# Implementation of OFDM Encryption and a New Frequency Hopping System

by

Yunjie Yi

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2018

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

## Abstract

As the rapid growth of wireless communication, physical layer security becomes important recently. Unlike wired transmissions, the nature of wireless transmissions makes the transmitted signals over the channel easily to be eavesdropped and jammed by malicious adversaries. The eavesdropper posts a significant threat to the privacy of public people, and the jamming attack blocks the wireless transmission. Therefore, privacy and reliability of the wireless communication system are easily compromised compared to the wired communication system. Consequently, wireless network security has attracted public attention in the recent years. Wireless networks can be secured in all layers of a network protocol stack which include application, transport, network, data link and physical layers. This thesis focuses on the physical layer security in wireless communication. Specifically, the physical layer security we are focusing on has two significant branches which are orthogonal frequency-division multiplexing (OFDM) related security system and frequency hopping (FH) system. The former one is to prevent transmitting information from stealing, and the latter one focuses on preventing jamming attacks. It is commonly known that OFDM is widely used in wireless communication systems, including WIFI and cellular system. In the first part of this thesis, we use software defined radio to implement an existing OFDM encryption scheme called *OFDM Enc* in IEEE 802.11a standard, and the implementations are done in microwave anechoic chamber and laboratory environment separately. Based on the implementation performed in the GNU radio, we find a multipath boundary in the *OFDM Enc*. In the second part of this thesis, we propose a new FH system named *randomly selective m-sequence based BLADES system*. Specifically, the collision properties of two distinct binary primitive polynomials of the same degree for the new FH system have been analysed and simulated.

# Acknowledgements

I would like to express my sincere thanks to Prof. Gong for leading me into the filed of communication security and her patient guidance in the last two years. Particularly, I remember that I first came to Waterloo without any background knowledge in the field of communication security. Prof. Gong supported me with professional knowledge and continuous encouragement when I encountered endless problems and challenges in the project. She is an excellent supervisor who enriches my mind and broadens my view, and I could not finish the project without her inspiration.

Meanwhile, I would like to express my appreciation to Dr. Xuan He who worked with me on the new FH system and Dr. DongXu Ma who has given me some valuable advices on the format of this thesis.

I would like to express my appreciation to TRI-L Solutions Inc. who provided us the microwave anechoic chamber DART-3300. The isolated environment in the chamber help us to find out potential problems in the current security system more easily.

Moreover, special thanks to all my colleagues and friends: Kalikinkar Mandal, Radi Abubaker and Gangqiang Yang for their suggestions on my research. Also, I would like to thank all members in Communication Security Lab at University of Waterloo where I have worked and studied for the past 2 years, and I was having a great time with them.

Again, I would like to express my warm thanks to all the people who made this thesis possible.

**Dedication**

*To my beloved family*
*thank for their endless love and supports*

# Table of Contents

**List of Tables** x

**List of Figures** xi

**Abbreviations** xiii

**1 Introduction** 1

**2 Literature Survey** 3

2.1 Orthogonal Frequency-Division Multiplexing (OFDM) Based Security . . . 3

2.1.1 OFDM Encryption Schemes . . . . . . . . . . . . . . . . . . . . . . 3

2.1.2 Some Unsolved Problems in OFDM Enc Encryption Scheme . . . . 5

2.2 Anti-jamming systems . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

2.2.1 Threat from Reactive Jamming Attack . . . . . . . . . . . . . . . . 6

2.2.2 Anti-jamming Systems and Performance Concerns . . . . . . . . . . 6

2.2.3 Current Limitation on Designing Physical Layer Security . . . . . . 7

**3 Background and Preliminaries** 8

3.1 OFDM Communication System . . . . . . . . . . . . . . . . . . . . . . 8

3.1.1 Introduction to OFDM System . . . . . . . . . . . . . . . . . . . . 8

3.1.2 Underlying Modulation . . . . . . . . . . . . . . . . . . . . . . . . 9

3.1.3 Inverse Discrete Fourier Transform (IDFT) and Discrete Fourier Transform (DFT) . . . 9
3.1.4 Orthogonality . . . 10
3.1.5 Cyclic Prefix . . . 10
3.2 Specification of OFDM in Wireless Communication Standard . . . 11
3.2.1 Introduction to IEEE 802.11a OFDM Standard . . . 11
3.2.2 Long-Term Evolution (LTE) OFDM Standard . . . 11
3.3 Finite Impulse Response (FIR) Filter and Multipath Channel . . . 13
3.3.1 FIR Filter . . . 13
3.3.2 Multipath Delay Effect on OFDM Enc . . . 14
3.4 Randomness Properties of M-sequences . . . 15
3.4.1 M-sequences . . . 16
3.4.2 Reciprocal Pairs of M-sequences . . . 18
3.4.3 Buffalo Laboratories Application of Digitally Exact Spectra (BLADES) 20
**4 Implementation of OFDM Enc in Software Defined Radio (SDR) 22**
4.1 SDR Overall . . . 22
4.1.1 Basic Theory of GNU Radio and GNU Radio Companion . . . 23
4.1.2 Data Type in GNU Radio . . . 24
4.2 Implementation of OFDM Enc Encryption Scheme in GNU Radio . . . 25
4.2.1 Implementation of the General OFDM System without OFDM Enc 25
4.2.2 Implementation of OFDM Enc Encryption in OFDM System . . . 28
4.2.3 Implementation of OFDM Decryption . . . 30
4.3 Parameters and Basic Properties of Universal Software Radio Peripheral (USRP) . . . 31
4.4 Tests of OFDM Enc . . . 32
4.4.1 Tests of OFDM Enc in Multipath Additive White Gaussian Noise (AWGN) Channel Model in GNU Radio . . . 32
4.4.2 Tests in Microwave Anechoic Chamber DART-3300 and Lab Environment . . . 33

**5 Analysis and Implementation Results of OFDM Enc 37**

5.1 Multipath Delay Boundary in OFDM Enc . . . . . . . . . . . . . . . . . . 37

5.1.1 Multipath Delay Analysis . . . . . . . . . . . . . . . . . . . . . . . 37

5.1.2 Results under Pure Multipath without AWGN . . . . . . . . . . . . 38

5.1.3 Results under Multipath with AWGN . . . . . . . . . . . . . . . . . 39

5.2 Implementation Results . . . . . . . . . . . . . . . . . . . . . . . . . . . 40

5.2.1 32-bit Data Flow of OFDM Enc from GNU Radio Implementation . 40

5.2.2 Implementation Results of OFDM Enc in DART-3300 . . . . . . . . 41

5.2.3 Implementation Results of OFDM Enc in Laboratory . . . . . . . . 42

5.2.4 Observation of OFDM Enc . . . . . . . . . . . . . . . . . . . . . . . 46

**6 A New Frequency Hopping (FH) System 47**

6.1 System Model of M-sequences Based BLADES System and Jammer . . . . 47

6.2 Collision Properties of Two Distinct Binary Primitive Polynomials of the Same Degree . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 49

6.2.1 Upper-Bound for the Collision Probability of Two Polynomials of $\mathcal{P}_n(x)$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 49

6.2.2 Upper-Bound for the Collision Probability of Reciprocal Polynomial Pairs of $\mathcal{P}_n(x)$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . 50

6.3 Simulations and Conjectures of the New Frequency Hopping System . . . . 51

**7 Conclusion and Future Work 53**

7.1 Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 53

7.2 Future Work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 54

**References 56**

**APPENDICES 60**

**A DATA: Multipath Channel Boundary 61**

B DATA: AWGN Multipath Channel with signal to noise (SNR) 62

C Fragments of Sent and Received Messages for the Implementation in Chamber 64

D Fragments of Sent and Received Messages for the Implementation in Laboratory 69

E Proof of Theorem 1 74

F Proof of Lemma 3 76

G Proof of Theorem 2 78

# List of Tables

5.1 Data Flow of the OFDM Enc . . . . . . . . . . . . . . . . . . . . . . . . 41

5.2 Bit Error Rate from the Implementations in Both the Chamber and the Lab 45

A.1 Multipath Boundary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 61

B.1 AWGN Multipath Channel with SNR $\approx 18.8dB$ . . . . . . . . . . . . . . . . 62

B.2 AWGN Multipath Channel with SNR $\approx 20.1dB$ . . . . . . . . . . . . . . . . 63

# List of Figures

3.1 802.11a OFDM Spectrum 64 Subcarriers Usage . . . . . . . . . . . . . . . . 12

3.2 FIR Filter . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 13

3.3 BLADES System . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 20

4.1 Software Defined Radio Physical Connection . . . . . . . . . . . . . . . . . 23

4.2 OFDM Sender without Encryption . . . . . . . . . . . . . . . . . . . . . 25

4.3 BPSK (Left) and QPSK (Right) Modulation for Each Input Byte . . . . . 26

4.4 Complex Number Stream after the OFDM Carrier Manipulator Block . . . 27

4.5 Cyclic Prefix before Each 64 Complex Numbers . . . . . . . . . . . . . . . 27

4.6 OFDM Encryption placed between the IFFT Block and the Cyclic Prefix Block . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 29

4.7 Linear Feedback Shift Register with Primitive Polynomial $1+x+x^4+x^6+x^{12}$ 30

4.8 OFDM Receiver . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 31

4.9 AWGN Channel in GNU Radio . . . . . . . . . . . . . . . . . . . . . . . . 32

4.10 Customized Key Stream Generator: Constant Sources and Stream MUX . 34

4.11 SDR Setup in Chamber DART-3300 . . . . . . . . . . . . . . . . . . . . . 35

5.1 Multipath BER Versus Taps Ratio . . . . . . . . . . . . . . . . . . . . . . 40

5.2 Spectrums of the OFDM System with OFDM Enc in the Chamber . . . . 43

5.3 Spectrums of the OFDM System with OFDM Enc in the Lab . . . . . . . 44

6.1 Collision Probabilities and Theoretical Upper-Bounds of Two Distinct Binary Primitive Polynomials of the Same Degree. . . . . . . . . . . . . . . . 51

C.1 Sent and Received Messages for the Case with $k1 = k2 = (1, -1, 1)$ in the Chamber . . . 65

C.2 Sent and Received Messages for the Case with $k1 = k2 = (1, -1, -1, 1)$ in the Chamber . . . 65

C.3 Sent and Received Messages for the Case with $k1 = k2 = (1, -1, -1, 1, 1)$ in the Chamber . . . 66

