as k_Y.

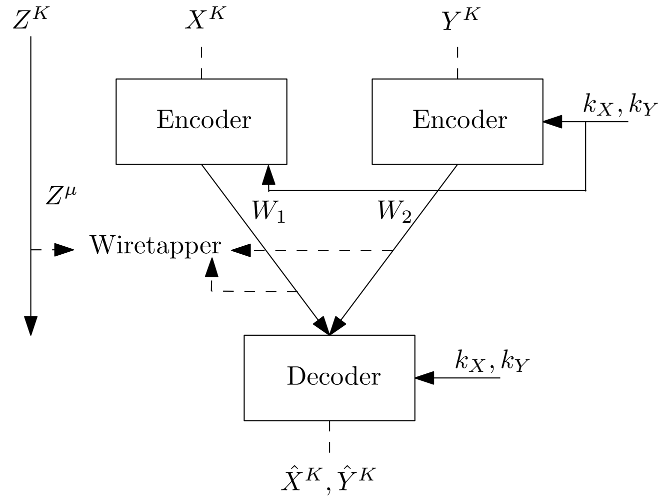

FIGURE 6.3: Shannon cipher system for three correlated sources

The encoder functions for X and Y, (E_X and E_Y respectively) are given as:

$$\begin{aligned} E_X : \mathcal{X}^K \times I_{M_{kX}} \quad &\rightarrow \quad I_{M'_X} = \{0, 1, \ldots, M'_X - 1\} \\ &\quad\quad I_{M'_{CX}} = \{0, 1, \ldots, M'_{CX} - 1\} \end{aligned} \tag{6.20}$$

$$\begin{aligned} E_Y : \mathcal{Y}^K \times I_{M_{kY}} \quad &\rightarrow \quad I_{M'_Y} = \{0, 1, \ldots, M'_Y - 1\} \\ &\quad\quad I_{M'_{CY}} = \{0, 1, \ldots, M'_{CY} - 1\} \end{aligned} \tag{6.21}$$

The decoder is defined as:

$$\begin{aligned} D_{XY} : (I_{M'_X}, I_{M'_Y}, I_{M'_{CX}}, I_{M'_{CY}}) \quad &\times \quad I_{M_{kX}}, I_{M_{kY}} \\ &\rightarrow \quad \mathcal{X}^K \times \mathcal{Y}^K \end{aligned} \tag{6.22}$$

The encoder and decoder mappings are below:

$$W_1 = F_{E_X}(X^K, W_{kX}) \tag{6.23}$$

$$W_2 = F_{E_Y}(Y^K, W_{kY}) \tag{6.24}$$

$$\widehat{X}^K = F_{D_X}(W_1, W_2, W_{kX}) \tag{6.25}$$

$$\widehat{Y}^K = F_{D_Y}(W_1, W_2, W_{kY}) \tag{6.26}$$

or

$$(\widehat{X}^K, \widehat{Y}^K) = F_{D_{XY}}(W_1, W_2, W_{kX}, W_{kY}) \tag{6.27}$$

The following conditions should be satisfied for cases 1- 4:

$$\frac{1}{K}\log M_X \leq R_X + \epsilon \tag{6.28}$$

$$\frac{1}{K}\log M_Y \leq R_Y + \epsilon \tag{6.29}$$

$$\frac{1}{K}\log M_{kX} \leq R_{kX} + \epsilon \tag{6.30}$$

$$\frac{1}{K}\log M_{kY} \leq R_{kY} + \epsilon \tag{6.31}$$

$$\Pr\{\widehat{X}^K \neq X^K\} \leq \epsilon \tag{6.32}$$

$$\Pr\{\widehat{Y}^K \neq Y^K\} \leq \epsilon \tag{6.33}$$

$$\frac{1}{K}H(X^K|W_1) \leq h_X + \epsilon \tag{6.34}$$

$$\frac{1}{K}H(Y^K|W_2) \leq h_Y + \epsilon \tag{6.35}$$

$$\frac{1}{K}H(X^K, Y^K|W_1, W_2) \leq h_{XY} + \epsilon \tag{6.36}$$

where R_X is the rate of source X's channel and R_Y is the rate of source Y's channel. Here, (R_{kX}, R_{kY}) is the rate of the key channel when allocating a key to X and Y. The security level for X and Y are measured by the total and individual uncertainties, (h_X, h_Y) and h_{XY} respectively.

The cases 1 - 3 that are considered are as follows:
Case 1: When (W_1, W_2, Z^μ) is leaked and (X^K, Y^K) needs to be kept secret. The security level of concern is represented by $\frac{1}{K}H(X^K, Y^K|W_1, W_2, Z^\mu)$.

Case 2: When (W_1, W_2, Z^μ) is leaked and (X^K, Y^K) needs to be kept secret. The security level of concern is represented by $(\frac{1}{K}H(X^K|W_1, W_2, Z^\mu), \frac{1}{K}H(Y^K|W_1, W_2, Z^\mu))$.
Case 3: When (W_1, W_2, Z^μ) is leaked and Y^K needs to be kept secret.The security level of concern is represented by $\frac{1}{K}H(Y^K|W_1, W_2, Z^\mu)$.

The admissible rate region for each case is defined as follows:
Definition 1a: $(R_X$, R_Y, R_{kX}, R_{kY}, $h_{XY})$ is admissible for case 1 if there exists a code $(F_{E_X}$, $F_{D_{XY}})$ and $(F_{E_Y}$, $F_{D_{XY}})$ such that (6.28) - (6.33) and (6.36) hold for any $\epsilon \to 0$ and sufficiently large K.
Definition 1b: $(R_X$, R_Y, R_{kX}, R_{kY}, h_X, $h_Y)$ is admissible for case 2 if there exists a code $(F_{E_X}$, $F_{D_{XY}})$ and $(F_{E_Y}$, $F_{D_{XY}})$ such that (6.28) - (6.35) hold for any $\epsilon \to 0$ and sufficiently large K.
Definition 1c: $(R_X$, R_Y, R_{kX}, R_{kY}, $h_Y)$ is admissible for case 3 if there exists a code $(F_{E_Y}$, $F_{D_{XY}})$ such that (6.28) - (6.33) and (6.35) hold for any $\epsilon \to 0$ and sufficiently large K.
Definition 2: The admissible rate regions of $\mathcal{R}_j$ for case j are defined as:

$$\begin{aligned}\mathcal{R}_1(h_{XY}) = \{&(R_X, R_Y, R_{kX}, R_{kY}) : \\ &(R_X, R_Y, R_{kX}, R_{kY}, h_{XY}) \text{ is admissible for case 1}\}\end{aligned} \tag{6.37}$$

$$\begin{aligned}\mathcal{R}_2(h_X, h_Y) = \{&(R_X, R_Y, R_{kX}, R_{kY}) : \\ &(R_X, R_Y, R_{kX}, R_{kY}, h_X, h_Y) \text{ is admissible for case 2}\}\end{aligned} \tag{6.38}$$

$$\begin{aligned}\mathcal{R}_3(h_Y) = \{&(R_X, R_Y, R_{kX}, R_{kY}) : \\ &(R_X, R_Y, R_{kX}, R_{kY}, h_Y) \text{ is admissible for case 3}\}\end{aligned} \tag{6.39}$$

Theorems for these regions have been developed:

Theorem 6: For $0 \leq h_{XY} \leq H(X,Y) - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z)$,

$$\begin{aligned}
&\mathcal{R}_1(h_{XY}) = \{(R_X, R_Y, R_{kX}, R_{kY}) : \\
&R_X \geq H(X|Y), \\
&R_Y \geq H(Y|X), \\
&R_X + R_Y \geq H(X,Y) \\
&R_{kX} + R_{kY} \geq h_{XY}\}
\end{aligned} \tag{6.40}$$

Theorem 7: For $0 \leq h_X \leq H(X) - \alpha_{CX}$ and $0 \leq h_Y \leq H(Y) - \alpha_{CY}$,

$$\begin{aligned}
&\mathcal{R}_2(h_Y) = \{(R_X, R_Y, R_{kX}, R_{kY}) : \\
&R_X \geq H(X|Y), \\
&R_Y \geq H(Y|X), \\
&R_X + R_Y \geq H(X,Y) \\
&R_{kX} + R_{kY} \geq \max(h_X, h_Y)\}
\end{aligned} \tag{6.41}$$

where $\mathcal{R}_1$ and $\mathcal{R}_2$ are the regions for cases 1 and 2 respectively. Here, α_{CX} and α_{CY} are the common portions (i.e. the correlated information) of the i.i.d source Z (for $I(X;Z)$ and $I(Y;Z)$ respectively) that are contained in Z^{μ} per symbol.

When $h_X = 0$ then case 3 can be reduced to that depicted in (6.41). Hence, Corollary 3 follows:
Corollary 3: For $0 \leq h_Y \leq H(Y) - \alpha_{CY}$, $\mathcal{R}_3(h_Y) = \mathcal{R}_2(0, h_Y)$

The proofs and converses of Theorems 6-7 are contained within Appendix C.

6.3 Information Leakage for the System using Matrix Partitions

The same setup (G matrix, H matrix and syndromes) as per the implementation in Section 4.5 is applied to implement this model. Using the method already specified, the information leakage for each of the following cases may be found. The leakage due to (T_X, T_Y) has been detailed in Section 4.5 and here the leaked Z^μ portion may be considered separately, thereby forming a solution for the following cases:

- The equivocation on (X^K, Y^K) when (T_X, T_Y, Z^μ) is leaked
- The equivocation on (X^K, Y^K) when (T_X, Z^μ) is leaked
- The equivocation on (X^K, Y^K) when (T_Y, Z^μ) is leaked

The information leakage on (X^K, Y^K) when μ bits of source Z is leaked is considered, which is done in two steps. First, since $d_H(Y^K, Z^K) \leq 1$, if there are $0 < \mu \leq K$ bits ($\mu = 0$ has been considered in Section 4.5), the number of possible sequences including repeated sequences is $2^{K-\mu}(K+1)$. However, there are $2^{K-\mu}$ different sequences repeated $K - \mu + 1$ times and there are $\mu 2^{K-\mu}$ different sequences that possibly occur once.

Second, from every possible Y^K, there are eight possible sequences for X^K with identical possibilities. Therefore, the information leakage due to Z^μ with respect to X^K and Y^K is detailed in (6.42).

$$\begin{aligned} L_{Z^\mu}^{X^K, Y^K} &= H(X^K, Y^K) + \tfrac{K-\mu+1}{K+1} \log_2 \tfrac{K-\mu+1}{2^{K-\mu}(K+1)} \\ &+\mu 2^{K-\mu} \tfrac{1}{2^{K-\mu}(K+1)} \log_2 \tfrac{1}{2^{K-\mu}(K+1)} - H(X^K|Y^K) \end{aligned} \tag{6.42}$$

where $H(X^K, Y^K) = 10$, $H(X^K|Y^K) = 3$ and $K = 7$.

The numerical results retrieved using (6.42) are presented in Figure 6.4. It is seen that the information leakage on (X^K, Y^K) increases as more μ bits are wiretapped and this is because of the correlation between the sources. The maximum information that Z^μ leaks about (X^K, Y^K) is four bits.

The information leakage represented in (6.42) may be used in the cases explored in this section to separately determine the information leakage of Z^μ on X^K and Y^K. The Z^μ bits also contribute to the information leakage and the correlation between X^K, Y^K and Z^μ plays a role in determining the overall leakage.

This section shows the information leakage for the model described in this chapter where various portions of the channel information and some source data symbols from Z are

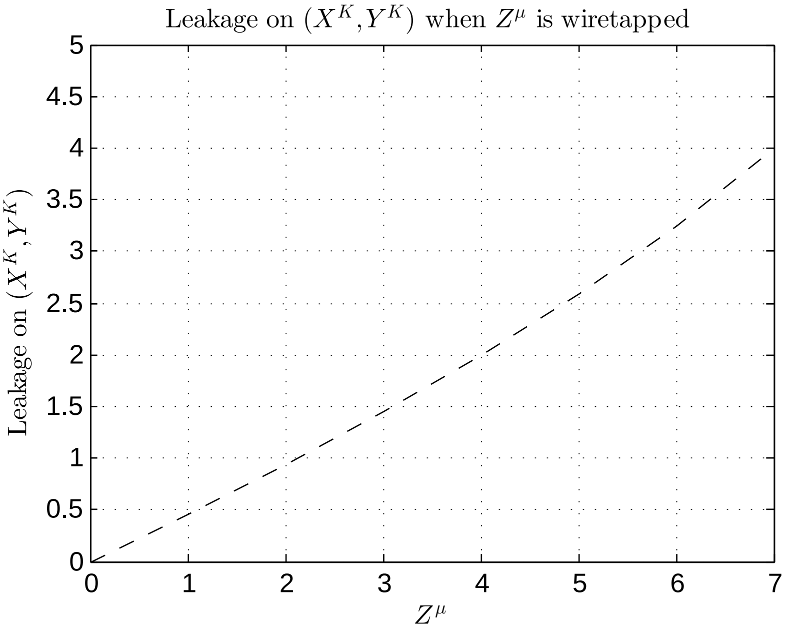

Figure 6.4: The information leakage on (X^K, Y^K) when Z^μ has been wiretapped

leaked. Again it is noted that the message bits given by u_1 and v_1 also contribute to information leakage as they are not masked in any way. If these are hidden in some way then the information leakage will be less. In addition, due to the correlation that exists between X^K, Y^K and Z^μ there is leakage on X^K and Y^K when Z^μ has been leaked.