C.4 Sent and Received Messages for the Case with $k1 = k2 = (1, -1, 1, 1, 1, -1)$ in the Chamber . . . 67

C.5 Sent and Received Messages for the Case with $k1 = k2 = (1, -1, 1, 1, 1, -1, -1)$ in the Chamber . . . 68

D.1 Sent and Received Messages for the Case with $k1 = k2 = (1, -1, 1)$ in the Laboratory . . . 70

D.2 Sent and Received Messages for the Case with $k1 = k2 = (1, -1, -1, 1)$ in the Laboratory . . . 71

D.3 Sent and Received Messages for the Case with $k1 = k2 = (1, -1, -1, 1, 1)$ in the Laboratory . . . 72

D.4 Sent and Received Messages for the Case with $k1 = k2 = (1, -1, 1, 1, 1, -1)$ in the Laboratory . . . 73

# Abbreviations

**4G-LTE** 4th generation Long Term Evolution 7, 11

**5G** 5th generation mobile networks 7

**ADC** analog-to-digital convertor 4, 8, 22, 31

**AWGN** additive white Gaussian noise 2, 5, 14, 15, 22, 30, 32, 33, 39, 53

**BER** bit error rate 2, 6, 7, 10, 21, 27, 30, 33, 35, 39, 41, 43, 45, 46, 49, 53, 54

**BLADES** Buffalo Laboratories Application of Digitally Exact Spectra 2, 6, 7, 15, 20, 21, 47, 49

**BPSK** binary phase-shift keying 9, 11

**CP** cyclic prefix 5, 8, 10, 13, 15, 27, 28, 35

**DAC** digital-to-analog convertor 4, 8, 10, 22, 31

**DC** direct current 10–12, 27

**DFT** discrete Fourier transform 8, 10

**DSP** digital signal processing 22

**EV** eavesdropper 3

**FDD** frequency division duplex 11, 12

**FFT** fast fourier transform 1, 4, 9, 10, 12, 13, 30

**FH** frequency hopping 2, 6, 7, 20, 47, 52, 54

**FIR** finite impulse response 8, 13, 14, 32, 33, 37, 39

**FPGA** field programmable gate array 31

**IDFT** inverse discrete Fourier transform 8–10

**IFFT** inverse fast fourier transform 1, 4, 8–13, 15, 27, 28

**IP** Internet Protocol 22, 23, 28

**ISI** intersymbol interference 3, 10, 13, 15

**LFSR** linear feedback shift register 16, 17, 28–30, 40

**LOS** line-of-sight 14

**LSB** least-significant-bits 24, 26, 29, 40

**LTE** Long-Term Evolution 11, 12, 55

**MFSK** M-ary frequency-shift keying 1

**MPSK** M-ary phase-shift keying 9

**MSB** most-significant-bits 24

**MUX** multiplexing 26, 34

**OFDM** orthogonal frequency-division multiplexing 1–5, 8–11, 14, 15, 22, 25, 30–34, 36, 38, 39, 41–43, 45, 46, 53

**PC** personal computer 22–24

**PRG** pseudorandom generator 4, 6, 7, 14, 20, 21, 48

**QAM** quadrature amplitude modulation 9

**QPSK** quadrature phase-shift keying 9, 11, 12

**RF** radio frequency 31, 33

**SC-FDMA** single carrier-frequency division multiple access 12, 13

**SDR** software defined radio 2, 5, 22–24, 27, 46, 53

**SNR** signal to noise ix, 5, 9, 27, 30, 33, 39, 46, 54, 62

**USRP** Universal Software Radio Peripheral 22–24, 27, 28, 30–32, 34, 36, 54

# Chapter 1

# Introduction

With the rapid growth of modern communication, the bandwidth used for transmission become precious and physical layer security becomes important than ever. Especially for wireless transmission, large amounts of data transmission happen in shared channel at the same time. Therefore, a communication scheme should provide high bandwidth efficiency and a security scheme built in the communication scheme should have high security and less negative effect on the performance of the overall communication system.

One of such communication modulations with high bandwidth efficiency is called orthogonal frequency-division multiplexing (OFDM). It not only has good resistance on intersymbol interference but also saves large bandwidth due to its orthogonality. As a special case of frequency division multiplexing, OFDM has high spectral efficiency compared to M-ary frequency-shift keying (MFSK) which needs large guard bandwidth among subcarriers to reduce the intercarrier interference. Furthermore, OFDM has good resistance on multipath delay in fading channel. In addition, it can be easily implemented by inverse fast fourier transform (IFFT) and fast fourier transform (FFT).

One interesting physical layer security scheme called *OFDM Enc* encryption scheme from the paper entitled as *"A new efficient physical layer OFDM encryption scheme"* by [17]. It demonstrates an effective way to secure OFDM samples in physical layer, which is fast and has a high efficiency of encryption. The simulation result of OFDM Enc given in [17] is simple and does not include implementations in a practical OFDM communication system so it is necessary to deeply analyse the influence of OFDM Enc on the performance of a practical OFDM system.

Jamming attack posts a threat to wireless communication, because it sends interference signals (generally artificial noises) to confuse receivers. The second part of this thesis proposes a new physical layer frequency hopping (FH) scheme for anti-jamming. We analyse and simulate the collision properties of two $m$-sequences which are generated from two distinct binary primitive polynomials of the same degree respectively.

The main contributions of our work can be summarized as below:

(i) Implemented the OFDM encryption scheme given by [17] in software defined radio (SDR) and tested in microwave anechoic chamber and lab environment separately. In fact, the spectrums at both sender side and receiver side are captured, and the bit error rate has been counted for the OFDM encryption scheme. Note that the original paper [17] only gives simulation results of the OFDM encryption scheme in additive white Gaussian noise (AWGN) channel in *Simulink*.

(ii) Found a multipath boundary in the OFDM encryption scheme. The performance of the OFDM encryption scheme in multipath AWGN channel is tested in GNU radio, and the results indicate a significant bit error rate (BER) increase comparing with that of the OFDM system without encryption. Note that the multipath effect on the OFDM encryption scheme is not considered in [17].

(iii) Proposed a new anti-jamming system called *randomly selective $m$-sequence based BLADES system*. The collision probability between two distinct binary primitive polynomials of the same degree is discussed in detail. The exhaustive emulation of the collision probability has also been given.

The organization of the thesis is given as follows. The literature survey is demonstrated in Chapter 2 for both OFDM Enc given by [17] and $m$-sequences related frequency hopping system. Chapter 3 is the background of OFDM related standard and $m$-sequences. Chapter 4 focuses on how to implement OFDM Enc using SDR and the experiments setup procedures. Chapter 5 is about the testing results and analysis of OFDM Enc. Chapter 6 proposes the new $m$-sequences based Buffalo Laboratories Application of Digitally Exact Spectra (BLADES) system and its simulation results. Finally, the conclusions and the future work are given in Chapter 7.

# Chapter 2

# Literature Survey

This chapter demonstrates the literature survey on OFDM related encryption schemes and anti-jamming systems. Section 2.1 demonstrates OFDM related encryption schemes. Additionally, it discussed some unsolved problems in one of the OFDM encryption schemes called OFDM Enc. Section 2.2 introduces several anti-jamming systems, security concerns and design limitations of an anti-jamming system.

## 2.1 Orthogonal Frequency-Division Multiplexing (OFDM) Based Security

This section describes the literature survey on several OFDM encryption schemes and some unsolved problems in the OFDM Enc encryption scheme.

### 2.1.1 OFDM Encryption Schemes

OFDM scheme becomes popular and it is widely used in the wireless system because of its high bandwidth efficiency and good intersymbol interference (ISI) resistance. One famous OFDM related security schemes is *ijam* given in [9]. In the presence of eavesdropper (EV), it allows two wireless devices to exchange secret keys without encryption. The *ijam* actively sends jamming signal in order to jam the transmitting signals, and the *ijam* shares the jamming info only to the legitimate receiver, so that only the legitimate receiver knows how to recover the jammed signal but EV cannot recover it.

Another OFDM related security given in [14] demonstrated a two-way authentication method between two OFDM devices. In fact, it uses the inherent physical features of the multi-path fading channel as signature for the message transmission. The OFDM related security given in [40] illustrates a encryption method by inserting dummy data to randomly reserved subcarriers to mix up OFDM subcarriers, which randomizes waveform. The dummy data and subcarriers' location are secrete info for transceiver which are generated by pre shared information. Furthermore, the OFDM security method given in [1] shows that the OFDM encryption can be done by hiding certain synchronization information based on a pre-shared secret key sequence. In paper [1], it mentioned that their security scheme is resistant to multipath fading and impulsive noise.

In the paper [17], the authors proposed a new OFDM security scheme called OFDM Enc. The operation of this scheme is mainly in physical layer, and key exchange is done in upper layer. The OFDM Enc actually encrypts the discrete time domain samples between the IFFT and digital-to-analog convertor (DAC), then it decrypts the discrete time samples between the FFT and analog-to-digital convertor (ADC).

In the following, we will provide a detailed specification of this scheme, since that is the scheme that we will implement. The encryption of OFDM Enc has two pseudorandom generator (PRG)s which outputs either $-1$ or 1. In detail, the first PRG is used to encrypt the real part of sample data by multiplication, and the second PRG is to encrypt the imaginary part of the data by multiplication; specifically, the first key stream is denoted as

$$\mathbf{u} = (u_0, u_1, u_2, \ldots)$$

and the second key stream is denoted as

$$\mathbf{v} = (v_0, v_1, v_2, \ldots).$$

Assume the sample data in discrete time domain before the OFDM Enc is

$$\mathbf{x} = (x_0, x_1, x_2, \ldots).$$

Then sample data after the OFDM Enc is

$$\begin{aligned}\mathbf{x}' &= Enc(\mathbf{x}) = (x'_0, x'_1, x'_2, \ldots)\\ &= (\Re\{x_0\}u_0 + j\Im\{x_0\}v_0, \Re\{x_1\}u_1 + j\Im\{x_1\}v_1, \Re\{x_2\}u_2 + j\Im\{x_2\}v_2, \ldots). \qquad (2.1)\end{aligned}$$

At the receiver side, the decryption use the same structure as the encryption part. Assume that the sample data before the OFDM Enc decryption at the receiver side is

$$\mathbf{y}' = (y'_0, y'_1, y'_2, \ldots)$$

and the decrypted data is

$$\begin{aligned}\mathbf{y} &= Dec(\mathbf{y}') = (y_0, y_1, y_2, \ldots) \\ &= (\Re\{y_0'\}u_0 + j\Im\{y_0'\}v_0, \Re\{y_1'\}u_1 + j\Im\{y_1'\}v_1, \Re\{y_2'\}u_2 + j\Im\{y_2'\}v_2, \ldots). \end{aligned} \tag{2.2}$$

### 2.1.2 Some Unsolved Problems in OFDM Enc Encryption Scheme

There are several problems arising from the implementation of the scheme OFDM Enc using SDR. The first problem is whether the OFDM Enc encryption scheme should be placed before or after the cyclic prefix (CP), which is not mentioned in [17]. It is necessary to figure out the best place to insert the OFDM Enc as the reference of CP.