The chapter described a novel heterogeneous encoded correlated source model where some source information has been leaked to a wiretapper. The security aspects for this model have been analyzed in terms of the Slepian-Wolf scenario and Shannon's cipher system. The information leakage bounds and rate regions for perfect secrecy have been provided based on the analysis of the security aspects. The chapter ends with the coding implementation for the novel model presented here, which is an important contribution as highlighted at the beginning of this chapter.

Chapter 7

Conclusion

This chapter concludes the thesis by initially comparing the novel correlated source models presented in Chapters 4-6 with existing models, and detailing the future work for this research project. Further, the contributions have been listed followed by a description of the contents of the thesis.

7.1 Comparison to other Models

The two correlated source model across a channel with an eavesdropper is a more generalised approach of Yamamoto's [5] model. If the links were combined into one link, the same situation as per Yamamoto's [5] would result. As described in the two correlated source model in Chapter 4 this specific model can be implemented for multiple sources with Shannon's cipher system. Due to the unique scenario incorporating multiple sources and multiple links, the models presented above are more secure as private information and common information from other link/s are required for decoding.

Further, information at the sources may be more secure in the two correlated source model presented in Chapter 4 because if one source is compromised then only one source's information is known. In Yamamoto's [5] method both source's information is contained at one station and when that source is compromised then information about both sources are known. The information transmitted along the channels (i.e. the syndromes) in these models presented in Chapters 4-6 do not have a fixed length as per Yamamoto's

[5] method. Here, the syndrome length may vary depending on the encoding procedure and nature of Slepian-Wolf codes.

In these novel models, information from more than one link may be required in order to determine the information for one source. This gives rise to added security as even if one link is wiretapped it may not be possible to determine the contents of a particular source. This is attributed to the fact that this model transmits common information portions from different links, which is different to Yamamoto's model.

At first glance, Yamamoto's model may seem to be a generalisation of the Luo *et al.* [47] model, however Luo *et al.* [47] incorporate a wiretapper at the source that has access to some source data symbols. In this work, Chapter 5 incorporates this concept in that the information known to the eavesdropper is Y^{K_2} source symbols of source Y^K.

Another major feature is that private information can be hidden using common information. Here, common information produced by a source may be used to mask its private codeword thus saving on key length. The key allocation is specified by the general rules presented in Chapter 4. The multiple correlated sources model presents a combination masking scheme where more than one common information is used to protect a private information, which is a practical approach. This is an added feature developed in order to protect the system. This approach has not been considered in the other models mentioned in this section.

The work by Yang *et al.* [2] uses the concept of side information to assist the decoder in determining the transmitted message. The side information could be considered to be a source and is related to this research when the side information is considered as correlated information. Similar work with side information that incorporates wiretappers, by Villard and Piantanida [26] and Villard *et al.* [23] may be generalised in the sense that side information can be considered to be a source, however these models are distinguishable as syndromes, which are independent of one another are transmitted across an error free channel. Further, to the author's knowledge Shannon's cipher system has not been incorporated into these models by Villard and Piantanida [26] and Villard *et al.* [23].

It is noted that the models presented in this thesis reduce to Yamamoto's model. Here, when the variations in the models presented in Chapters 5 and 6 (two correlated sources with some source information wiretapped and the heterogeneous model respectively) are removed it reduces to the two correlated source model presented in Chapter 4. When the two correlated sources become one source transmitting information across a single link then the model further reduces to that of Yamamoto's. This thesis therefore incorporates models that build on Yamamoto's model.

7.2 Future Work

This research project has room future work. It would be interesting to consider the case where the channel capacity has certain constraints (according to the assumptions in Chapter 4 the channel capacity is enough at all times). In the two correlated source models, the channels are either protected by keys or not however this is limited and a real case scenario where there are varying security levels for the channels is an avenue for future work.

7.3 Contributions

This thesis contributes the following:

- Information leakage quantification for two correlated source models (Sections 4.2 and 5.1)
- Shannon cipher approach for two correlated source models (Sections 4.4 annd 5.2)
- Information leakage quantification for heterogeneous encoding method correlated source model (Section 6.1)
- Shannon cipher approach for heterogeneous encoding method correlated source model (Section 6.2)
- Coding implementation for the various correlated source models developed (Sections 4.5, 5.3 and 6.3).

The contributions listed above are to the author's knowledge novel. There has been much work conducted in this field of security for correlated sources, which has been detailed in the literature review. The field of information theory took off with Shannon's model for a communication system [15], where the concept of entropy was introduced. The research after this important paper related to correlated sources and security aspects of wiretap networks has been described in Chapter 2. The techniques and methodologies presented in Chapter 3 gave an overview of the concepts, theorems and techniques utilized for the research. These include those developed for use by the Slepian-Wolf theorem, the wiretap channel and coding implementation for correlated sources. Initially a generalized model for correlated sources is presented where the information leakage is described and thereafter the Shannon cipher system approach is presented. These security aspects are presented for each of the correlated source models thereafter; In Chapters 4-5, where two correlated source models are presented and in Chapter 6 where a heterogeneous encoding method correlated source model is presented. The implementation for these models are also presented. The implementation uses a matrix partition method and is significant because it provides a link between information theory and coding theory. The correlated source models contained herein are for applications where there is existence of common information in communication networks (two correlated source model), there exists some predetermined information (two correlated source model with some source data symbols wiretapped), where a source is more prone to wiretapper access (heterogeneous encoding method correlated source model).

The use of correlated sources in communication networks is major as can be seen by the applications detailed in Chapters 1-2. Based on this research significant steps can be taken to advance in the field of security for correlated sources (in the broader field of information theory). The literature survey provides evidence that this research has not been conducted before and to the author's knowledge the contributions are novel.

This chapter presents a conclusion for the research project. The novel models presented have been compared to existing models and the future work has been described. This is followed by a list of the contributions and a summary of the details of the thesis.

Appendix A

Proof of Theorems 2-3

This section proves the direct parts of Theorems 2 - 3 and thereafter the converse parts. Before the theorems are proved it is necessary to develop the prototype code $(W_X, W_Y, W_{CX}, W_{CY})$. Proofs of Theorems 4-7 covered in Appendix B and C also make use of this code.

All the channel rates in the theorems above are in accordance with Slepian-Wolf's theorem, hence there is no need to prove them. A code based on the prototype code $(W_X, W_Y, W_{CX}, W_{CY})$ in Lemma 1 is constructed. In order to include a key in the prototype code, W_X is divided into two parts as per the method used by Yamamoto [5]:

$$W_{X1} = W_X \bmod M_{X1} \in I_{M_{X1}} = \{0, 1, 2, \ldots, M_{X1} - 1\} \tag{A.1}$$

$$W_{X2} = \frac{W_X - W_{X1}}{M_{X1}} \in I_{M_{X2}} = \{0, 1, 2, \ldots, M_{X2} - 1\} \tag{A.2}$$

where M_{X1} is a given integer and M_{X2} is the ceiling of M_X/M_{X1}. The M_X/M_{X1} is considered an integer for simplicity, because the difference between the ceiling value and the actual value can be ignored when K is sufficiently large. In the same way, W_Y is divided:

$$W_{Y1} = W_Y \bmod M_{Y1} \in I_{M_{Y1}} = \{0, 1, 2, \ldots, M_{Y1} - 1\} \tag{A.3}$$

$$W_{Y2} = \frac{W_Y - W_{Y1}}{M_{Y1}} \in I_{M_{Y2}} = \{0, 1, 2, \ldots, M_{Y2} - 1\} \tag{A.4}$$

The common information components W_{CX} and W_{CY} are already portions and are not divided further. In this scenario $W_{CX} + W_{CY}$ lie between 0 and $I(X;Y)$. It can be represented by X and Y, X only or Y only. It can be shown that when some of the codewords are wiretapped the uncertainties of X^K and Y^K are bounded as follows:

$$\frac{1}{K}H(X^K|W_{X2}, W_Y) \geq I(X;Y) + \frac{1}{K}\log M_{X1} - \epsilon_0^{'} \tag{A.5}$$

$$\frac{1}{K}H(Y^K|W_X, W_{Y2}) \geq I(X;Y) + \frac{1}{K}\log M_{Y1} - \epsilon_0^{'} \tag{A.6}$$

$$\frac{1}{K}H(X^K|W_X, W_{Y2}) \geq I(X;Y) - \epsilon_0^{'} \tag{A.7}$$

$$\frac{1}{K}H(X^K|W_X, W_Y, W_{CY}) \geq \frac{1}{K}\log M_{CX} - \epsilon_0^{'} \tag{A.8}$$

$$\frac{1}{K}H(Y^K|W_X, W_Y, W_{CY}) \geq \frac{1}{K}\log M_{CX} - \epsilon_0^{'} \tag{A.9}$$

$$\frac{1}{K}H(X^K|W_Y, W_{CY}) \geq H(X|Y) + \frac{1}{K}\log M_{CX} - \epsilon_0^{'} \tag{A.10}$$

$$\frac{1}{K}H(Y^K|W_Y, W_{CY}) \geq \frac{1}{K}\log M_{CX} - \epsilon_0^{'} \tag{A.11}$$

where $\epsilon_0^{'} \to 0$ as $\epsilon_0 \to 0$. The proofs for (A.5) - (A.11) are the same as per Yamamoto's [5] proof in Lemma A1. The difference is that W_{CX}, W_{CY}, M_{CX} and M_{CY} are described as W_{C1}, W_{C2}, M_{C1} and M_{C2} respectively by Yamamoto. Here, W_{CX} and W_{CY} is considered to be represented by Yamamoto's W_{C1} and W_{C2} respectively. In addition there are some more inequalities considered here:

$$\begin{aligned}\frac{1}{K}H(Y^K|W_X, W_{CX}, W_{CY}, W_{Y2}) &\geq \frac{1}{K}\log M_{Y1} \\ &- \epsilon_0^{'}\end{aligned} \tag{A.12}$$

$$\begin{aligned}\frac{1}{K}H(Y^K|W_X, W_{CX}, W_{CY}) &\geq \frac{1}{K}\log M_{Y1} \\ &+ \frac{1}{K}\log M_{Y2} - \epsilon_0^{'}\end{aligned} \tag{A.13}$$

$$\begin{aligned}\frac{1}{K}H(X^K|W_{X2}, W_{CY}) &\geq \frac{1}{K}\log M_{X1} \\ &+ \frac{1}{K}\log M_{CX} - \epsilon_0^{'}\end{aligned} \tag{A.14}$$

$$\begin{aligned}\frac{1}{K}H(Y^K|W_{X2}, W_{CY}) &\geq \frac{1}{K}\log M_{Y1} \\ &+ \frac{1}{K}\log M_{Y2} + \frac{1}{K}\log M_{CX} \\ &- \epsilon_0^{'}\end{aligned} \tag{A.15}$$

The inequalities (A.12) and (A.13) can be proven in the same way as per Yamamoto's[5] Lemma A2, and (A.14) and (A.15) can be proven in the same way as per Yamamoto's[5] Lemma A1.