Secondly, the symbol error rate versus SNR ratio plot of OFDM Enc in [17] was obtained from a simulated AWGN channel. The paper does not consider other commonly existed channel effect, such as multipath delay effect. However, the multipath effect exists in practice. Therefore, it is necessary to analyse the performance of the entire OFDM system with OFDM Enc in the multipath channel.

The third is that multipath fading effect on OFDM Enc is not considered in [17]. One assumption is that the performance of OFDM system with OFDM Enc may be reduced by the multipath channel compared to the OFDM system without using OFDM Enc. In fact, the OFDM modulation and demodulation have good resistance on multipath delay when enough CP is provided [31]. However, it will leave "noise" in the data if the OFDM Enc decryption cannot completely recover the cyphertext data samples at the receiver side due to the multipath effect.

Based on the assumption, one concern is that the OFDM demodulator may not be able to remove the left noise effectively. Furthermore, if the OFDM demodulator can remove the residual noise, it needs to sacrifice the performance in terms of bit error rate. The detail analysis of the impact of multipath delay on 802.11 OFDM scheme with OFDM Enc will be given, which is important for its future improvements.

## 2.2 Anti-jamming systems

This section gives the literature survey on anti-jamming systems and security concerns. In addition, the limitation on designing physical layer security is given.

### 2.2.1 Threat from Reactive Jamming Attack

The well-known effective smart jamming attack is reactive jamming attack [5, 6], which can jam the signal while there is a transmission and stay quiet while there is no signal sending by the sender. This strategy gives the reactive jammer good energy use efficiency and makes it hard to be detected and removed from the system.

### 2.2.2 Anti-jamming Systems and Performance Concerns

Anti-jamming systems are invented [21, 25, 29, 30, 33] in order to overcome the jamming attack. FH system has been invented to solve those jamming attacks [2, 5, 22]. BLADES system was proposed in the middle of 1950s and successfully implemented in 1963 as the first working FH system in the world [5, 32, 34]. BLADES system uses two sequences to generate hopping frequencies instead of using just one sequence [5].

Jamming attack posts a threat on a communication system by sending interference signals to change current transmitting bits, insert bits, damage underlying modulation and so on [6]. Actually, there are several commonly known jamming attacks, like full-band jamming attack, partial band jamming, pulse jamming attack, single tone jamming attack, multitone jamming attack and the repeat back jamming attack [5]. Full-band jammer can jam entire band but it has low power efficiency and is easy to be found. Partial band jammer, pulse jamming jammer, single tone jammer and multitone jammer use lower power but still can be detected. The most effective jamming attack is the reactive jamming attack. It will stay quiet when there is no transmission and start to jam when it senses the transmission in the channel [6]. This property makes it hard to be detected.

For the BLADES system, if the two PRGs output the same hopping frequency at certain time $i$, which means a collision happened, then the receiver could not despread the hopping frequency at that time, so it will increase the BER of the system. If two distinct primitive polynomials of the same degree are used as the two PRGs in BLADES system, then there is no previous work about how to select the two distinct primitive polynomials of the same degree to reduce the number of collisions.

If $\exists t \geq 0$, $f_{a_t} = f_{b_t}$, then the receiver could not despread the hopping frequency at time $i$. Therefore collisions between two PRGs increase the BER. In order to reduce the probability of occurrence of the collision, we need to analyse the collision properties of two distinct binary primitive polynomials of the same degree. This could help us to figure out how to select the best pairs to reduce the collision probabilityn. In brief, the motivation of analyzing the collision properties in the BLADES system is to reduce the BER caused by the collisions.

### 2.2.3 Current Limitation on Designing Physical Layer Security

Light-weight PRG have less effect on transmission rate. $M$-sequence generators are one of this kind. As the growth of the high speed wireless communication, the 5th generation mobile networks (5G) will be used in commercial for future years. The transmission data rate of 5G is about 10-50 Gbps that is much higher than the data rate of 4th generation Long Term Evolution (4G-LTE) which has 3 Gbps in downlink [13]. Based on the fact, the speed of the PRG which generates hopping frequencies should have higher or equal data rate, otherwise FH system will become the bottleneck in a communication system which cannot be tolerated. Actually, an $m$-sequence is built by using small number of XOR gates and shift registers. Therefore, the speed of generating $m$-sequence depends on the speed of a XOR gate or a shift register. The optical shift register can reach 100Gbps [24] and the optical XOR gate can reach up to 40 Gbps [38]. Since $m$-sequence generation speed is limited by the XOR gate, it matches the data rate of 5G which is 10-50 Gbps in theory. Based on this property, $m$-sequence could be a solution in FH systems.

# Chapter 3

# Background and Preliminaries

This chapter demonstrates background and preliminaries of this thesis. Section 3.1 introduces basic theories of OFDM communication system. Section 3.2 introduces the OFDM standards used in WIFI and the cellular system. Section 3.3 introduces the finite impulse response (FIR) filter and multipath delay effect. Section 3.4 introduces the $m$-sequence and its randomness properties.

## 3.1 OFDM Communication System

This section introduces the basic structure of the OFDM system. In detail, it gives basic concepts of underlying modulation, inverse discrete Fourier transform (IDFT), discrete Fourier transform (DFT), the orthogonality and CP for a general OFDM system.

### 3.1.1 Introduction to OFDM System

In [4], the authors proposed a communication scheme called OFDM to transmit multiple messages simultaneously on a linear bandlimited channel without involving intersymbol interference and inter-channel interference. The total bandwidth $W$ has been divided into multiple sub-channels, and those sub-channels are overlapping with each other one by one. However, they will not affect each other during the transmission in a linear bandlimited channel due to the orthogonality of the subcarriers. According to [17], [20] and [15], the basic model of OFDM system contains serial-to-parallel conversion, underlying modulation, N-IFFT and DAC conversion at the sender side. At the receiver side, it contains ADC conversion, N-FFT, parallel-to-serial conversion and underlying demodulation. From [37] and [35], pilot symbols and pilot carriers are used for channel estimation. The number of subcarriers $N$ is equal to the size of the IFFT and FFT, and each subcarrier is orthogonal to each other. We will restate the details on the usage of those subcarriers in the next section, and the properties of OFDM will be deferred to Chapter 4.

### 3.1.2 Underlying Modulation

The underlying modulation is also called sub-carrier modulation. The process of underlying modulation is done before the serial-to-parallel conversion. The purpose of the underlying modulation is to map the input bits into constellation in complex domain. The underlying modulations include binary phase-shift keying (BPSK), quadrature phase-shift keying (QPSK), quadrature amplitude modulation (QAM) and so on. The selection of those modulations depends on the channel condition and the communication regulation. Under a limited transmission power, the system under better channel conditions, such as optical channel which has little noise, can use higher modulation methods, such as 32-QAM or 64-QAM, to increase the information rate. In contrast, it is better to choose lower modulation methods such as BPSK or QPSK to keep the low error probability in a high noise channel, such as wireless channels. For instance, the bit error probability of M-ary phase-shift keying (MPSK) is given in Equation (3.1) [8].

$$P_b \approx \frac{2}{\log_2 M} Q(\sqrt{\frac{2E_b}{N_0} \log_2 M sin(\frac{\pi}{M}})). \tag{3.1}$$

Under the same SNR, $\frac{E_b}{N_0}$, increasing the value $M$ will increase the bit error probability.

### 3.1.3 Inverse Discrete Fourier Transform (IDFT) and Discrete Fourier Transform (DFT)

IFFT is a significant part in the OFDM system. The IDFT is shown in Equation (3.2).

$$s_i = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} S_k e^{\frac{j2\pi ik}{N}}, i, k = 0, 1, \cdots, N-1. \tag{3.2}$$

The IDFT is used at the OFDM sender to convert frequency domain samples to time domain samples. The IFFT has a lower complexity to get the time domain samples for the realization purpose in hardware.

The DFT is shown in Equation (3.2).

$$S_i = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} s_k e^{-\frac{j2\pi ik}{N}}, i, k = 0, 1, \cdots, N-1. \tag{3.3}$$

The IDFT is used at the OFDM receiver to calculate the frequency domain samples from the time domain samples. The FFT is the low complexity method to calculate the DFT in hardware.

### 3.1.4 Orthogonality

Orthogonality is a word to demonstrate that the frequency domain signals do not affect each other and the product integral between their time domain signals is zero. In fact, the samples before the IFFT in OFDM system are viewed as discrete frequency samples, and the IFFT will convert them to discrete time samples. Therefore, the subcarriers of those time samples after the DAC and low-pass filter are orthogonal to each other. The basic idea of OFDM system is equivalent to window the sampling train in time domain, and this is also equivalent to convolute frequency domain train by a sinc function, which is to make sure that the sidelobes of each subcarrier will be zeros at the other subcarriers' center point. The mathematic derivation is shown in Chapter 4.3. Finally, the low-pass filter is a process to window the spectrum in frequency domain and this is the process to shape the discrete signal pulses in continuous time domain. Because of the property of the IDFT, the frequency domain spectrum during the transmission is orthogonal to each other.

### 3.1.5 Cyclic Prefix

CP is used to reduce the ISI [8]. According to [26], if the duration of CP is longer than channel delay spread, the ISI will be completely removed. The reason that uses CP instead of using padding zeros is to avoid involving direct current (DC) offset which increases the BER a lot [16]. The prefix interval generally will be $N/4$ which is 16 when $N$ is equal to 64 in our case.

## 3.2 Specification of OFDM in Wireless Communication Standard

This section introduces two OFDM related wireless communication standards which are IEEE 802.11a standard and 4G-LTE standard.

### 3.2.1 Introduction to IEEE 802.11a OFDM Standard

According to [18], the channel usage for 64-IFFT OFDM system in the IEEE 802.11a is shown in Figure 3.1. The standard assumes that the subcarriers have been labeled from $-32$ to 31. In detail, only 48 subcarriers are used to transmit data and 4 subcarriers $(-21, -7, 7, 21)$ are used for pilot carriers for channel estimation as shown in Figure 3.1. Unused subcarriers from -31 to -25 and from 27 to 31 is to prevent the leakage of 52 subcarriers' sidelobes power to the outside of the total bandwidth. Finally, the DC is labeled as 0 subcarrier and IEEE 802.11a OFDM does not use the DC subcarrier to transmit the information; therefore, the DC subcarrier is inserted a complex number 0 at the carrier allocator before the IFFT.

In summary, the IEEE 802.11a OFDM has the following specifications.

- Total bandwidth is 20 MHz, and total subcarrier is 52 from $-26$ to 26 (not include DC at 0), and subcarriers from -32 to -27 and from 27 to 31 are not used. DC subcarrier 0 is not used.
- Underlying modulation could be BPSK, QPSK, 16-QAM, and 64-QAM.
- There are 48 data subcarrier and 4 pilot subcarriers used for the channel estimation. The pilot subcarriers are located at $-21, -7, 7, 21$, and pilot symbols are modulated by BPSK.
- The information rate could be $6, 9, 12, 18, 24, 36, 48, 54$ Mbits/s.

### 3.2.2 Long-Term Evolution (LTE) OFDM Standard

According to [19], the total Bandwidth of Long-Term Evolution (LTE) frequency division duplex (FDD) could be 1.4 MHz, 3 MHz, 5MHz, 10 MHz, 15 MHz, and 20 MHz. In detail, LTE physical layer for 1.4MHz bandwidth is specified as following.

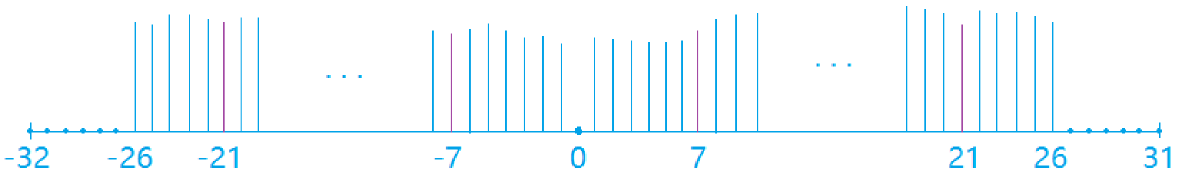


Figure 3.1: 802.11a OFDM Spectrum 64 Subcarriers Usage

- Each LTE FDD frame has 10 microseconds and 10 subframes.
- Each subframe occupied two time slots. Each time slot contains 7 symbols, and is divided into 6 resources block in frequency domain.
- Each resource block has 180kHz bandwidth and contains 12 subcarriers (not include DC subcarrier).
- By calculation, each subcarrier has 15 kHz bandwidth.
- There are total 73 subcarriers (DC subcarrier included) for its downlink, and 72 subcarriers (no DC subcarrier) for its uplink.

The resource block is the smallest unit to be assigned to each user [19]. LTE uses single carrier-frequency division multiple access (SC-FDMA) which has lower peak-to-average power ratio and reduces the cost of amplifier and less power usage. In SC-FDMA [19], the users' data modulates for uplink is shown in the following procedure.

Step 1: Each user data is modulated by underlying modulation (QPSK, 16-QAM, or 64-QAM), and those data are viewed as time domain data.

Step 2: The modulated data is converted to frequency domain by using FFT.

Step 3: The frequency domain points are mapped onto the subcarrier which assigned to the users.

Step 4: The entire Frequency domain points are converted into time domain by using IFFT.

The FFT size is the number of total subcarriers assigned to a user, which has minimum one resource block length (12 subcarriers). The size of the IFFT is the total number of the subcarriers. Generally, each user's data does not occupy entire spectrum, so that the size of FFT is smaller than the IFFT size at the sender side.

Comparing with IEEE 802.11 standard, the biggest difference is that SC-FDMA has FFT between the underlying modulation and carrier allocator at the sender side; therefore, the user data in IEEE 802.11 is viewed as frequency domain points, and the user data in SC-FDMA is viewed as time domain points.

## 3.3 Finite Impulse Response (FIR) Filter and Multipath Channel

This section introduces the FIR filter and the multipath channel model.

### 3.3.1 FIR Filter

The structure of general FIR filter is shown in Figure 3.2. Each $Z^{-1}$ in $Z$ transform means delay 1 sample. In addition, $\alpha_k$ is the multiplication factor for each delay. For example, if $h$ is equal to 2, then $y[2] = \alpha_0 x[2] + \alpha_1 x[1]$. The past signal with delay effect will interfere the current transmitting signal. Furthermore, if $h - 1$ is lager than the length of CP, then it will cause ISI.

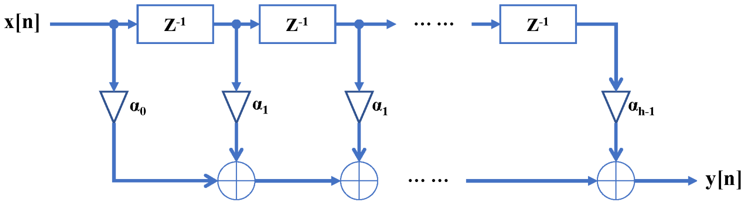


Figure 3.2: FIR Filter

The FIR filter is commonly used to simulate the multipath delay effect in digital communication system. The higher the integer value $h$, the longer the delay effect for each sample will be on future received samples.

### 3.3.2 Multipath Delay Effect on OFDM Enc

Recall the notation in Section 2.1.1, $x_k$ is the sending samples in OFDM system without OFDM Enc at the sender side, and $x'_k$ is the sending samples after the OFDM Enc at the sender side. At the receiver side, $y'_k$ is the received discrete samples before OFDM Enc decryption and $\tilde{y}_k$ is the samples after the decryption. Additionally, $\{u_k\}$ and $\{v_k\}$ are two key streams from PRG respectively, and $\{u_k\}, \{v_k\} \in \{-1, 1\}$.

$$\begin{aligned} x_k &= \Re\{x_k\} + j\Im\{x_k\} \\ &= a_k + jb_k, \text{ where } a_k = \Re\{x_k\} \text{ and } b_k = \Im\{x_k\} \end{aligned} \tag{3.4}$$

$$\begin{aligned} x'_k = Enc(x_k) &= a_k u_k + jb_k v_k \\ &= a'_k + jb'_k, \text{ where } a'_k = a_k u_k \text{ and } b'_k = b_k v_k. \end{aligned} \tag{3.5}$$

In general, the line-of-sight (LOS) is the path which directly connects the transmitter and the receiver, where is no boundary between them. The signal passing through it has the lowest fading effect, so it has the strongest power compared with the signals passing the through the other longer paths. In other words, a signal with longer transmission distance generally has longer transmission delay and lower power at the receiver side due to fading effect. The other paths which are not LOS generally causes multipath delay by reflection and scattering from buildings and other obstacles [3].

$$y'_k = \sum_{i=0}^{h-1} \alpha_i x'_{k-i} + \beta_k, k \geq k - i \geq 0, h \geq 1 \tag{3.6}$$

where $\alpha_i$ is the fading coefficient on $i$'th path and $\beta_i$ is the Gaussian noise variable. Equation (3.6) indicates a multipath AWGN channel in discrete time domain. In detail, the parameter $h$ in the equation is the number of the total paths in the transmission, and the $\beta_i$ in the equation is AWGN noise introduced during the transmission and $\alpha_i$ is FIR filter's coefficient which indicates the impact of the $(k - i)$th sample on the $k$th sample. The first received sample $y_0$ at the beginning of the transmission will not be affected by any multipath delay because there is no previous transmission but only the current signal $x_0$. However, the multipath delay takes effect from the second received sample $y_1$ if the multipath number $h$ is higher than or equal to two. Furthermore, from Equation (3.6), $y'_1$ has term $\alpha_0 x'_1$, so the higher the coefficient $\alpha_0$ is, the greater the effect of the first sample will be on the second received sample. For simplicity, we assume that all attenuation coefficients $\alpha_k$ and AWGN $\beta_k$ are real.

In general, the multipath channel does not enlarge the signal strength, so that the result of $\alpha_0 + \alpha_1 + \ldots + \alpha_{h-1}$ should be lower than or equal to 1 after normalization. In our case, the sum is always normalized to be 1.

For OFDM system, multipath AWGN channel can be formulated into Equation (3.7) (see Chapter 12.4 in [8]).

$$y'_k = x'_k * \alpha_k + \beta'_k, \text{ where "*" denotes the convolution of } \{x_k\} \text{ and } \{\alpha_k\}. \tag{3.7}$$

We rewrite Equation (3.6) in order to show the influence of multipath AWGN channel on each $N$ samples where $N$ is the size of the inverse fast fourier transform. Note that $y_0$ in Equation (3.7) is the first sample in each IFFT output $N$ samples and it is not the first sample at the beginning of the transmission as before.

The matrix form of Equation (3.7) is

$$\begin{pmatrix} y'_{N-1} \\ y'_{N-2} \\ \vdots \\ y'_0 \end{pmatrix} = \begin{pmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{h-1} & 0 & \ldots & 0 \\ 0 & \alpha_0 & \ldots & \alpha_{h-2} & \alpha_{h-1} & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & \alpha_0 & \ddots & \alpha_{h-2} & \alpha_{h-1} \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \alpha_2 & \alpha_3 & \ldots & \alpha_{h-3} & \ldots & \alpha_0 & \alpha_1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_{h-2} & \ldots & 0 & \alpha_0 \end{pmatrix} \begin{pmatrix} x'_{N-1} \\ x'_{N-2} \\ \vdots \\ x'_0 \end{pmatrix} + \begin{pmatrix} \beta_{N-1} \\ \beta_{N-2} \\ \vdots \\ \beta_0 \end{pmatrix} \tag{3.8}$$

In Equation (3.8), the first several samples consist of CP terms inserted to reduce the ISI. For example,

$$y'_0 = \alpha_1 x'_{N-1} + \alpha_2 x'_{N-2} + \ldots + \alpha_{h-1} x'_{N-h+1} + 0 + \ldots + 0 + \alpha_0 x'_0.$$

The CP terms on $y'_0$ are $\alpha_1 x'_{N-1} + \alpha_2 x'_{N-2} + \ldots + \alpha_{h-1} x'_{N-h+1}$. In opposite, if there is no CP inserted, then from the $x_{N-1}$ to $x_{N-h+1}$ in those terms will be replaced by previous block's terms which are from $x_{-1}$ to $x_{-h+1}$. It means that $y'_0$ is affected by ISI from previous block and has to be discarded at the receiver side [8].