A.1 Direct parts

Proof of Theorem 2. Suppose that $(R_X,\ R_Y,\ R_{KX},\ R_{KY}) \in \mathcal{R}_1$ for $h_{XY} \leq H(X, Y)$. Then, Theorem 2 is as follows:

$$\begin{aligned} &R_X \geq H(X^K|Y^K) \\ &R_Y \geq H(Y^K|X^K) \\ &R_X + R_Y \geq H(X^K, Y^K) \end{aligned} \tag{A.16}$$

$$R_{kX} + R_{kY} \geq h_{XY} \tag{A.17}$$

Here the keys are uniform random numbers. For the first case, consider the following: $h_{XY} > I(X;Y)$.

$$M_{X1} = \min(2^{KH(X|Y)}, 2^{K(h_{XY} - I(X;Y))}) \tag{A.18}$$

$$M_{Y1} = 2^{K(h_{XY} - I(X;Y))} \tag{A.19}$$

The codewords W_1 and W_2 and the key $W_{kX}$and W_{kY} are now defined:

$$W_1 = (W_{X1} \oplus W_{kY1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{A.20}$$

$$W_2 = (W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}) \tag{A.21}$$

$$W_{kX} = W_{kCX} \tag{A.22}$$

$$W_{kY} = (W_{kY1}, W_{kCY}) \tag{A.23}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know W_{X1}, W_{CX} W_{Y1} and W_{CY} as these are protected by keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy from (4.15) - (4.17) and (A.16) - (A.23), that

$$\begin{aligned}
\frac{1}{K}\log M_X + \frac{1}{K}\log M_Y &= \frac{1}{K}(\log M_{X1} + \log M_{X2} \\
&+ \log M_{CX}) + \frac{1}{K}(\log M_{Y1} \\
&+ \log M_{Y2} + \log M_{CY}) \\
&\leq H(X|Y) + H(Y|X) \\
&+ I(X;Y) + 3\epsilon_0 \\
&= H(X,Y) + 3\epsilon_0 \\
&\leq R_X + R_Y + 3\epsilon_0
\end{aligned} \tag{A.24}$$

$$\begin{aligned}
& \frac{1}{K}[\log M_{kX} + \log M_{kY}] \\
= \;& \frac{1}{K}[\log M_{CX} + \log M_{CY} + \log M_{Y1}] \\
\leq \;& I(X;Y) + h_{XY} - I(X;Y) - \epsilon_0 && \text{(A.25)} \\
= \;& h_{XY} - \epsilon_0 \\
\leq \;& R_{kX} + R_{kY} - \epsilon_0 && \text{(A.26)}
\end{aligned}$$

where (A.25) results from (A.19).

The security levels thus result:

$$\begin{aligned}
& \frac{1}{K}H(X^K, Y^K|W_1, W_2) \\
= \;& \frac{1}{K}H(X^K, Y^K|W_{X1} \oplus W_{kY1}, W_{X2}, W_{CX} \oplus W_{kCX} \\
& W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}) \\
\geq \;& \frac{1}{K}H(X^K, Y^K|W_{X1}, W_{X2}, \\
& W_{Y1} \oplus W_{kY1}, W_{Y2}) - \epsilon_0^{''} && \text{(A.27)} \\
= \;& \frac{1}{K}H(X^K, Y^K|W_X, W_{Y2}) - \epsilon_0^{''} \\
\geq \;& I(X;Y) + \frac{1}{K}\log M_{Y1} - \epsilon_0^{'} - \epsilon_0^{''} \\
= \;& I(X;Y) + h_{XY} - I(X;Y) - \epsilon_0^{'} - \epsilon_0^{''} \\
= \;& h_{XY} - \epsilon_0^{'} - \epsilon_0^{''} && \text{(A.28)}
\end{aligned}$$

where (A.27) holds because W_{CX} and W_{CY} are covered by uniform random keys and the result of Yamamoto's Lemma A2.

Therefore (R_X, R_Y, R_{kX}, R_{kY}, h_{XY}) is admissible from (A.24) - (A.28).

Next the case where: $h_{XY} \leq I(X;Y)$ is considered. The codewords and keys are now defined:

$$W_1 = (W_{X1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{A.29}$$

$$W_2 = (W_{Y1}, W_{Y2}, W_{CY}) \tag{A.30}$$

$$W_{kX} = (W_{kCX}) \tag{A.31}$$

$$M_{CX} = 2^{Kh_{XY}} \tag{A.32}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know the W_X and W_Y that are covered with keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy that

$$\begin{aligned}
\frac{1}{K}[\log M_{kX} + \log M_{kY}] &= \frac{1}{K}\log M_{CX} \\
&= h_{XY} \\
&\leq R_{kX} + R_{kY} \qquad \text{(A.33)}
\end{aligned}$$

where (A.33) results from (A.32).

The security level thus results:

$$\begin{aligned}
\frac{1}{K}H(X^K, Y^K | W_1, W_2) &= \frac{1}{K}H(X^K, Y^K | W_{X1}, W_{X2}, W_{CX} \oplus W_{kCX}, \\
&\quad W_{Y1}, W_{Y2}, W_{CY}) \\
&\geq \frac{1}{K}\log M_{CX} - \epsilon_0^{'} \\
&= h_{XY} - \epsilon_0^{'} \qquad \text{(A.34)} \\
&\geq h_{XY} - \epsilon_0^{'} \qquad \text{(A.35)}
\end{aligned}$$

where (A.34) holds from (A.32).

Therefore (R_X, R_Y, R_{kX}, R_{kY}, h_{XY}) is admissible from (A.29) - (A.71).

□

Theorem 3 proof. In the same way as Theorem 2, suppose that (R_X, R_Y, R_{kX}, R_{kY}) $\in \mathcal{R}_2$ for $h_X \leq H(X)$ and $h_Y \leq H(Y)$. Without loss of generality, we assume that $h_X \leq h_Y$. Then resulting from Theorem 3,

$$\begin{aligned} R_X &\geq H(X^K|Y^K) \\ R_Y &\geq H(Y^K|X^K) \\ R_X + R_Y &\geq H(X^K, Y^K) \end{aligned} \tag{A.36}$$

$$R_{kX} + R_{kY} \geq \max(h_X, h_Y) \tag{A.37}$$

Consider the following: $h_X > I(X;Y)$.

$$M_{X1} = \min(2^{KH(X|Y)}, 2^{K(h_Y - I(X;Y))}) \tag{A.38}$$

$$M_{Y1} = 2^{K(h_Y - I(X;Y))} \tag{A.39}$$

The codeword W_2 and the key W_{kY} is now defined:

$$W_1 = (W_{X1} \oplus W_{kY1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{A.40}$$

$$W_2 = (W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}) \tag{A.41}$$

$$W_{kX} = W_{kCX} \tag{A.42}$$

$$W_{kY} = (W_{kY1}, W_{kCY}) \tag{A.43}$$

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy from (4.15) - (4.17) and (A.38) - (A.43), that

$$\begin{aligned}
\frac{1}{K}\log M_X + \frac{1}{K}\log M_Y &= \frac{1}{K}(\log M_{X1} + \log M_{X2} \\
&+ \log M_{CX}) + \frac{1}{K}(\log M_{Y1} \\
&+ \log M_{Y2} + \log M_{CY}) \\
&\leq H(X|Y) + H(Y|X) \\
&+ I(X;Y) + 3\epsilon_0 \\
&= H(X,Y) + 3\epsilon_0 \\
&\leq R_X + R_Y + 3\epsilon_0 \qquad (A.44)
\end{aligned}$$

$$\begin{aligned}
&\frac{1}{K}[\log M_{kX} + \log M_{kY}] \\
=\ &\frac{1}{K}[\log M_{CX} + \log M_{CY} + \log M_{Y1}] \\
\leq\ &I(X;Y) + h_Y - I(X;Y) - \epsilon_0 \qquad (A.45) \\
=\ &h_Y - \epsilon_0 \\
\leq\ &R_{kX} + R_{kY} - \epsilon_0 \qquad (A.46)
\end{aligned}$$

The security levels thus result:

$$\begin{aligned}
& \frac{1}{K}H(X^K|W_1,W_2) \\
= & \frac{1}{K}H(X^K|W_{X1}\oplus W_{kY1},W_{X2},W_{CX}\oplus W_{kCX} \\
& W_{Y1}\oplus W_{kY1},W_{Y2},W_{CY}\oplus W_{kCY}) \\
\geq & \frac{1}{K}H(X^K,Y^K|W_{X1}\oplus W_{kY1},W_{X2},W_{Y1}\oplus W_{kY1} \qquad (A.47) \\
& W_{Y2})-\epsilon_0^{''} \\
= & \frac{1}{K}H(X^K,Y^K|W_{X2},W_{Y2})-\epsilon_0^{''} \\
\geq & I(X;Y)+\frac{1}{K}\log M_{X1}-\epsilon_0^{''} \\
= & I(X;Y)+\min(2^{KH(X|Y)},2^{h_Y-I(X;Y)})-\epsilon_0^{''} \\
\geq & h_Y-\epsilon_0^{''} \\
\geq & h_X \qquad (A.48)
\end{aligned}$$

$$\begin{aligned}
\frac{1}{K}H(Y^K|W_1,W_2) = & \frac{1}{K}H(Y^K|W_{X1}\oplus W_{kX1}, \\
& W_{X2},W_{CX}\oplus W_{kCX} \\
& W_{Y1}\oplus W_{kY1},W_{Y2} \\
& W_{CY}\oplus W_{kCY}) \\
\geq & \frac{1}{K}\log M_{Y1}+I(X;Y)-\epsilon_0^{''} \\
= & I(X;Y)+\min(H(X|Y), \\
& h_Y-I(X;Y))-\epsilon_0^{''} \qquad (A.49) \\
\geq & h_Y \qquad (A.50)
\end{aligned}$$

where (A.49) comes from (A.39).

Therefore (R_X, R_Y, R_{kX}, R_{kY}, h_X, h_Y) is admissible from (A.44) - (A.50).

Next the case where $h_X \leq I(X;Y)$ is considered. If $h_Y > I(X;Y)$ the following results. The codewords W_1 and W_2 and their keys W_{kX} and W_{kY} are now defined:

$$W_1 = (W_{X1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{A.51}$$

$$W_2 = (W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}) \tag{A.52}$$

$$W_{kX} = W_{kCX} \tag{A.53}$$

$$W_{kY} = (W_{kY1}, W_{kCY}) \tag{A.54}$$

$$M_{Y1} = 2^{K(h_Y - I(X;Y))} \tag{A.55}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know the W_X and W_Y that are covered with keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy that

$$\begin{aligned}
\frac{1}{K}[\log M_{kX} + \log M_{kY}] &= \frac{1}{K}[\log M_{CX} + \log M_{Y1} + \log M_{CY}] \\
&\leq I(X;Y) + \frac{1}{K}\log M_{Y1} - \epsilon_0 \\
&= I(X;Y) + h_Y - I(X;Y) - \epsilon_0 \qquad \text{(A.56)} \\
&= h_Y - \epsilon_0 \\
&\leq R_{kX} + R_{kY} + \epsilon_0 \qquad \text{(A.57)}
\end{aligned}$$

where (A.56) results from (A.55).

The security levels thus result:

$$
\begin{aligned}
& \frac{1}{K} H(X^K|W_1, W_2) \\
= \ & \frac{1}{K} H(X^K|W_{X1}, W_{X2} \\
& W_{CX} \oplus W_{kCX}, W_{Y1} \oplus W_{kY1}, W_{Y2}, \\
& W_{CY} \oplus W_{kCY}) \\
\geq \ & I(X;Y) - \epsilon_0^{'} && \text{(A.58)} \\
= \ & I(X;Y) - \epsilon_0^{'} && \text{(A.59)} \\
\geq \ & h_X - \epsilon_0^{'} && \text{(A.60)}
\end{aligned}
$$

where (A.59) results from (A.55).

$$
\begin{aligned}
& \frac{1}{K} H(Y^K|W_1, W_2) \\
= \ & \frac{1}{K} H(Y^K|W_{X1}, W_{X2} \\
& W_{CX} \oplus W_{kCX}, W_{Y1} \oplus W_{kY1}, \\
& W_{Y2}, W_{CY} \oplus W_{kCY}) \\
\geq \ & I(X;Y) + \frac{1}{K} \log M_{Y1} - \epsilon_0 && \text{(A.61)} \\
= \ & I(X;Y) + h_Y - I(X;Y) - \epsilon_0^{'} && \text{(A.62)} \\
\geq \ & h_Y - \epsilon_0^{'} && \text{(A.63)}
\end{aligned}
$$

where (A.62) holds from (A.55).