## 3.4 Randomness Properties of M-sequences

This section introduces randomness properties of $m$-sequences and basic concepts of reciprocal pairs of $m$-sequences. The last subsection introduces the structure of BLADES system.

### 3.4.1 M-sequences

First of all, the left shift operator $L^i$ on an infinite sequence $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ is defined as follows

$$L^i\mathbf{a} = (a_i, a_{i+1}, a_{i+2}, \ldots),\ i = 1, 2, \ldots. \tag{3.9}$$

For convenience, we define $L^0\mathbf{a} = \mathbf{a}$ as the identity map. A infinite sequence $\mathbf{a}$ is called *a periodic sequence with period* $T$ if it satisfies expression $\mathbf{a} = L^T\mathbf{a}$ and $L^i\mathbf{a} \neq \mathbf{a}$ for any $0 < i < T$.

For two infinite sequences $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ and $\mathbf{b} = (b_0, b_1, b_2, \ldots)$, if there exists a non-negative numbers $i$ which satisfies $L^i\mathbf{a} = \mathbf{b}$, then $\mathbf{a}$ and $\mathbf{b}$ are called shift-equivalent and denoted as $\mathbf{a} \sim \mathbf{b}$. Otherwise, they are not shift-equivalent denoted as $\mathbf{a} \nsim \mathbf{b}$.

We uses the following notation to represent a $l$-tuple started at $a_k$, i.e.,

$$\mathbf{a}[k, l] = (a_k, a_{k+1}, \ldots, a_{k+l-1}), 0 \leq k < k + l.$$

For any starting point k, the set consisting all $l$-tuples of $\mathbf{a}$ is denoted by

$$\mathbf{a}[l] = \{\mathbf{a}[k, l] : k \geq 0\}, \forall l > 0.$$

Let $S$ be a set consisting of $N$ sequences with period $T$. We use $S[l]$ to represent the set consisting all $l$-tuples of all sequences in $S$, i.e.,

$$S[l] = \bigcup_{\mathbf{a} \in S} \mathbf{a}[l], \forall l > 0.$$

If all sequences in $S$ are shift-equivalent, then $S$ is called *a shift-equivalent class*. We have the following property

**Property 1.** *If $S$ is a shift equivalent class, then*

$$S[l] = \mathbf{a}[l], \forall l > 0, \mathbf{a} \in S.$$

The linear feedback function of an n-stage linear feedback shift register (LFSR) is associated with a polynomial [5] as

$$\begin{array}{rcl} f(x_0, x_1, \ldots, x_{n-1}) & = & c_0x_0 + \quad c_1x_1 + \ldots + \quad c_{n-1}x_{n-1} \\ \updownarrow & & \\ f(x) & = & c_0 + \quad c_1x + \ldots + \quad c_{n-1}x^{n-1} + x^n. \end{array}$$

The polynomial $f(x)$ is called a *characteristic polynomial* of the LFSR, and a characteristic polynomial of a LFSR determines its output sequence's period [5]. In general, the period of sequence generated by an n-stage LFSR is defined in Definition 1.

**Definition 1.** *Let* $\mathbf{a}$ *be a sequence generated by an n-stage LFSR over* $\mathbb{F}$*, then the period of* $\mathbf{a}$ *is less than or equal to* $q^n - 1$ *[11, Chapter 4].*

$M$-sequence is a special case of Definition 1, and it is defined in Definition 2.

**Definition 2.** *A 2-ary sequence generated by an n-stage LFSR is called a maximal length binary sequence if it has period* $2^n - 1$*. which is also called binary m-sequence [11].*

In this thesis, all $m$-sequences are binary $m$-sequences. A binary polynomial of degree $n$ with period $2^n-1$ is also called *primitive polynomial* over $\mathbb{F}_2$, and the LFSR corresponded to a primitive polynomial generates $m$-sequences [5]. In brief, the binary primitive polynomial of degree $n$ can be used to generate $m$-sequence with period $2^n - 1$. In detail, if a binary primitive polynomial $f(x)$ for a LFSR is used to define a finite field $GF(2^n)$, the root of the $f(x)$ is denoted as $\alpha$ satisfied $f(\alpha) = 0$. Then the $m$-sequence generated by the primitive polynomial $f(x)$ is defined as

$$a_i = Tr(\alpha^i), i = 0, 1, 2, \ldots, n-1$$

where the trace function $Tr(x)$ is defined as

$$Tr(x) = x + x^2 + \ldots + x^{2n-1}, i = 0, 1, 2, \ldots, n-1.$$

In [11], it demonstrates that if an $m$-sequence $\mathbf{a}$ is generated by a primitive polynomial $f(x)$ with a nonzero initial value, it defines $G(f)$ as

$$G(f) = \{L^i\mathbf{a} : 0 \leq i \leq 2^n - 2\} \cup \{\mathbf{0}\}$$

and we also define $G(f)^* = G(f) \setminus \{\mathbf{0}\}$.

In order to classify the $m$-sequence pairs, $\mathcal{P}_n(x)$ is used to denote the set of all the binary primitive polynomials with degree $n$, and use $N = 2^n - 1$ to denote the period of the $m$-sequence.

Additionally, Property 2 shows the properties of the $m$-sequence which will be uesd in this thesis.

**Property 2.** *M-sequences have following properties given in [5]*

*(i) All m-sequences generated by the same LFSR are shift equivalent. If two m-sequences are generated by two different LFSRs, then they are shift distinct.*

*(ii) Any* $2^i$*-decimation of* $\mathbf{a}$ *is a shift of* $\mathbf{a}$ *for* $i = 1, 2, \ldots, n-1$

(iii) *If $s$ satisfies $gcd(s, 2^n - 1) = 1$ and $s \neq 2^i$ with $i = 0, 1, 2, \ldots$, $s$-decimation of* **a** *is still an m-sequence of period $2^n - 1$ but it is shift distinct from* **a**.

(iv) *All m-sequence of period $2^n-1$ are decimation equivalent, which means all m-sequences with period $2^n - 1$ can be derived from one of them.*

Let $f(x) \in \mathcal{P}_n(x)$, the first property in Property 2 indicates that if there are two $m$-sequences **a** and **b**, $\forall \mathbf{a}, \mathbf{b} \in G(f)^*$, then **a** and **b** are shift-equivalent. In addition, if two $m$-sequences are shift-equivalent, they must be generated by the same characteristic polynomial. Furthermore, the second, the third and the last properties in Property 2 provide a method to generate all $m$-sequences with period $2^n$.

The $m$-sequence meets the three randomness postulates which are *balance property*, *run property* and *two-level correlation property* [10]. The randomness properties of $m$-sequences are shown below

**Property 3.** *M-sequences have following randomness properties given in [5]*

(i) *Each nonzero n-tuple can be convected to a integer which occurs exactly once in one period of an m-sequence of period $2^n - 1$.*

(ii) *Any m-sequences is balanced: each period of the sequence has $2^{n-1}$ one's and $2^{n-1} - 1$ zero's.*

(iii) *For $1 \leq k \leq n-2$, there are $2^{n-k-2}$ runs of 1's (or 0's) of length $k$. For other cases, there is only one 0 run of 0's of length $n-1$ and one run of 1's of length $n$.*

(iv) *Autocorrelation function of m-sequence* **a** *is 2-level, which is*

$$AC(\tau) = \begin{cases} 2^n - 1 & \tau \equiv 0(mod\ 2^n - 1) \\ -1 & \tau \not\equiv 0(mod\ 2^n - 1). \end{cases}$$

The first property of $m$-sequence in Property 3 indicates that each n-tuple in $m$-sequence with period $2^n - 1$ can be converted to a integer which does not appear twice in one period.

### 3.4.2 Reciprocal Pairs of M-sequences

$M$-sequences collision will be analysed in $m$-sequence reciprocal pairs, so it is necessary to make notation for reciprocal $m$-sequence pairs. The reciprocal polynomial of f(x) given in [11, Chapter 3.4.4] is defined as $\frac{x^n}{c_0}f(x^{-1})$, and the expansion of $f^{-1}(x)$ is shown below

$$f^{-1}(x) = x^n f(x^{-1}) = x^n + c_1x^{n-1} + \cdots + c_{n-1}x + 1, c_i \in GF(2^n) \tag{3.10}$$

that is, $f^{-1}(x)$ is got from reversing the order of the coefficients of $f(x)$.

Assume $m$-sequence $\mathbf{a}$ is generated by the primitive polynomial $f^{-1}(x)$,

$$\mathbf{a} = (a_0, a_1, \ldots, a_{T-1}, a_0, a_1, \ldots)$$

and we define its reciprocal $m$-sequence $\tilde{\mathbf{a}}$ is generated by the reciprocal primitive polynomial $f^{-1}(x)$. Let

$$\tilde{\mathbf{a}} = \mathbf{b} = (b_0, b_1, \ldots, b_{T-1}, b_0, b_1, \ldots).$$

According to [7, Chapter 2.2], the reciprocal $m$-sequence $\mathbf{b}$ is defined as

$$b_i = a_{(-i \bmod 2^n-1)}, \text{ for } i = 0, 1, 2, \ldots.$$

Therefore, the reciprocal sequence $\tilde{\mathbf{a}}$ is

$$\tilde{\mathbf{a}} \;\; = \;\; (a_0, a_{T-1}, \ldots, a_1, a_0, a_{T-1}, \ldots).$$

Let $\mathbf{b}$ be a periodic sequence with period $T$,

$$\mathbf{b} = (b_0, b_1, \ldots, b_{T-1}, b_0, b_1, \ldots)$$

then we define $\mathbf{b}^{-1}$ as the reverse of sequence $\mathbf{b}$,

$$\mathbf{b}^{-1} = (b_{T-1}, b_{T-2}, \ldots, b_0, b_{T-1}, b_{T-2}, \ldots).$$

If $\mathbf{b}$ is not a periodic sequence and has finite length $l$,

$$\mathbf{b} = (b_0, b_1, \ldots, b_{l-1})$$

then we define $\mathbf{b}^{-1}$ as the reverse of sequence $\mathbf{b}$,

$$\mathbf{b}^{-1} = (b_{l-1}, b_{l-2}, \ldots, b_0).$$

For a reciprocal $m$-sequence pair which is $\mathbf{a}$ and $\tilde{\mathbf{a}}$, the relation between the reciprocal $m$-sequence $\tilde{\mathbf{a}}$ and the reverse sequence $\mathbf{a}^{-1}$ is

$$\mathbf{a}^{-1} = L^1(\tilde{\mathbf{a}}).$$

In summary, the relation between generated sequences $\mathbf{a}$ from $f(x)$ and $\mathbf{a}^{-1}$ from $f(x^{-1})$ is defined as

$$\mathbf{a} \in G(f) \iff \mathbf{a}^{-1} \in G(f^{-1}).$$

The characteristic polynomials of any reciprocal $m$-sequence pairs, $f(x)$ and $f(x^{-1})$, will never be the same.