Next the case where $h_Y \leq I(X;Y)$ is considered. The codewords W_1 and W_2 and their keys W_{kX} and W_{kY} are now defined:

$$W_1 = (W_{X1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{A.64}$$

$$W_2 = (W_{Y1}, W_{Y2}, W_{CY}) \tag{A.65}$$

$$W_{kX} = W_{kCX} \tag{A.66}$$

$$M_{CX} = 2^{Kh_Y} \tag{A.67}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know the W_X and W_Y that are covered with keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy that

$$\begin{aligned}
\frac{1}{K}[\log M_{kX} + \log M_{kY}] &= \frac{1}{K}\log M_{CX} \\
&= h_Y && \text{(A.68)} \\
&\leq R_{kX} + R_{kY} && \text{(A.69)}
\end{aligned}$$

where (A.68) results from (A.67).

The security levels thus result:

$$\begin{aligned}
& \frac{1}{K}H(X^K|W_1, W_2) \\
= \; & \frac{1}{K}H(X^K|W_{X1}, W_{X2} \\
& W_{CX} \oplus W_{kCX}, W_{Y1}, W_{Y2}, W_{CY}) \\
= \; & \frac{1}{K}\log M_{CY} \\
\geq \; & h_Y && \text{(A.70)} \\
\geq \; & h_X && \text{(A.71)}
\end{aligned}$$

where (A.70) results from (A.67).

$$\begin{aligned}
\frac{1}{K}H(Y^K|W_1,W_2) &= \frac{1}{K}H(Y^K|W_{X1},W_{X2} \\
&\quad W_{CX}\oplus W_{kCX},W_{Y1},W_{Y2},W_{CY}) \\
&= \frac{1}{K}\log M_{CY} && \text{(A.72)} \\
&\geq h_Y && \text{(A.73)}
\end{aligned}$$

where (A.72) holds from (A.67).

Therefore (R_X, R_Y, R_{kX}, R_{kY}, h_X, h_Y) is admissible for $\min(h_X,h_Y)$ (A.64) - (A.73).

□

A.2 Converse parts

From Slepian-Wolf's theorem it is known that the channel rate must satisfy $R_X \geq H(X|Y)$, $R_Y \geq H(Y|X)$ and $R_X + R_Y \geq H(X,Y)$ to achieve a low error probability when decoding. Hence, only the key rates are considered in this subsection.

Converse part of Theorem 2:

$$\begin{aligned}
R_{kX} &\geq \frac{1}{K}\log M_{kX} - \epsilon \\
&\geq \frac{1}{K}H(W_{kX}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kX|W_1}) - \epsilon \\
&= \frac{1}{K}[H(W_{kX}) - I(W_{kX};W_1)] - \epsilon \\
&= \frac{1}{K}H(W_{kX}|X^K,Y^K,W_1) + I(W_{kX};W_1) \\
&+ I(W_{kX};X|Y,W_1) + I(X,Y,W_{kX}|W_1) \\
&+ I(Y,W_{kX}|X,W_1) - I(W_{kX};W_1) - \epsilon \\
&= \frac{1}{K}[H(X^K,Y^K|W_1) - H(X^K,Y^K|W_1,W_{kX})] - \epsilon \\
&\geq h_{XY} - \frac{1}{K}H(X,Y|W_1,W_{kX}) - 2\epsilon && \text{(A.74)} \\
&= h_{XY} - H(V_{CY}) - 2\epsilon \\
&= h_{XY} - 2\epsilon && \text{(A.75)}
\end{aligned}$$

where (A.74) results from equation $\frac{1}{K}H(X^K, Y^K|W_1, W_2) \leq h_{XY} + \epsilon$ as described in Chapter 4. Here, the extremes of $H(V_{CY})$ are considered in order to determine the limit for R_{kX}. When this quantity is minimum then the maximum bound of h_{XY} can be achieved.

$$\begin{aligned}
R_{kY} &\geq \frac{1}{K}\log M_{kY} - \epsilon \\
&\geq \frac{1}{K}H(W_{kY}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kY|W_2}) - \epsilon \\
&= \frac{1}{K}[H(W_{kY}) - I(W_{kY}; W_2)] - \epsilon \\
&= \frac{1}{K}H(W_{kY}|X^K, Y^K, W_2) + I(W_{kY}; W_2) \\
&+ I(W_{kY}; X|Y, W_2) + I(X, Y, W_{kY}|W_2) \\
&+ I(Y, W_{kY}|X, W_2) - I(W_{kY}; W_2) - \epsilon \\
&= \frac{1}{K}[H(X^K, Y^K|W_2) - H(X^K, Y^K|W_2, W_{kY})] - \epsilon \\
&\geq h_{XY} - \frac{1}{K}H(X^K, Y^K|W_2, W_{kY}) - 2\epsilon \qquad \text{(A.76)} \\
&= h_{XY} - H(V_{CX}) - 2\epsilon \\
&= h_{XY} - 2\epsilon \qquad \text{(A.77)}
\end{aligned}$$

where (A.76) results from equation $\frac{1}{K}H(X^K, Y^K|W_1, W_2) \leq h_{XY} + \epsilon$ as described in Chapter 4. Here, the extremes of $H(V_{CX})$ are considered in order to determine the limit for R_{kY}. When this quantity is minimum the maximum bound of h_{XY} can be achieved.

Converse part of Theorem 3:

$$\begin{aligned}
R_{kX} &\geq \frac{1}{K}\log M_{kX} - \epsilon \\
&\geq \frac{1}{K}H(W_{kX}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kX|W_1}) - \epsilon \\
&= \frac{1}{K}[H(W_{kX}) - I(W_{kX};W_1)] - \epsilon \\
&= \frac{1}{K}H(W_{kX}|X^K, W_1) + I(W_{kX};W_1) \\
&+ I(X, W_{kX}|W_1) - I(W_{kX};W_1) - \epsilon \\
&\geq \frac{1}{K}I(X^K, W_{kX}|W_1) - \epsilon \\
&= \frac{1}{K}[H(X^K|W_1) - H(X^K|W_1, W_{kX})] - \epsilon \\
&\geq h_X - H(V_{CY}) - 2\epsilon \qquad (A.78) \\
&= h_X - 2\epsilon \qquad (A.79)
\end{aligned}$$

where (A.78) results from $\frac{1}{K}H(X^K|W_1) \leq h_X + \epsilon$ described in Chapter 4. Here, the extremes of $H(V_{CY})$ are considered in order to determine the limit for R_{kX}. When this quantity is minimum the maximum bound of h_X can be achieved.

$$\begin{aligned}
R_{kY} &\geq \frac{1}{K}\log M_{kY} - \epsilon \\
&\geq \frac{1}{K}H(W_{kY}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kY|W_2}) - \epsilon \\
&= \frac{1}{K}[H(W_{kY}) - I(W_{kY};W_2)] - \epsilon \\
&= \frac{1}{K}H(W_{kY}|Y^K, W_2) + I(W_{kY};W_2) \\
&+ I(X, W_{kY}|W_2) - I(W_{kY};W_2) - \epsilon \\
&\geq \frac{1}{K}I(Y^K, W_{kY}|W_2) - \epsilon \\
&= \frac{1}{K}[H(Y^K|W_2) - H(Y^K|W_2, W_{kY})] - \epsilon \\
&\geq h_Y - H(V_{CX}) - 2\epsilon \qquad (A.80) \\
&= h_Y - 2\epsilon \qquad (A.81)
\end{aligned}$$

where (A.80) results from $\frac{1}{K}H(Y^K|W_2) \leq h_Y + \epsilon$ described in Chapter 4. Here, the extremes of $H(V_{CX})$ are considered in order to determine the limit for R_{kY}. When this quantity is minimum then the maximum bound of h_Y can be achieved.

Appendix B

Proof of Theorems 4-5

B.1 Direct parts

The prototype code $(W_X, W_Y, W_{CX}, W_{CY}$ that has been described in Chapter 4 and Appendix A is applied here.

Proof of Theorem 4. Suppose that $(R_X,\ R_Y,\ R_{kX},\ R_{kY}) \in \mathcal{R}_1$ for $h_{XY} \leq H(X,Y) - \mu_C - \mu_Y$. Without loss of generality, $h_{XY} \leq R_{kX} + R_{kY}$ is assumed. Then, from (5.47)

$$\begin{aligned} & R_X \geq H(X^K|Y^K) \\ & R_Y \geq H(Y^K|X^K) \\ & R_X + R_Y \geq H(X^K, Y^K) \end{aligned} \tag{B.1}$$

$$R_{kX} + R_{kY} \geq h_{XY} \tag{B.2}$$

Here the keys are uniform random numbers. For the first case, consider the following: $h_{XY} > I(X;Y)$.

$$M_{X1} = \min(2^{KH(X|Y)}, 2^{K(h_{XY} - I(X;Y))}) \tag{B.3}$$

$$M_{Y1} = 2^{K(h_{XY} - I(X;Y))} \tag{B.4}$$

The codewords W_1 and W_2 and the key W_{kX} and W_{kY} are now defined:

$$W_1 = (W_{X1} \oplus W_{kY1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{B.5}$$

$$W_2 = (W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}) \tag{B.6}$$

$$W_{kX} = W_{kCX} \tag{B.7}$$

$$W_{kY} = (W_{kY1}, W_{kCY}) \tag{B.8}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know W_{X1}, W_{CX}, W_{Y1} and W_{CY} as these are protected by keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy from (B.1) - (B.8), that

$$\begin{aligned}
\frac{1}{K}\log M_X + \frac{1}{K}\log M_Y &= \frac{1}{K}(\log M_{X1} + \log M_{X2} \\
&+ \log M_{CX}) + \frac{1}{K}(\log M_{Y1} \\
&+ \log M_{Y2} + \log M_{CY}) \\
&\leq H(X|Y) + H(Y|X) \\
&+ I(X;Y) + 3\epsilon_0 \\
&= H(X,Y) + 3\epsilon_0 \\
&\leq R_X + R_Y + 3\epsilon_0 \qquad \text{(B.9)}
\end{aligned}$$

$$\begin{aligned}
& \frac{1}{K}[\log M_{kX} + \log M_{kY}] \\
= \; & \frac{1}{K}[\log M_{CX} + \log M_{CY} + \log M_{Y1}] \\
\leq \; & I(X;Y) + h_{XY} - I(X;Y) - \epsilon_0 \qquad \text{(B.10)} \\
= \; & h_{XY} - \epsilon_0 \\
\leq \; & R_{kX} + R_{kY} - \epsilon_0 \qquad \text{(B.11)}
\end{aligned}$$

where (B.30) results from (B.4).

The security levels thus result:

$$\begin{aligned}
& \frac{1}{K}H(X^K, Y^K|W_1, W_2, Y^{K_2}) \\
= \;& \frac{1}{K}H(X^K, Y^K|W_{X1} \oplus W_{kY1}, W_{X2}, W_{CX} \oplus W_{kCX}, \\
& W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}, Y^{K_2}) \\
\geq \;& \frac{1}{K}H(X^K, Y^K|W_{X1}, W_{X2}, \\
& W_{Y1} \oplus W_{kY1}, W_{Y2}, Y^{K_2}) - \epsilon_0^{''} \qquad \text{(B.12)} \\
= \;& \frac{1}{K}H(X^K, Y^K|W_X, W_{Y2}, Y^{K_2}) - \epsilon_0^{''} \\
\geq \;& I(X;Y) + \frac{1}{K}\log M_{Y1} \\
- \;& \mu_C - \mu_Y - 2\epsilon_0^{'} - \epsilon_0^{''} \\
= \;& I(X;Y) + h_{XY} - I(X;Y) - \mu_C - \mu_Y \\
- \;& 2\epsilon_0^{'} - \epsilon_0^{''} \\
= \;& h_{XY} - \mu_C - \mu_Y - 2\epsilon_0^{'} - \epsilon_0^{''} \qquad \text{(B.13)}
\end{aligned}$$

where (B.12) holds because W_{CX} and W_{CY} are covered by uniform random keys and the result of Yamamoto's Lemma A2.

Therefore (R_X, R_Y, R_{kX}, R_{kY}, h_{XY}) is admissible from (B.9) - (B.13).

Next the case where: $h_{XY} \leq I(X;Y)$ is considered. The codewords and keys are now defined:

$$W_1 = (W_{X1}, W_{X2}, W_{CX} \oplus W_{kCX}) \qquad \text{(B.14)}$$

$$W_2 = (W_{Y1}, W_{Y2}, W_{CY}) \qquad \text{(B.15)}$$

$$W_{kX} = (W_{kCX}) \qquad \text{(B.16)}$$

$$M_{CX} = 2^{Kh_{XY}} \tag{B.17}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know the W_X and W_Y that are covered with keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy that

$$\begin{aligned}
\frac{1}{K}(\log M_{kX} + \log M_{kY}) &= \frac{1}{K}\log M_{CX} \\
&= h_{XY} \\
&\leq R_{kX} + R_{kY} \qquad \text{(B.18)}
\end{aligned}$$

where (B.18) results from (B.17).

The security level thus results:

$$\begin{aligned}
\frac{1}{K}H(X^K, Y^K|W_1, W_2, Y^{K_2}) &= \frac{1}{K}H(X^K, Y^K|W_{X1}, W_{X2}, \\
&\quad W_{CX} \oplus W_{kCX}, \\
&\quad W_{Y1}, W_{Y2}, W_{CY}, Y^{K_2}) \\
&\geq \frac{1}{K}\log M_{CX} - \mu_C - 2\epsilon_0^{'} \\
&= h_{XY} - \mu_C - 2\epsilon_0^{'} \qquad \text{(B.19)} \\
&\geq h_{XY} - 2\epsilon_0^{'} \qquad \text{(B.20)}
\end{aligned}$$

where (B.44) holds from (B.17).

Therefore (R_X, R_Y, R_{kX}, R_{kY}, h_{XY}) is admissible from (B.14) - (B.20).

□

Proof of Theorem 5. In the same way as Theorem 4, suppose that (R_X, R_Y, R_{kX}, R_{kY}) $\in \mathcal{R}_2$ for $h_X \leq H(X) - \mu_C$ and $h_Y \leq H(Y) - \mu_C - \mu_Y$. Without loss of generality,

$h_X \leq h_Y$ and $h_X + h_Y \leq R_{kX} + R_{kY}$ are assumed. Then, from (5.48)

$$\begin{aligned} R_X &\geq H(X^K|Y^K) \\ R_Y &\geq H(Y^K|X^K) \\ R_X + R_Y &\geq H(X^K, Y^K) \end{aligned} \tag{B.21}$$

$$\max((h_X, h_Y) \leq R_{kX} + R_{kY} \tag{B.22}$$

Consider the following: $h_X > I(X;Y)$.

$$M_{X1} = \min(2^{KH(X|Y)}, 2^{K(h_Y - I(X;Y))}) \tag{B.23}$$

$$M_{Y1} = 2^{K(h_Y - I(X;Y))} \tag{B.24}$$

The codeword W_2 and the key W_{kY} is now defined:

$$W_1 = (W_{X1} \oplus W_{kY1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{B.25}$$

$$W_2 = (W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}) \tag{B.26}$$

$$W_{kX} = W_{kCX} \tag{B.27}$$

$$W_{kY} = (W_{kY1}, W_{kCY}) \tag{B.28}$$

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy from (B.23) - (B.28), that

$$\begin{aligned}
\frac{1}{K}\log M_X + \frac{1}{K}\log M_Y &= \frac{1}{K}(\log M_{X1} + \log M_{X2} \\
&+ \log M_{CX}) + \frac{1}{K}(\log M_{Y1} \\
&+ \log M_{Y2} + \log M_{CY}) \\
&\leq H(X|Y) + H(Y|X) + I(X;Y) + 3\epsilon_0 \\
&= H(X,Y) + 3\epsilon_0 \\
&\leq R_X + R_Y + 3\epsilon_0 \qquad \text{(B.29)}
\end{aligned}$$

$$\begin{aligned}
&\frac{1}{K}[\log M_{kX} + \log M_{kY}] \\
=\ &\frac{1}{K}[\log M_{CX} + \log M_{CY} + \log M_{Y1}] \\
\leq\ &I(X;Y) + h_Y - I(X;Y) - \epsilon_0 \qquad \text{(B.30)} \\
=\ &h_Y - \epsilon_0 \\
\leq\ &R_{kX} + R_{kY} - \epsilon_0 \qquad \text{(B.31)}
\end{aligned}$$

The security levels thus result:

$$\begin{aligned}
& \frac{1}{K}H(X^K|W_1, W_2, Y^{K_2}) \\
= & \frac{1}{K}H(X^K|W_{X1} \oplus W_{kY1}, W_{X2}, W_{CX} \oplus W_{kCX} \\
& W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}, Y^{K_2}) \\
\geq & \frac{1}{K}H(X^K, Y^K|W_{X1} \oplus W_{kY1}, W_{X2}, W_{Y1} \oplus W_{kY1} \qquad \text{(B.32)} \\
& W_{Y2}, Y^{K_2}) - \epsilon_0^{''} \\
= & \frac{1}{K}H(X^K, Y^K|W_{X2}, W_{Y2}, Y^{K_2}) - \epsilon_0^{''} \\
\geq & I(X;Y) + \frac{1}{K}\log M_{X1} - \mu_C - 2\epsilon_0^{'} - \epsilon_0^{''} \\
= & I(X;Y) + \min(2^{KH(X|Y)}, 2^{h_Y - I(X;Y)}) \\
- & \mu_C - 2\epsilon_0^{'} - \epsilon_0^{''} \\
\geq & h_Y - \mu_C - 2\epsilon_0^{'} - \epsilon_0^{''} \\
\geq & h_X \qquad \text{(B.33)}
\end{aligned}$$

$$\begin{aligned}
\frac{1}{K}H(Y^K|W_1, W_2) = & \frac{1}{K}H(Y^K|W_{X1} \oplus W_{kX1}, \\
& W_{X2}, W_{CX} \oplus W_{kCX} \\
& W_{Y1} \oplus W_{kY1}, W_{Y2} \\
& W_{CY} \oplus W_{kCY}, Y^{K_2}) \\
\geq & \frac{1}{K}\log M_{Y1} + I(X;Y) - \mu_C - \mu_Y - \epsilon_0^{'} \\
= & I(X;Y) + \min(H(X|Y), h_Y - I(X;Y)) \\
- & \mu_C - \mu_Y - \epsilon_0^{'} \qquad \text{(B.34)} \\
\geq & h_Y - \epsilon_0^{'} \qquad \text{(B.35)}
\end{aligned}$$

where (B.34) comes from (B.24).

Therefore (R_X, R_Y, R_{kX}, R_{kY}, h_X, h_Y) is admissible from (B.29) - (B.35).

Next the case where $h_X \leq I(X;Y)$ is considered. If $h_Y > I(X;Y)$ the following results. The codewords W_1 and W_2 and their keys W_{kX} and W_{kY} are now defined:

$$W_1 = (W_{X1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{B.36}$$

$$W_2 = (W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}) \tag{B.37}$$

$$W_{kX} = (W_{kCX}) \tag{B.38}$$

$$W_{kY} = (W_{kY1}, W_{kCY}) \tag{B.39}$$

$$M_{Y1} = 2^{K(h_Y - I(X;Y))} \tag{B.40}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know the W_X and W_Y that are covered with keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy that

$$\begin{aligned}
\frac{1}{K}[\log M_{kX} + \log M_{kY}] &= \frac{1}{K}[\log M_{CX} + \log M_{Y1} + \log M_{CY}] \\
&\leq I(X;Y) + \frac{1}{K}\log M_{Y1} - \epsilon_0 \\
&= I(X;Y) + h_Y - I(X;Y) - \epsilon_0 \qquad \text{(B.41)} \\
&= h_Y - \epsilon_0 \\
&\leq R_{kX} + R_{kY} + \epsilon_0 \qquad \text{(B.42)}
\end{aligned}$$

where (B.41) results from (B.40).

The security levels thus result:

$$
\begin{aligned}
& \frac{1}{K} H(X^K | W_1, W_2) \\
= \; & \frac{1}{K} H(X^K | W_{X1}, W_{X2} \\
& W_{CX} \oplus W_{kCX}, W_{Y1} \oplus W_{kY1}, W_{Y2}, \\
& W_{CY} \oplus W_{kCY}, Y^{K_2}) \\
\geq \; & I(X;Y) - \mu_C - \epsilon_0^{'} && \text{(B.43)} \\
= \; & I(X;Y) - \mu_C - \epsilon_0^{'} && \text{(B.44)} \\
\geq \; & h_X - \epsilon_0^{'} && \text{(B.45)}
\end{aligned}
$$

where (B.44) results from (B.40).

$$
\begin{aligned}
& \frac{1}{K} H(Y^K | W_1, W_2) \\
= \; & \frac{1}{K} H(Y^K | W_{X1}, W_{X2} \\
& W_{CX} \oplus W_{kCX}, W_{Y1} \oplus W_{kY1}, \\
& W_{Y2}, W_{CY} \oplus W_{kCY}, Y^{K_2}) \\
\geq \; & I(X;Y) + \frac{1}{K} \log M_{Y1} \\
- \; & \mu_C - \mu_Y - \epsilon_0 && \text{(B.46)} \\
= \; & I(X;Y) + h_Y - I(X;Y) \\
- \; & \mu_C - \mu_Y - \epsilon_0^{'} && \text{(B.47)} \\
\geq \; & h_Y - \epsilon_0^{'} && \text{(B.48)}
\end{aligned}
$$

where (B.47) holds from (B.40).

Next the case where $h_Y \leq I(X;Y)$ is considered. The codewords W_1 and W_2 and their keys W_{kX} and W_{kY} are now defined:

$$W_1 = (W_{X1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{B.49}$$

$$W_2 = (W_{Y1}, W_{Y2}, W_{CY}) \tag{B.50}$$

$$W_{kX} = W_{kCX} \tag{B.51}$$

$$M_{CX} = 2^{Kh_Y} \tag{B.52}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know the W_X and W_Y that are covered with keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy that

$$\begin{aligned}
\frac{1}{K}[\log M_{kX} + \log M_{kY}] &= \frac{1}{K}\log M_{CX} \\
&= h_Y && \text{(B.53)} \\
&\leq R_{kX} + R_{kY} && \text{(B.54)}
\end{aligned}$$

where (B.53) results from (B.52).

The security levels thus result:

$$\begin{aligned}
& \frac{1}{K}H(X^K|W_1, W_2) \\
= \;& \frac{1}{K}H(X^K|W_{X1}, W_{X2} \\
& W_{CX} \oplus W_{kCX}, W_{Y1}, W_{Y2}, \\
& W_{CY}, Y^{K_2}) \\
\geq \;& h_Y - \mu_C - \epsilon_0^{'} && \text{(B.55)} \\
\geq \;& h_X - \epsilon_0^{'} && \text{(B.56)}
\end{aligned}$$

where (B.55) results from (B.52).

$$\begin{aligned}
\frac{1}{K}H(Y^K|W_1, W_2) &= \frac{1}{K}H(Y^K|W_{X1}, W_{X2} \\
&\quad W_{CX} \oplus W_{kCX}, W_{Y1}, W_{Y2}, \\
&\quad W_{CY}, Y^{K_2}) \\
&\geq h_Y - \mu_C - \mu_Y - \epsilon_0 && \text{(B.57)} \\
&\geq h_Y - \epsilon_0^{'} && \text{(B.58)}
\end{aligned}$$

where (B.57) holds from (B.52).

Therefore $(R_X,\ R_Y,\ R_{kX},\ R_{kY},\ h_X,\ h_Y)$ is admissible for $\min(h_X, h_Y)$ from (B.49) - (B.58). □

B.2 Converse parts

From Slepian-Wolf's theorem it is known that the channel rate must satisfy $R_X \geq H(X|Y)$, $R_Y \geq H(Y|X)$ and $R_X + R_Y \geq H(X,Y)$ to achieve a low error probability when decoding. Hence, only the key rates are considered in this subsection.