### 3.4.3 Buffalo Laboratories Application of Digitally Exact Spectra (BLADES)

The basic structure of the BLADES system is shown in Figure 3.3. In detail, the output bit stream of the first PRG on the top of the structure is **a** and the output bit stream of the second PRG is **b**.

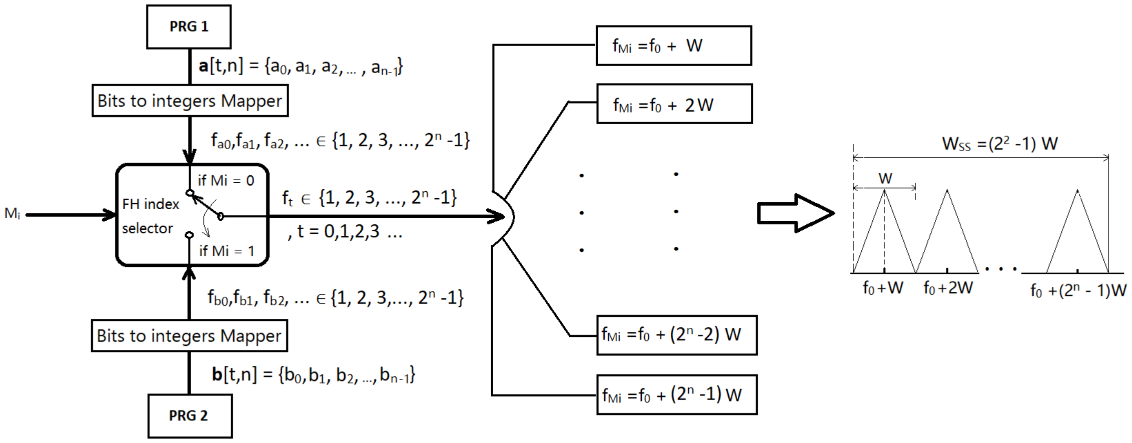

PRG 1
$\mathbf{a}[t,n] = \{a_0, a_1, a_2, \ldots, a_{n-1}\}$
Bits to integers Mapper
$f_{a0}, f_{a1}, f_{a2}, \ldots \in \{1, 2, 3, \ldots, 2^n - 1\}$
if Mi = 0
$M_i$
FH index selector
if Mi = 1
$f_t \in \{1, 2, 3, \ldots, 2^n - 1\}$
, t = 0,1,2,3 ...
$f_{b0}, f_{b1}, f_{b2}, \ldots \in \{1, 2, 3, \ldots, 2^n - 1\}$
Bits to integers Mapper
$\mathbf{b}[t,n] = \{b_0, b_1, b_2, \ldots, b_{n-1}\}$
PRG 2
$f_{Mi} = f_0 + W$
$f_{Mi} = f_0 + 2W$
$f_{Mi} = f_0 + (2^n - 2) W$
$f_{Mi} = f_0 + (2^n - 1) W$
$W_{SS} = (2^2 - 1) W$
W
$f_0 + W$
$f_0 + 2W$
$f_0 + (2^n - 1)W$

Figure 3.3: BLADES System

The upper bits-to-integers mapper converts each $\mathbf{a}[t, n]$ bits to an integer value $f_{a_t}$, where $t = 0, 1, 2, 3, \ldots$; similarly, the lower one converts each $\mathbf{a}[t, n]$ bits to an integer value $f_{b_t}$, where $t = 0, 1, 2, 3, \ldots$.

The next block in the middle of the figure is the selector and it's the core of the BLADES system. Assume the input indicator bit stream of the selector is $M_t$ for $t = 0, 1, 2, 3, \ldots$ and the output integer stream is $f_t$ for $t = 0, 1, 2, 3, \ldots$. Then the relation between the output and the inputs is $f_t = f_{at}$, $\forall M_t = 0$ and $f_t = f_{bt}$, $\forall M_t = 1$.

After the selector, the mixer send baseband signal with bandwidth $W$ to the hopping frequency $f_{M_i}$ which is the center frequency of hopping slot. Assume the reference frequency of the hopping system is $f_0$ which is located at far left of the bandwidth $W_{ss}$, and the total FH bandwidth is $W_{ss}$ as shown on the right side of Figure 3.3. The basic idea of the BLADES system can be summarized as

$$f_t = \begin{cases} f_0 + W * f_{at} & M_t = 0 \\ f_0 + W * f_{bt} & M_t = 1 \end{cases} \tag{3.11}$$

For security purpose, the pre-shared information used to generate pseudorandom numbers $\mathbf{a}$ and $\mathbf{b}$ are randomly picked and should be kept as secret keys of the sender and the receiver. The jammer firstly needs to find the frequency of transmitting signal and then send jamming signal to this frequency. This model be discussed in detail in Section 6.1.

If $\exists t \geq 0$, $f_{a_t} = f_{b_t}$, then the receiver could not despread the hopping frequency at time $i$. Therefore collisions between two PRGs increase the BER. In order to reduce the probability of occurrence of the collision, we need to analyse the collision properties of two distinct binary primitive polynomials of the same degree. This could help us to figure out how to select the best pairs to reduce the collision probabilityn. In brief, the motivation of analyzing the collision properties in the BLADES system is to reduce the BER caused by the collisions.

# Chapter 4

# Implementation of OFDM Enc in Software Defined Radio (SDR)

This chapter provides several basic concepts of SDR and the implementation of OFDM Enc. In addition, the details of parameters setting in GNU radio for OFDM schemes with OFDM Enc will be given. Section 4.1 introduces an overall structure for SDR and data type in GNU radio. Section 4.2 demonstrates the implementation of IEEE 802.11a OFDM system with OFDM Enc in GNU radio. Section 4.3 indicates the basic theory of USRP-N210. Section 4.4 demonstrates the implementation of OFDM Enc in a multipath AWGN model in GNU radio, and demonstrates the implementations of OFDM Enc on USRP-N210 in DART-3300 and laboratory.

## 4.1 SDR Overall

The overall connection of SDR is shown in Figure 4.1. SDR has two main parts which are Universal Software Radio Peripheral (USRP) and GNU radio. USRP is the hardware consisting of ADC, DAC, low pass filer and mixer. GNU radio is a digital signal processing (DSP) software on Linux system. By setting up the Internet Protocol (IP) address in a USRP block in GNU radio, GNU radio on personal computer (PC) can send and receive sample data from USRP hardware devices. Physically, an ethernet cable creates a connection between the USRP device and GNU radio. Since each USRP device has its own subnet, the PC needs two network cards to connect two USRP devices at the same time. Instead of using an gigabit ethernet switch [36], we use two gigabit ethernet adaptors to

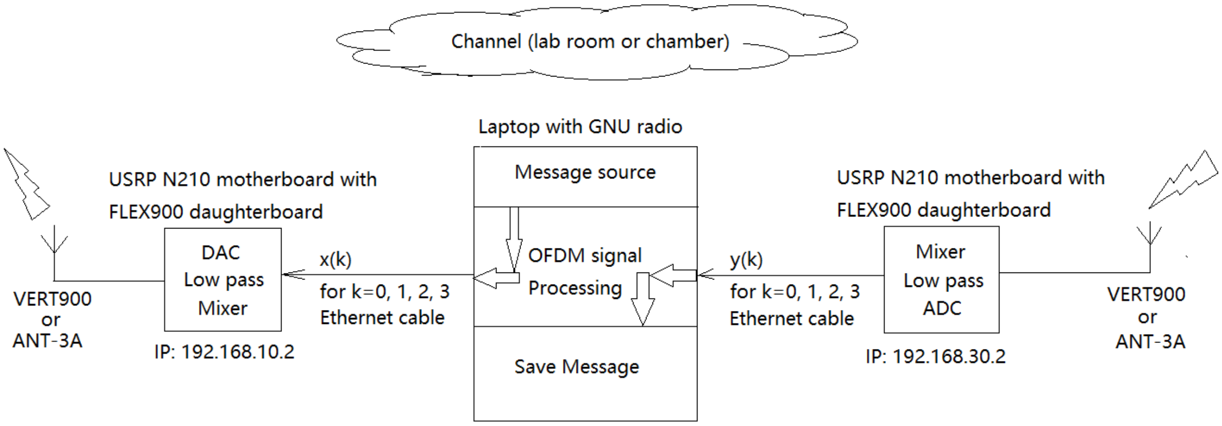


Figure 4.1: Software Defined Radio Physical Connection

connect two USRP devices separately and set up their own IP addresses and subnets. After running SDR, the data transmission between USRP devices and GNU radio are recorded in real-time. As a result, we can use the QT-GUI-frequency-sink block in GNU radio to analyse the spectrum of the sampled data obtained from USRP devices in real-time.

### 4.1.1 Basic Theory of GNU Radio and GNU Radio Companion

GNU radio is a software working under GUN General Public License which is a copyleft license and free to use. GNU radio contains lots of signal processing libraries and USRP communication functions. Additionally, the GNU radio companion is a graphical software combining those functions to form graphical intergraded blocks. By wiring those blocks and setting the parameters inside those blocks, we can build a complete communication scheme efficiently. It is similar to the Simulink in Matlab. In brief, the GNU radio companion helps us focus on prototyping and signal processing graphically.

The GNU radio companion could run on Linux platform or Windows platform, but it widely runs on Linux. In this thesis, the GNU radio companion Ver. 3.7.9 is running on Ubuntu 16.04 OS which is further running on visual machine on Windows 10.

In Figure 4.1, GNU radio on a PC is used to process digital signals in a communication system, and the connected USRP devices process the analogy signals. For the sender part of SDR, the ethernet cable is used to transfer the discrete time sample data from GNU radio to the USRP device on the left side of Figure 4.1. Afterwards, the USRP device converts it into analogy signals and passes them through the low pass filter, the mixer and the antenna. For the receiver part of SDR, the USRP device on the right side of Figure 4.1 receives the analogy signal from its antenna and converts it to baseband signals. Finally, the filtered signals will be converted into discrete time signal, then send to PC through the ethernet cable.

### 4.1.2 Data Type in GNU Radio

There are five main data types used in GNU radio which are complex, float, byte, short and integer. In detail,

- One integer contains 4 bytes.
- One short integer contains 2 bytes.
- One float number contains 32 bits.
- One complex number contains one 32-bit real float number and one 32-bit imaginary float number.

In IEEE-754 floating point standard, each 32-bit float number contains 1-bit sign number at the most significant bit followed by 8-bit exponent numbers, and 23-bit mantissas. Let the 8-bit exponent numbers be $[e_7, e_6, \ldots, e^0]$ and the 23-bit mantissas be $[m_1, m_2, \ldots, m^{23}]$. Then we have following relation

$$\begin{array}{lcl} Sign & \in & \{0, 1\} \\ Exponent & = & -127 + (e_7 \cdot 2^7 + e_6 \cdot 2^6 + \ldots + e_0 \cdot 2^0) \\ Mantissa & = & m_1 \cdot 2^{-1} + m_2 \cdot 2^{-2} + m_3 \cdot 2^{-3} + \ldots + m_{23} \cdot 2^{-23} \\ Decimal & = & 2^{Sign} * (2^{\text{Exponent}} + \text{Mantissa}). \end{array} \tag{4.1}$$

For example,

$$3fe00000_{hex} = (-1)^0 \cdot (2^{-127+127} + 2^{-1} + 2^{-2}) = 1.75_{dec}.$$

IEEE-754 floating point numbers are operated in the format of least-significant-bits (LSB) in GNU radio. In detail, the LSB format is actually the mirror of the most-significant-bits (MSB) format. For example, if $3fe00000_{hex}$ represents $1.75_{dec}$ in MSB, its mirror $0000e03f_{hex}$ represents $1.75_{dec}$ in LSB.

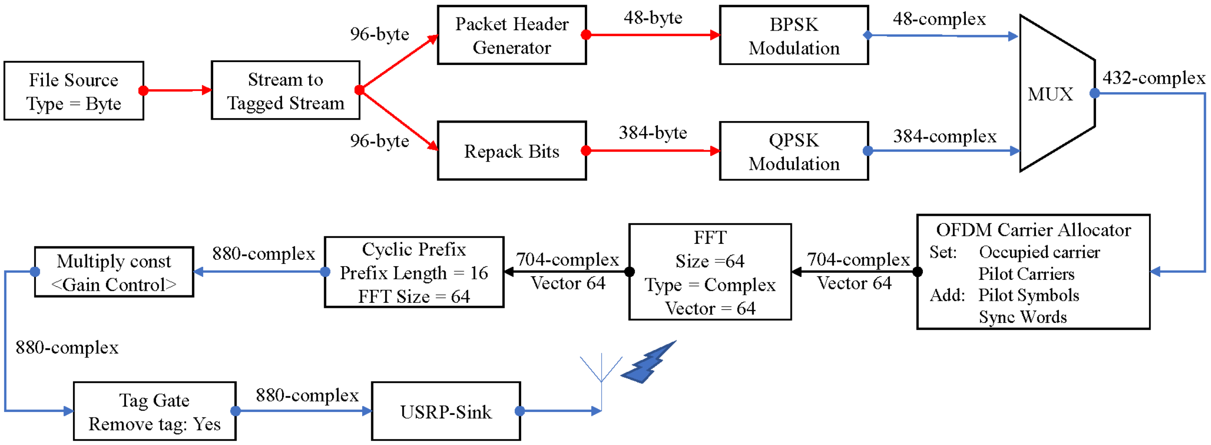


Figure 4.2: OFDM Sender without Encryption

## 4.2 Implementation of OFDM Enc Encryption Scheme in GNU Radio

The implementation of the OFDM Enc encryption scheme is given in this section. Firstly, it demonstrates the implementation of OFDM system under IEEE802.11a standard without OFDM Enc. Secondly, it demonstrates the implementation of OFDM Enc encryption. Finally, it discusses the implementation of the decryption part of OFDM Enc.

### 4.2.1 Implementation of the General OFDM System without OFDM Enc

The IEEE 802.11a OFDM sender's structure without the OFDM Enc is shown in Figure 4.2. In detail, the message-source block in GNU radio is used to output bytes from a binary file to its next block, and it is set to repeat sending the message bit stream automatically during the test. Each 96 bytes from the file-source block will be tagged in the stream-to-tagged-stream block. After that, the following blocks will manipulate each 96 message bytes at a time. For example, the packet-header-generator block generates 48 header bytes for each tagged message which is the tagged 96-byte.

The repack-bits block in Figure 4.2 operates 1-byte at a time. We define 1-byte input in bit type as

$$\mathbf{a} = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7).$$

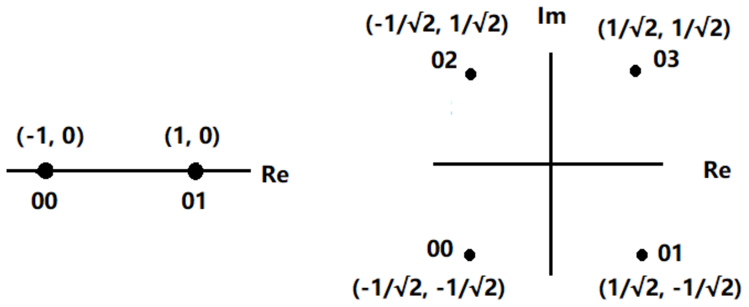


Figure 4.3: BPSK (Left) and QPSK (Right) Modulation for Each Input Byte

The repack-bits block converts each 2-bit to an decimal number,

$$\mathbf{d} = (d_0, d_1, d_2, d_3).$$

After that, each decimal number will be converted to a byte **b** which is

$$\mathbf{b} = (b_0, b_1, b_2, b_3).$$

The output of the repack-bits block is

$$\mathbf{b} = (b_3, b_2, b_1, b_0)$$

which is in the endianness of LSB. Comparing the input **a** with the output **b**, it indicates that each input byte corresponds to four output bytes, which explains that each 96-byte input has 384-byte for the repack-bits block in Figure 4.2.

The BPSK-modulation block also converts each byte to a 8-byte complex number. In detail, it maps bytes $(00, 01)_{hex}$ to complex numbers $((-1, 0), (1, 0))_{decimal}$ as shown in the left side of Figure 4.3.

Similarly, a QPSK-modulation block converts each byte input into a complex number. In detail, it maps input bytes $(00, 01, 02, 03)_{hex}$ to output complex numbers $((-1/\sqrt{2}, -1/\sqrt{2}), (1/\sqrt{2}, -1/\sqrt{2}), (-1/\sqrt{2}, 1/\sqrt{2}), (1/\sqrt{2}, 1/\sqrt{2}))_{decimal}$ respectively as shown in the right side of the signal constellation graph in Figure 4.3.

The multiplexing (MUX) block is used to combine each 48-complex header and 384-complex payload at a time. Therefore, the output of MUX block is 432 complex numbers in total, and it will be sent to the OFDM-carrier-allocator block.

The OFDM-carrier-allocator block in Figure 4.2 creates 11 complex vectors for each 432 complex numbers input, and those vectors are shown in Figure 4.4. The complex vectors are labeled as $M_i$ for $i = 1, 2, \ldots, 11$, and each vector contains 64 complex numbers

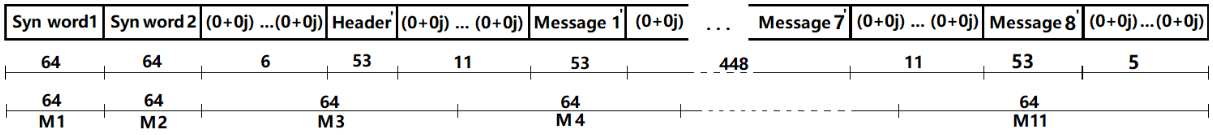


Figure 4.4: Complex Number Stream after the OFDM Carrier Manipulator Block

as 64 subcarriers, where $M_1$ and $M_2$ are two synchronization words. Additionally, each header prime and each message prime in Figure 4.4 come from the header and message data after inserted 4 pilot carriers and 0 DC subcarrier. Namely, the pilot complex numbers $[1, 1, 1, -1]$ are inserted into the subcarriers $[-21, -7, 7, 21]$ respectively for each 64 subcarriers. Furthermore, the subcarriers from $-32$ to $-27$ and from 27 to 31 and subcarrier 0 are set to be complex value zeros. Thus, the format of subcarriers exactly matches the IEEE 802.11 standard in Figure 3.1.

The IFFT size in IFFT block is set to 64, so that IFFT block manipulates each 64 complex subcarriers at a time. In detail, it converts each 64 complex numbers which are discrete samples in frequency domain to 64 complex numbers which are discrete samples in time domain.

The CP block inserts 16 complex numbers CP at the beginning of the each 64 complex numbers input. The prefix is the copy of the last 16 complex numbers of the 64 complex numbers. The process is demonstrated in Figure 4.5.

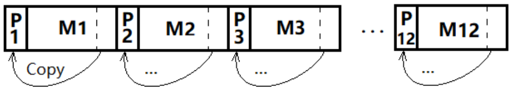


Figure 4.5: Cyclic Prefix before Each 64 Complex Numbers

The multiply-const block is used to multiply each input complex number by a constant number in order to adjust the gain of signals. The constant number is set from 0.01 to 0.03 for the implementation by using USRPs. In other words, if the constant number is lower than 0.01, then the SNR will be too small. In contrast, if constant number is higher than 0.03, the USRP will be saturated for high SNR. SDR will get high BER for both situations. Note that this constant number is the reference number for USRP devices which may not be linearly proportion to the sending signal's power, and its range is not accurate for each USRP device. Finally, the tag-gate block is used to remove the tag which is an internal variable passed by blocks.

The USRP-sink block in the GNU radio companion provides an interface to setup the parameters of the USRP device. In detail, the USRP block has parameters IP address, center frequency and sample rate. In our experiments, the USRP-sink block is used to set the parameters for the USRP sender. Its IP is set to be $addr$ = 192.168.10.2, the center frequency 892MHz, the sample rate 195.312kHz. Similarly, USRP-source block is the receiver which has the same parameter as the sender except that the IP is set to be $adr$ = 192.168.30.2.