Converse part of Theorem 4:

$$\begin{aligned}
R_{kX} &\geq \frac{1}{K}\log M_{kX} - \epsilon \\
&\geq \frac{1}{K}H(W_{kX}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kX}|W) - \epsilon \\
&= \frac{1}{K}[H(W_{kX}) - I(W_{kX};W)] - \epsilon \\
&= \frac{1}{K}H(W_{kX}|X^K,Y^K,W) + I(W_{kX};W) \\
&+ I(W_{kX};X|Y,W) + I(X,Y,W_{kX}|W) \\
&+ I(Y,W_{kX}|X,W) - I(W_{kX};W) - \epsilon \\
&= \frac{1}{K}[H(X^K,Y^K|W) - H(X^K,Y^K|W,W_{kX})] - \epsilon \\
&\geq h_{XY} - \frac{1}{K}H(X^K,Y^K|W,W_{kX}) - \epsilon \qquad \text{(B.59)} \\
&= h_{XY} - \frac{1}{K}H(Y^K|X^K) - \mu_C - \epsilon - \epsilon_0^{''} \\
&\geq h_{XY} - \mu_C - \epsilon - \epsilon_0^{''} \qquad \text{(B.60)}
\end{aligned}$$

where $W = (W_1, W_2, Y^{K_2})$ are the wiretapped portions, (B.59) results from equation (5.43). Here, the extremes of $H(Y|X)$ and $H(W_Y)$ are considered in order to determine the limit for R_{kX}. When this quantity is minimum then the maximum bound of h_{XY} can be achieved.

$$\begin{aligned}
R_{kY} &\geq \frac{1}{K}\log M_{kY} - \epsilon \\
&\geq \frac{1}{K}H(W_{kY}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kY|W}) - \epsilon \\
&= \frac{1}{K}[H(W_{kY}) - I(W_{kY};W) - \epsilon \\
&= \frac{1}{K}H(W_{kY}|X,Y,W) + I(W_{kY};W) \\
&+ I(W_{kY};X|Y,W) + I(X,Y,W_{kY}|W) \\
&+ I(Y,W_{kY}|X,W) - I(W_{kY};W)] - \epsilon \\
&= \frac{1}{K}[H(X^K,Y^K|W) - H(X^K,Y^K|W,W_{kY})] - \epsilon \\
&\geq h_{XY} - \frac{1}{K}H(X^K,Y^K|W,W_{kY}) - \epsilon \qquad \text{(B.61)} \\
&= h_{XY} - \frac{1}{K}H(X^K|Y^K) - \mu_C - \mu_Y - \epsilon - \epsilon_0^{''} \\
&\geq h_{XY} - \mu_C - \mu_Y - \epsilon - \epsilon_0^{''} \qquad \text{(B.62)}
\end{aligned}$$

where (B.61) results from equation (5.43). Here, the extremes of $H(X|Y)$ are considered in order to determine the limit for R_{kY}. When this quantity is minimum then the maximum bound of h_{XY} can be achieved.

Converse part of Theorem 5:

$$\begin{aligned}
R_{kX} &\geq \frac{1}{K}\log M_{kX} - \epsilon \\
&\geq \frac{1}{K}H(W_{kX}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kX}|W) - \epsilon \\
&= \frac{1}{K}[H(W_{kX}) - I(W_{kX};W)] - \epsilon \\
&= \frac{1}{K}H((W_{kX}|X^K,W) + I(W_{kX};W) \\
&+ I(X,W_{kX}|W) - I(W_{kX};W) - \epsilon \\
&\geq \frac{1}{K}I(X^K,W_{kX}|W) - \epsilon \\
&= \frac{1}{K}[H(X^K|W) - H(X^K|W,W_{kX})] - \epsilon \\
&\geq h_X - H(W_{CY}) - \mu_C - \epsilon - \epsilon_0^{''} \qquad \text{(B.63)} \\
&\geq h_X - \mu_C - \epsilon - \epsilon_0^{''} \qquad \text{(B.64)}
\end{aligned}$$

where $W = (W_1, W_2)$, (B.63) results from (5.41). Here, the extremes of $H(W_{CY})$ are considered in order to determine the limit for R_{kX}. When this quantity is minimum then the maximum bound of h_X can be achieved.

$$\begin{aligned}
R_{kY} &\geq \frac{1}{K}\log M_{kY} - \epsilon \\
&\geq \frac{1}{K}H(W_{kY}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kY}|W) - \epsilon \\
&= \frac{1}{K}[H(W_{kY}) - I(W_{kY};W)] - \epsilon \\
&= \frac{1}{K}H(W_{kY}|Y^K, W) + I(W_{kY};W) \\
&+ I(X, W_{kY}|W) - I(W_{kY};W) - \epsilon \\
&\geq \frac{1}{K}I(Y^K, W_{kY}|W) - \epsilon \\
&= \frac{1}{K}[H(Y^K|W) - H(Y^K|W, W_{kY})] - \epsilon \\
&\geq h_Y - H(W_{CX}) - \mu_C - \mu_Y - \epsilon - \epsilon_0^{''} \qquad \text{(B.65)} \\
&\geq h_Y - \mu_C - \mu_Y - \epsilon - \epsilon_0^{''} \qquad \text{(B.66)}
\end{aligned}$$

where (B.65) results from (5.42). The same consideration as above for $H(Y^{K_2})$ is presented here. Here, the extremes of $H(W_{CX})$ are considered in order to determine the limit for R_{kY}. When this quantity is minimum the maximum bound of h_Y can be achieved.

Appendix C

Proof of Theorems 6-7

This section initially proves the direct parts of Theorems 6 - 7 and thereafter the converse parts.

C.1 Direct parts

The prototype code $(W_X, W_Y, W_{CX}, W_{CY})$ described in Chapter 4 and Appendix A is applied here.

Proof of Theorem 6. Suppose that (R_X, R_Y, R_{KX}, R_{KY}) $\in \mathcal{R}_1$ for $h_{XY} \leq H(X,Y) - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z)$. Then, from (6.40)

$$\begin{aligned} R_X &\geq H(X^K|Y^K) \\ R_Y &\geq H(Y^K|X^K) \\ R_X + R_Y &\geq H(X^K, Y^K) \end{aligned} \tag{C.1}$$

$$R_{kX} + R_{kY} \geq h_{XY} \tag{C.2}$$

Here the keys are uniform random numbers. For the first case, consider the following: $h_{XY} > I(X;Y)$.

$$M_{X1} = \min(2^{KH(X|Y)}, 2^{K(h_{XY}-I(X;Y))}) \tag{C.3}$$

$$M_{Y1} = 2^{K(h_{XY}-I(X;Y))} \tag{C.4}$$

The codewords W_1 and W_2 and the key $W_{kX}$and W_{kY} are now defined:

$$W_1 = (W_{X1} \oplus W_{kY1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{C.5}$$

$$W_2 = (W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}) \tag{C.6}$$

$$W_{kX} = W_{kCX} \tag{C.7}$$

$$W_{kY} = (W_{kY1}, W_{kCY}) \tag{C.8}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know W_{X1}, W_{CX} W_{Y1} and W_{CY} as these are protected by keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy from (C.1) - (C.8), that

$$\begin{aligned}
\frac{1}{K}\log M_X + \frac{1}{K}\log M_Y &= \frac{1}{K}(\log M_{X1} + \log M_{X2} \\
&+ \log M_{CX}) + \frac{1}{K}(\log M_{Y1} \\
&+ \log M_{Y2} + \log M_{CY}) \\
&\leq H(X|Y) + H(Y|X) \\
&+ I(X;Y) + 3\epsilon_0 \\
&= H(X,Y) + 3\epsilon_0 \\
&\leq R_X + R_Y + 3\epsilon_0 \qquad \text{(C.9)}
\end{aligned}$$

$$\begin{aligned}
&\frac{1}{K}[\log M_{kX} + \log M_{kY}] \\
= \ &\frac{1}{K}[\log M_{CX} + \log M_{CY} + \log M_{Y1}] \\
\leq \ &I(X;Y) + h_{XY} - I(X;Y) - \epsilon_0 \qquad \text{(C.10)} \\
= \ &h_{XY} - \epsilon_0 \\
\leq \ &R_{kX} + R_{kY} - \epsilon_0 \qquad \text{(C.11)}
\end{aligned}$$

where (C.10) results from (C.4).

The security levels thus result:

$$
\begin{aligned}
& \frac{1}{K}H(X^K, Y^K|W_1, W_2, Z^\mu) \\
= \; & \frac{1}{K}H(X^K, Y^K|W_{X1} \oplus W_{kY1}, W_{X2}, W_{CX} \oplus W_{kCX}, \\
& W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}, Z^\mu) \\
\geq \; & \frac{1}{K}H(X^K, Y^K|W_{X1}, W_{X2}, \\
& W_{Y1} \oplus W_{kY1}, W_{Y2}) - \epsilon_0^{''} && \text{(C.12)} \\
= \; & \frac{1}{K}H(X^K, Y^K|W_X, W_{Y2}, Z^\mu) - \epsilon_0^{''} \\
\geq \; & I(X;Y) + \frac{1}{K}\log M_{Y1} \\
- \; & \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - 2\epsilon_0^{'} - \epsilon_0^{''} \\
= \; & I(X;Y) + h_{XY} - I(X;Y) - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) \\
- \; & 2\epsilon_0^{'} - \epsilon_0^{''} \\
= \; & h_{XY} - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - 2\epsilon_0^{'} - \epsilon_0^{''} && \text{(C.13)}
\end{aligned}
$$

where (C.12) holds because W_{CX} and W_{CY} are covered by uniform random keys and the result of Yamamoto's Lemma A2.

Therefore (R_X, R_Y, R_{kX}, R_{kY}, h_{XY}) is admissible from (C.9) - (C.13).

Next the case where: $h_{XY} \leq I(X;Y)$ is considered. The codewords and keys are now defined:

$$W_1 = (W_{X1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{C.14}$$

$$W_2 = (W_{Y1}, W_{Y2}, W_{CY}) \tag{C.15}$$

$$W_{kX} = (W_{kCX}) \tag{C.16}$$

$$M_{CX} = 2^{Kh_{XY}} \tag{C.17}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know the W_X and W_Y that are covered with keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy that

$$\begin{aligned} \frac{1}{K}[\log M_{kX} + \log M_{kY}] &= \frac{1}{K}\log M_{CX} \\ &= h_{XY} \\ &\leq R_{kX} + R_{kY} \end{aligned} \tag{C.18}$$

where (C.18) results from (C.17).

The security level thus results:

$$\begin{aligned} \frac{1}{K}H(X^K, Y^K|W_1, W_2, Z^\mu) &= \frac{1}{K}H(X^K, Y^K|W_{X1}, W_{X2}, \\ & W_{CX} \oplus W_{kCX}, \\ & W_{Y1}, W_{Y2}, W_{CY}, Z^\mu) \\ &\geq \frac{1}{K}\log M_{CX} - \alpha_{CX} - \alpha_{CY} \\ &+ I(X;Y;Z) - \epsilon_0^{'} \\ &= h_{XY} - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) \\ &- \epsilon_0^{'} \end{aligned} \tag{C.19}$$

where (C.19) holds from (C.17).

Therefore (R_X, R_Y, R_{kX}, R_{kY}, h_{XY}) is admissible from (C.14) - (C.19).

□

Theorem 7 proof. In the same way as Theorem 6, suppose that (R_X, R_Y, R_{kX}, R_{kY}) $\in \mathcal{R}_2$ for $h_X \leq H(X) - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z)$ and $h_Y \leq H(Y) - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z)$.

Without loss of generality, we assume that $h_X \leq h_Y$. Then, from (6.41)

$$\begin{aligned} R_X &\geq H(X^K|Y^K) \\ R_Y &\geq H(Y^K|X^K) \\ R_X + R_Y &\geq H(X^K, Y^K) \end{aligned} \tag{C.20}$$

$$R_{kX} + R_{kY} \geq \max(h_X, h_Y) \tag{C.21}$$

Consider the following: $h_X > I(X;Y)$.

$$M_{X1} = \min(2^{KH(X|Y)}, 2^{K(h_Y - I(X;Y))}) \tag{C.22}$$

$$M_{Y1} = 2^{K(h_Y - I(X;Y))} \tag{C.23}$$

The codeword W_2 and the key W_{kY} is now defined:

$$W_1 = (W_{X1} \oplus W_{kY1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{C.24}$$

$$W_2 = (W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}) \tag{C.25}$$

$$W_{kX} = W_{kCX} \tag{C.26}$$

$$W_{kY} = (W_{kY1}, W_{kCY}) \tag{C.27}$$

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy from (C.22) - (C.27), that

$$\begin{aligned}
\frac{1}{K}\log M_X + \frac{1}{K}\log M_Y &= \frac{1}{K}(\log M_{X1} + \log M_{X2} \\
&+ \log M_{CX}) + \frac{1}{K}(\log M_{Y1} \\
&+ \log M_{Y2} + \log M_{CY}) \\
&\leq H(X|Y) + H(Y|X) \\
&+ I(X;Y) + 3\epsilon_0 \\
&= H(X,Y) + 3\epsilon_0 \\
&\leq R_X + R_Y + 3\epsilon_0 \qquad \text{(C.28)}
\end{aligned}$$

$$\begin{aligned}
&\frac{1}{K}[\log M_{kX} + \log M_{kY}] \\
= \;&\frac{1}{K}[\log M_{CX} + \log M_{CY} + \log M_{Y1}] \\
\leq \;& I(X;Y) + h_Y - I(X;Y) - \epsilon_0 \qquad \text{(C.29)} \\
= \;& h_Y - \epsilon_0 \\
\leq \;& R_{kX} + R_{kY} - \epsilon_0 \qquad \text{(C.30)}
\end{aligned}$$

The security levels thus result:

$$\begin{aligned}
& \frac{1}{K}H(X^K|W_1, W_2, Z^\mu) \\
= \;& \frac{1}{K}H(X^K|W_{X1} \oplus W_{kY1}, W_{X2}, W_{CX} \oplus W_{kCX}, \\
& W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}, Z^\mu) \\
\geq \;& \frac{1}{K}H(X^K, Y^K|W_{X1} \oplus W_{kY1}, W_{X2}, W_{Y1} \oplus W_{kY1} && \text{(C.31)} \\
& W_{Y2}, Z^\mu) - \epsilon_0^{''} \\
= \;& \frac{1}{K}H(X^K, Y^K|W_{X2}, W_{Y2}, Z^\mu) - \epsilon_0^{''} \\
\geq \;& I(X;Y) + \frac{1}{K}\log M_{X1} - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) \\
& && \text{(C.32)} \\
- \;& 2\epsilon_0^{'} - \epsilon_0^{''} \\
= \;& I(X;Y) + \min(2^{KH(X|Y)}, 2^{h_Y - I(X;Y)}) \\
- \;& \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - 2\epsilon_0^{'} - \epsilon_0^{''} \\
\geq \;& h_Y - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - 2\epsilon_0^{'} - \epsilon_0^{''} \\
\geq \;& h_X && \text{(C.33)}
\end{aligned}$$

$$\begin{aligned}
\frac{1}{K}H(Y^K|W_1, W_2) \;=\;& \frac{1}{K}H(Y^K|W_{X1} \oplus W_{kX1}, W_{X2}, W_{CX} \oplus W_{kCX}, \\
& W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}, Z^\mu) \\
\geq \;& \frac{1}{K}\log M_{Y1} + I(X;Y) - \alpha_{CX} \\
- \;& \alpha_{CY} + I(X;Y;Z) - \epsilon_0^{'} \\
= \;& I(X;Y) + \min(H(X|Y), h_Y - I(X;Y)) \\
- \;& \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - \epsilon_0^{'} && \text{(C.34)} \\
\geq \;& h_Y - \epsilon_0^{'} && \text{(C.35)}
\end{aligned}$$

where (C.34) comes from (C.23).

Therefore (R_X, R_Y, R_{kX}, R_{kY}, h_X, h_Y) is admissible from (C.28) - (C.35).

Next the case where $h_X \leq I(X;Y)$ is considered. If $h_Y > I(X;Y)$ the following results. The codewords W_1 and W_2 and their keys W_{kX} and W_{kY} are now defined:

$$W_1 = (W_{X1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{C.36}$$

$$W_2 = (W_{Y1} \oplus W_{kY1}, W_{Y2}, W_{CY} \oplus W_{kCY}) \tag{C.37}$$

$$W_{kX} = (W_{kCX}) \tag{C.38}$$

$$W_{kY} = (W_{kY1}, W_{kCY}) \tag{C.39}$$

$$M_{Y1} = 2^{K(h_Y - I(X;Y)})} \tag{C.40}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know the W_X and W_Y that are covered with keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy that

$$\begin{aligned}
\frac{1}{K}[\log M_{kX} + \log M_{kY}] &= \frac{1}{K}[\log M_{CX} + \log M_{Y1} + \log M_{CY}] \\
&\leq I(X;Y) + \frac{1}{K}\log M_{Y1} - \epsilon_0 \\
&= I(X;Y) + h_Y - I(X;Y) - \epsilon_0 && \text{(C.41)} \\
&= h_Y - \epsilon_0 \\
&\leq R_{kX} + R_{kY} + \epsilon_0 && \text{(C.42)}
\end{aligned}$$

where (C.41) results from (C.40).

The security levels thus result:

$$\begin{aligned}
& \frac{1}{K}H(X^K|W_1, W_2) \\
= \ & \frac{1}{K}H(X^K|W_{X1}, W_{X2} \\
& W_{CX} \oplus W_{kCX}, W_{Y1} \oplus W_{kY1}, W_{Y2}, \\
& W_{CY} \oplus W_{kCY}, Z^{\mu}) \\
\geq \ & I(X;Y) - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - \epsilon_0^{'} && \text{(C.43)} \\
= \ & I(X;Y) - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - \epsilon_0^{'} && \text{(C.44)} \\
\geq \ & h_X - \epsilon_0^{'} && \text{(C.45)}
\end{aligned}$$

where (C.44) results from (C.40).

$$\begin{aligned}
& \frac{1}{K}H(Y^K|W_1, W_2) \\
= \ & \frac{1}{K}H(Y^K|W_{X1}, W_{X2} \\
& W_{CX} \oplus W_{kCX}, W_{Y1} \oplus W_{kY1}, \\
& W_{Y2}, W_{CY} \oplus W_{kCY}, Z^{\mu}) \\
\geq \ & I(X;Y) + \frac{1}{K}\log M_{Y1} \\
- \ & \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - \epsilon_0 && \text{(C.46)} \\
= \ & I(X;Y) + h_Y - I(X;Y) \\
- \ & \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - \epsilon_0^{'} && \text{(C.47)} \\
\geq \ & h_Y - \epsilon_0^{'} && \text{(C.48)}
\end{aligned}$$

where (C.47) holds from (C.40).

Next the case where $h_Y \leq I(X;Y)$ is considered. The codewords W_1 and W_2 and their keys W_{kX} and W_{kY} are now defined:

$$W_1 = (W_{X1}, W_{X2}, W_{CX} \oplus W_{kCX}) \tag{C.49}$$

$$W_2 = (W_{Y1}, W_{Y2}, W_{CY}) \tag{C.50}$$

$$W_{kX} = W_{kCX} \tag{C.51}$$

$$M_{CX} = 2^{Kh_Y} \tag{C.52}$$

where $W_\alpha \in I_{M_\alpha} = \{0, 1, \ldots, M_\alpha - 1\}$. The wiretapper will not know the W_X and W_Y that are covered with keys.

In this case, R_X, R_Y, R_{kX} and R_{kY} satisfy that

$$\begin{aligned}
\frac{1}{K}[\log M_{kX} + \log M_{kY}] &= \frac{1}{K}\log M_{CX} \\
&= h_Y && \text{(C.53)} \\
&\leq R_{kX} + R_{kY} && \text{(C.54)}
\end{aligned}$$

where (C.53) results from (C.52).

The security levels thus result:

$$\begin{aligned}
& \frac{1}{K} H(X^K | W_1, W_2, Z^\mu) \\
= \ & \frac{1}{K} H(X^K | W_{X1}, W_{X2} \\
& W_{CX} \oplus W_{kCX}, W_{Y1}, W_{Y2}, W_{CY}, Z^\mu) \\
\geq \ & h_Y - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - \epsilon_0^{'} && \text{(C.55)} \\
\geq \ & h_X - \epsilon_0^{'} && \text{(C.56)}
\end{aligned}$$

where (C.55) results from (C.52).

$$
\begin{aligned}
\frac{1}{K}H(Y^K|W_1, W_2, Z^\mu) &= \frac{1}{K}H(Y^K|W_{X1}, W_{X2} \\
&\quad W_{CX} \oplus W_{kCX}, W_{Y1}, W_{Y2}, \\
&\quad W_{CY}, Z^\mu) \\
&\geq \frac{1}{K}\log M_{CY} - \alpha_{CX} - \alpha_{CY} \\
&+ I(X;Y;Z) - \epsilon_0^{'} \qquad (C.57) \\
&\geq h_Y - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) \qquad (C.58)
\end{aligned}
$$

where (C.57) holds from (C.52).

Therefore (R_X, R_Y, R_{kX}, R_{kY}, h_X, h_Y) is admissible for $\min(h_X, h_Y)$ from (C.49) - (C.58). □

C.2 Converse parts

From Slepian-Wolf's theorem it is known that the channel rate must satisfy $R_X \geq H(X|Y)$, $R_Y \geq H(Y|X)$ and $R_X + R_Y \geq H(X, Y)$ to achieve a low error probability when decoding. Hence, only the key rates are considered in this subsection.

Converse part of Theorem 6:

$$\begin{aligned}
R_{kX} &\geq \frac{1}{K}\log M_{kX} - \epsilon \\
&\geq \frac{1}{K}H(W_{kX}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kX}|W) - \epsilon \\
&= \frac{1}{K}[H(W_{kX}) - I(W_{kX};W)] - \epsilon \\
&= \frac{1}{K}H(W_{kX}|X^K, Y^K, W) + I(W_{kX};W) \\
&+ I(W_{kX};X|Y,W) + I(X,Y,W_{kX}|W) \\
&+ I(Y,W_{kX}|X,W) - I(W_{kX};W) - \epsilon \\
&= \frac{1}{K}[H(X^K,Y^K|W) - H(X^K,Y^K|W,W_{kX})] - \epsilon \\
&\geq h_{XY} - \frac{1}{K}H(X^K,Y^K|W,W_{kX}) - \epsilon \qquad \text{(C.59)} \\
&= h_{XY} - \frac{1}{K}H(Y^K|X^K) - \alpha_{CX} - \alpha_{CY} \\
&+ I(X;Y;Z) - \epsilon - \epsilon_0^{''} \\
&\geq h_{XY} - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - \epsilon - \epsilon_0^{''} \qquad \text{(C.60)}
\end{aligned}$$

where $W = (W_1, W_2, Z^{\mu})$ are the wiretapped portions, (C.59) results from equation (6.36). Here, the extremes of $H(Y|X)$ and $H(W_Y)$ are considered in order to determine the limit for R_{kX}. When this quantity is minimum then the maximum bound of h_{XY} can be achieved.

$$
\begin{aligned}
R_{kY} &\geq \frac{1}{K}\log M_{kY} - \epsilon \\
&\geq \frac{1}{K}H(W_{kY}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kY|W}) - \epsilon \\
&= \frac{1}{K}[H(W_{kY}) - I(W_{kY};W) - \epsilon \\
&= \frac{1}{K}H(W_{kY}|X,Y,W) + I(W_{kY};W) \\
&+ I(W_{kY};X|Y,W) + I(X,Y,W_{kY}|W) \\
&+ I(Y,W_{kY}|X,W) - I(W_{kY};W)] - \epsilon \\
&= \frac{1}{K}[H(X^K,Y^K|W) - H(X^K,Y^K|W,W_{kY})] - \epsilon \\
&\geq h_{XY} - \frac{1}{K}H(X^K,Y^K|W,W_{kY}) - \epsilon \qquad \text{(C.61)} \\
&= h_{XY} - \frac{1}{K}H(X^K|Y^K) - \alpha_{CX} - \alpha_{CY} \\
&+ I(X;Y;Z) - \epsilon - \epsilon_0^{''} \\
&\geq h_{XY} - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - \epsilon - \epsilon_0^{''} \qquad \text{(C.62)}
\end{aligned}
$$

where (C.61) results from equation (6.36). Here, the extremes of $H(V_{CX})$ are considered in order to determine the limit for R_{kY}. When this quantity is minimum then the maximum bound of h_{XY} can be achieved.

Converse part of Theorem 7:

$$\begin{aligned}
R_{kX} &\geq \frac{1}{K}\log M_{kX} - \epsilon \\
&\geq \frac{1}{K}H(W_{kX}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kX}|W) - \epsilon \\
&= \frac{1}{K}[H(W_{kX}) - I(W_{kX};W)] - \epsilon \\
&= \frac{1}{K}H((W_{kX}|X^K, W) + I(W_{kX};W) \\
&+ I(X, W_{kX}|W) - I(W_{kX};W) - \epsilon \\
&\geq \frac{1}{K}I(X^K, W_{kX}|W) - \epsilon \\
&= \frac{1}{K}[H(X^K|W) - H(X^K|W, W_{kX})] - \epsilon \\
&\geq h_X - H(W_{CY}) - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) \\
&- \epsilon - \epsilon_0^{''} \qquad \text{(C.63)} \\
&\geq h_X - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - \epsilon - \epsilon_0^{''} \qquad \text{(C.64)}
\end{aligned}$$

where $W = (W_1, W_2, Z^{\mu})$, (C.63) results from (6.34). Here, the extremes of $H(W_{CY})$ are considered in order to determine the limit for R_{kX}. When this quantity is minimum then the maximum bound of h_X can be achieved.

$$
\begin{aligned}
R_{kY} &\geq \frac{1}{K}\log M_{kY} - \epsilon \\
&\geq \frac{1}{K}H(W_{kY}) - \epsilon \\
&\geq \frac{1}{K}H(W_{kY}|W) - \epsilon \\
&= \frac{1}{K}[H(W_{kY}) - I(W_{kY};W)] - \epsilon \\
&= \frac{1}{K}H(W_{kY}|Y^K, W) + I(W_{kY};W) \\
&+ I(X, W_{kY}|W) - I(W_{kY};W) - \epsilon \\
&\geq \frac{1}{K}I(Y^K, W_{kY}|W) - \epsilon \\
&= \frac{1}{K}[H(Y^K|W) - H(Y^K|W, W_{kY})] - \epsilon \\
&\geq h_Y - H(W_{CX}) - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) \\
&- \epsilon - \epsilon_0^{''} \qquad (C.65) \\
&\geq h_Y - \alpha_{CX} - \alpha_{CY} + I(X;Y;Z) - \epsilon - \epsilon_0^{''} \qquad (C.66)
\end{aligned}
$$

where (C.65) results from (6.35). The same consideration as above for $H(Z^\mu)$ is presented here. Here, the extremes of $H(W_{CX})$ are considered in order to determine the limit for R_{kY}. When this quantity is minimum then the maximum bound of h_Y can be achieved.

Bibliography

[1] R. Yeung, *Information Theory and Network Coding.* Springer, 2008.

[2] E. Yang, D. He, T. Uyematsu, and R. Yeung, "Universal Multiterminal Source Coding Algorithms with Asymptotically Zero Feedback: Fixed Database Case," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5575 – 5590, December 2008.

[3] A. Vinck, "Applications of coding and information theory in biometrics," in *19th European Signal Processsing Conference*, August 2011, pp. 2254 – 2258.

[4] T. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. John Wiley and sons, 2006.

[5] H. Yamamoto, "Coding Theorems for Shannon's Cipher System with Correlated Source Ouputs, and Common Information," *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 85 – 95, January 1994.

[6] S. Rouayheb, E. Soljanin, and A. Sprintson, "Secure Network Coding for Wiretap Networks of Type II," *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1361 – 1371, March 2012.

[7] V. Wei, "Generalized Hamming Weights for Linear Codes," *IEEE Transactions on Information Theory,*, vol. 37, no. 5, pp. 1412 – 1418, September 1991.

[8] G. Mark and N. Su, "Making infrastructure visible for nomadic work," *Pervasive and Mobile Computing*, pp. 312 – 323, 2010.

[9] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of mobile ad hoc networks: Applications and challenges," *Ghent University, Belgium, Department of Information Technology*, pp. 60 – 66.

[10] A. Goldsmith, *Wireless Communications*, 1st ed. United States of America: Cambridge University Press, 2005.

[11] P. Del and C. Landi, "Real-time smart meter with embedded web server capability," in *IEEE International Conference on Instrumentation and Measurement Technology*, 2012, pp. 682 – 687.

[12] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1437 – 1443, September 2012.

[13] W. Sun and S. Rane, "On information leakage during secure verification of compatibility between signals," in *Canadian Workshop on Information Theory*, June 2009, pp. 75 – 78.

[14] N. Merhav, "Shannon's Secrecy System With Informed Receivers and its Application to Systematic Coding for Wiretapped Channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2723 – 2734, June 2008.

[15] C. Shannon, "A Mathematical Theory of Communication," *The Bell System Technical Journal*, vol. 27, p. 623–656, October 1984.

[16] D. He, A. Jagmohan, and L. Ligang, "Secure collaboration using Slepian-Wolf codes," in *15th IEEE International Conference on Image Processing*, 2008, pp. 2216 – 2219.

[17] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471 – 480, July 1973.

[18] S. Draper, C. Cheng, and A. Sahai, "Sequential Random Binning for Streaming Distributed Source Coding," in *International Symposium on Information Theory*, 2005, pp. 1396 – 1400.

[19] S. Draper, A. Khisti, E. Martinian, and A. Vetro, "Secure storage of fingerprint biometrics using Slepian-Wolf codes," in *Information Theory and Apps. Workshop, UCSD*, 2007.

[20] V. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via Sources and Channels," *IEEE Transactions on Information Theory*, vol. 58, no. 11, pp. 6747 – 6765, November 2012.

[21] J. K. Wolf and B. M. Kurkoski, “Slepian-Wolf coding,” *Scholarpedia*, vol. 3, no. 11, p. 6789, 2008.

[22] S. Wei and S. Rane, “On Information Leakage During Secure Verification of Compatibility between Signals,” in *11th Annual Canadian Conference on Information Theory*, 2009, pp. 75 – 78.

[23] J. Villard, P. Piantanida, and S. Shamai, “Secure Transmission of Sources Over Noisy Channels With Side Information at the Receivers,” *IEEE Transactions of Information Thory*, vol. 60, no. 1, pp. 713 – 739, January 2014.

[24] R. Ahlswede and I. Csiszar, “Common Randomness in Information Theory and Cryptography - Part 1: Secrect Sharing,” *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121 – 1132, July 1993.

[25] M. Johnson, P. Ishwar, and V. Prabhakaran, “On Compressing Encrypted Data,” *IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 2992 – 3006, 2004.

[26] J. Villard and P. Piantanida, “Secure Multiterminal Source Coding With Side Information at the Eavesdropper,” *IEEE Transactions on Information Theory*, vol. 59, no. 6, pp. 3668 – 3692, June 2013.

[27] U. Maurer, “Secret Key Agreement by Public Discussion from Common Information,” *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733 – 742, May 1993.

[28] T. Ho, M. Médard, M. Effros, and R. Koetter, “Network coding for correlated sources,” in *Proceedings of Conference for Information Science and Systems*, 2004, pp. 1 – 6.

[29] J. Barros and S. Servetto, “Netowrk Information Flow with Correlated Sources,” *IEEE Transactions on Information Theory*, vol. 52, no. 1, pp. 155 – 170, January 2006.

[30] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, “Extracting Correlations,” in *50th Annual IEEE Symposium on Foundations of Computer Science*, 2009, pp. 261 – 270.

[31] A. Bogdanov and E. Mossel, “On Extracting Common Random Bits from Correlated Sources,” in *IEEE Transactions on Informaiton Theory*, 2011, pp. 6351 – 6355.

[32] K. Prasad, S. Soni, T. Faruquie, and L. Subramaniam, “Data Consolidation Solution for Internal Security Needs,” in *IEEE Internation Conference on Service Operations and Logistics, and Informatics (SOLI)*, 2012, pp. 84 – 89.

[33] B. Dai, A. Vinck, Y. Luo, and Z. Zhuang, “Capacity Region of Non-degraded Wiretap Channel with Noiseless Feedback,” in *IEEE International Symposium on Information Theory*, 2012, pp. 244 – 248.

[34] R. Ahlswede and J. Korner, “Source coding with side information and a converse for degraded broadcast channels,” *IEEE Transactions on Information Theory*, vol. 21, no. 6, pp. 629 – 637, November 1975.

[35] L. Grokop, A. Sahai, and M. Gastpar, “Discriminatory source coding for a noiseless broadcast channel,” in *International Syposium on Infomation Theory*, 2005, pp. 77 – 81.

[36] Y. Hayashi and H. Yamamoto, “Coding Theorems for the Shannon Cipher System With a Guessing Wiretapper and Correlated Source Outputs,” in *IEEE Transactions on Information Theory*, June 2008, pp. 2808 – 2817.

[37] H. Yamamoto, “Coding Theorem for Secret Sharing Communication Systems with Two Noisy Channels,” *IEEE Transactions on Information Theory*, vol. 35, no. 3, pp. 572 – 578, May 1989.

[38] ——, “On Secret Sharing Communication Systems with Two or Three Channels,” *IEEE Transactions on Information Theory*, vol. 32, no. 3, pp. 387 – 393, May 1986.

[39] M. Hanawal and R. Sundaresan, “The Shannon Cipher System with a Guessing Wiretapper: General Sources,” in *2009 International Symposium on Information Theory*, Seoul, Korea, July 2009, pp. 1949 – 1953.

[40] H. Yamamoto, “Rate-Distortion Theory for the Shannon Cipher System,” *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827 – 835, May 1997.

[41] V. Aggarwal, L. Lai, A. Calderbank, and H. Poor, “Wiretap Channel Type II with an Active Eavesdropper,” in *IEEE International Symposium on Information Theory*, June 2008, pp. 1944 – 1948.

[42] N. Cai and R. Yeung, “Secure Network Coding on a Wiretap Network,” *IEEE Transactions on Information Theory,*, vol. 57, no. 1, pp. 424 – 435, January 2011.

[43] M. Bloch, R. Narasimha, and S. McLaughlin, “Network security for client-server architecture using wiretap codes,” *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 404 – 413, September 2008.

[44] D. Silva and R. Kschischang, “Security for wiretap networks via rank-metric codes,” in *IEEE International Symposium on Information Theory*, July 2008, pp. 176 – 180.

[45] L. Ozarow and A. Wyner, “Wire-Tap Channel II,” in *Advances in Cryptology - EUROCRYPT*, 1985, pp. 33 – 50.

[46] C. Mitrpant, A. Vinck, and Y. Luo, “An Achievable Region for the Gaussian Wiretap Channel With Side Information,” *IEEE Transactions on Information Theory*, vol. 52, no. 5, May 2006.

[47] Y. Luo, C. Mitpant, and A. Vinck, “Some New Characteristics on the Wiretap Channel of Type II,” *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 1222 – 1229, March 2005.

[48] Z. Zhang, “Wiretap networks ii with partial information leakage,” in *Fourth International Conference on Communications and Networking (ChinaCOM)*, August 2009, pp. 1 – 5.

[49] F. Cheng, R. Yeung, and K. Shum, “Imperfect Secrecy in Wiretap Channel II,” in *IEEE International Symposium on Information Theory*, 2012, pp. 71 – 75.

[50] A. V. B Dai, Y Luo, “Wiretap Channel with Side Information from Part of Encoder,” in *IFIP International Conference on Network and Parallel Computing*, 2008, pp. 353 – 357.

[51] R. Balmahoon and L. Cheng, “Information Leakage of Correlated Source Coded Sequences over Wiretap Channel,” in *arXiv*, no. 1401.6264, 2014, pp. 1 – 20.

[52] C. Ngai, R. Yeung, and Z. Zhang, "Network generalized hamming weight," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1136 – 1143, February 2011.

[53] S. Pradhan and K. Ramchandran, "Distributed Source Coding using Syndromes (DISCUS): Design and Construction," in *Data Compression Conference*, 1999, pp. 158 – 167.

[54] Y. Yang, S. Cheng, Z. Xiong, and Z. Wei, "Wyner-Ziv coding based on TCQ and LDPC codes," *Asilomar*, pp. 825 – 829, 2003.

[55] S. Pradhan and K. Ramchandran, "Generalized Coset Codes for Distributed Binning," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3457 – 3474, October 2005.

[56] A. Liveris, Z. Xiong, and C. Georghiades, "Nested Convolutional/Turbo Codes for the Binary Wyner-Ziv Problem," in *International Conference on Image Processing*, September 2003, pp. 601 – 604.

[57] R. Ma and S. Cheng, "Zero-Error Slepian-Wolf Coding of Confined-Correlated Sources with Deviation Symmetry," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8195 – 8209, December 2013.

[58] V. Stankovic, A. Liveris, Z. Xiong, and C. Georghiades, "Design of Slepian Wolf Codes by Channel Code Partitioning," in *IEEE Data Compression Conference*, 2004, pp. 302 – 311.

[59] S. Ho, "Markov Lemma for Countable Alphabets," in *IEEE International Symposium on Information Theory*, 2010, pp. 1448 – 1452.

[60] J. Villard, P. Piantanida, and S. Shamai, "Secure Lossy Source-Channel Wiretapping with Side Information at the Receiving Terminals," in *IEEE International Symposium on Information Theory*, 2011, pp. 1141 – 1145.

[61] ——, "Hybrid Digital/Analog Schemes for Secure Transmission with Side Information," in *IEEE Information Theory Workshop*, 2011, pp. 678 – 682.

[62] R. Balmahoon, H. Vinck, and L. Cheng, "Information Leakage for Correlated Sources with Compromised Source Symbols over Wiretap Channel II," in *52nd Annual Allerton Conference on Communication, Control and Computing*, October 2014.

[63] R. Balmahoon and L. Cheng, "Information Leakage of Heterogeneous Encoded Correlated Sequences over an Eavesdropped Channel," in *IEEE International Symposium on Information Theory.* Hong Kong, China, June 2015.