### 4.2.2 Implementation of OFDM Enc Encryption in OFDM System

According to the OFDM Enc encryption scheme given in [17], the scheme uses two key stream bits to encrypt one complex number after the IFFT. However, it did not consider whether the OFDM Enc should be done before adding the CP or after adding the CP. From Figure 4.2, we can see that the CP block is inserted between the IFFT and the USRP-sink block, so we first determine whether the OFDM Enc should be inserted before the CP block or after the CP block.

We propose that the OFDM Enc should be inserted between the IFFT block and CP block, because it saves double length of CP in key bits. For instance, for a block of 64 symbols in the OFDM system if we put OFDM Enc after the CP block, it needs 128 bits to encrypt 64 complex numbers at the IFFT output. However, if we put OFDM Enc after the CP block, it firstly uses 32 bits to encrypt the CP and then uses 128 bits to encrypt the 64 complex numbers.

Based on the analysis, putting OFDM Enc between the IFFT block and CP block saves 32 key bits for each 64 complex number inputs, as shown in Figure 4.6. Note that the add block, subtract block and file sink block are used to generate key stream for the use in decryption at the receiver side. In general, we have the following property.

**Property 4.** *For OFDM system with a block of $N$ symbols, the encryption needs $2N$ key stream bits to encrypt it if OFDM Enc is placed between IFFT output and CP. It needs $2len(CP) + 2N$ key stream bits if OFDM Enc is placed after CP where $len(CP)$ is the length of CP.*

The vector-to-stream block converts a vector to a stream. The reason to use this block is the following OFDM Enc encryption scheme can only operates float stream in GNU radio. In detail, the LFSR block can only output float number stream which is viewed as a stream in GNU radio.

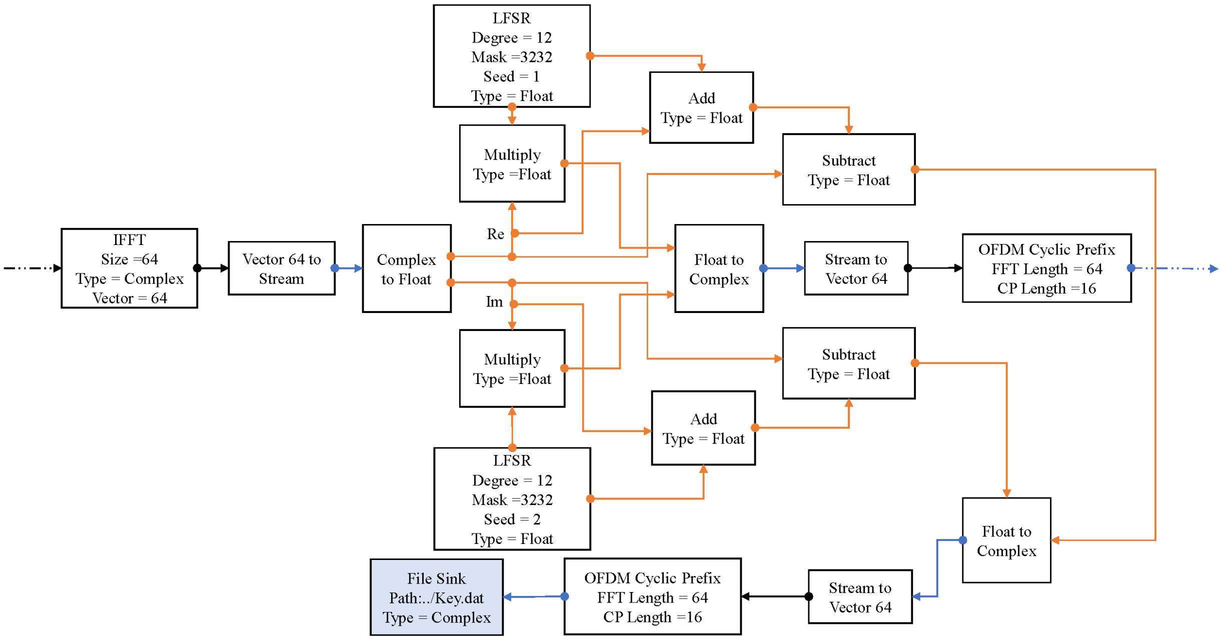


Figure 4.6: OFDM Encryption placed between the IFFT Block and the Cyclic Prefix Block

The complex-to-float block divides each input complex number into a 32-bit float real number and a 32-bit float imaginary number. Then the real part and imaginary part are multiplied by the two key streams from the two LFSR separately for simplicity and test purpose.

The first LFSR block outputs 32-bit float number $0000803F$ and $000080BF$ in hex in LSB, which represents 1 and $-1$ in decimal respectively. Note that $\{0,1\}$ over GF(2) is mapped to the $\{-1,1\}$ in this case. Assume the primitive polynomial over $GF(2)$ of degree $n$ is

$$c_0 + c_1x + c_2x^2 + ... + c_{n-1}x^{n-1} + x^n.$$

In the LFSR block, the degree is set to be 12 and the mask is set to be 3232 which is the integer representation of the corresponding primitive polynomial's coefficients. By converting the integer 3232 into binary numbers, we have the coefficients,

$$(c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, c_{10}, c_{11}) = (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$$

then the corresponding primitive polynomial is

$$1 + x + x^4 + x^6 + x^{12}.$$

Its corresponding LFSR is shown in Figure 4.7. Additionally, the seed in the LFSR block is used to set the initials state of the LFSR. The initial output of the LFSR block is

$$(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}) = (1, -1, -1, -1, -1, -1, 1, -1, 1, -1, -1, 1).$$

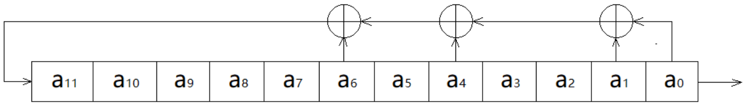


Figure 4.7: Linear Feedback Shift Register with Primitive Polynomial $1 + x + x^4 + x^6 + x^{12}$

For simplicity, the second LFSR is the same as the first one but it has different initials state. The initial output of the second LFSR block will be

$$(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}) = (-1, 1, -1, -1, -1, -1, -1, 1, -1, 1, -1, -1).$$

### 4.2.3 Implementation of OFDM Decryption

The frequency-sink block in GNU radio is used to analyse the spectrum power at both sender and receiver. It is a 1024-FFT block with the sampling rate of 195.312kHz. By using this block, we could get the power spectrum of the discrete time samples. At the receiver side, we could use the spectrums to calculate the SNR for analysing multipath delay effect in AWGN model in GNU radio. In other words, SNR is derived by subtracting noise power in dB from received signal power in dB in AWGN channel.

The 1024-FFT block works as probe and connects to the place after the gain-control block in Figure 4.2. The captured frequency is defined as sending frequency. Similarly, add the same block at the receiver side between the USRP block and OFDM Enc decryption as shown in Figure 4.8 to measure the spectrum power of the received signal.

The delay block is to pad complex number zeros before the complex sample data in order to match the key bits and the samples. Actually, the mismatch generally happens at the beginning of the transmission in our case.

The file-source block in Figure 4.8 outputs key stream bits at the OFDM sender side. The complex-to-float block converts complex number stream to two float key stream bits, which are used for decrypting real part and imaginary part of the samples respectively.

The OFDM demodulation procedures included header detector, FFT, frame equalizer, OFDM serializer, underlying demodulation and repack are put in one block as shown in Figure 4.8 for simplicity. The file-sink block in Figure 4.8 is used to save the demodulated message bytes, and it is used to get BER by comparing with the original sending data.

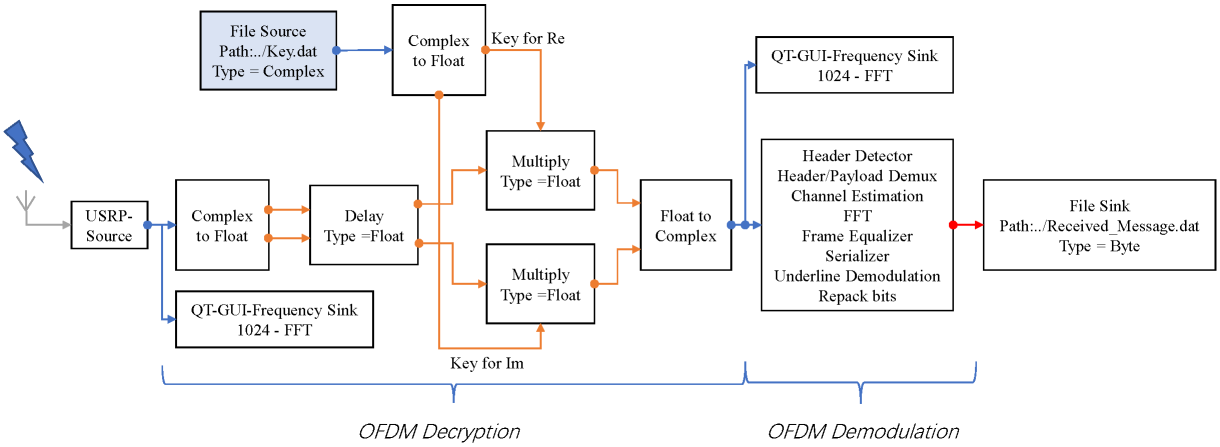
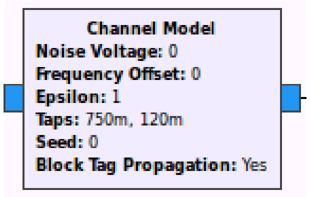


Figure 4.8: OFDM Receiver

## 4.3 Parameters and Basic Properties of Universal Software Radio Peripheral (USRP)

USRP is a communication field programmable gate array (FPGA) board. In the implementation, we use N210 motherboard from Ettus Research$^{\text{TM}}$as USRP. The N210 has dual ADC convertors which can sample up to 100 MS/s. Also it has dual DAC convertors sampled up to 400 MS/s. By using the Gigabit ethernet, it creates a 50 MS/s connection between the USRP device and GNU radio. Furthermore, FLEX-900 radio frequency (RF) daughterboard and vertical antenna VERT900 are used in order to transmit high frequency signal between 824 MHz and 960MHz. FLEX900 RF daughterboard is inserted into N210, and it is also manufactured by Ettus Research$^{\text{TM}}$. Additionally, the FLEX-900 daughterboard provides two RF ports that one is used for transceiver and the other one is used for receiving signals only. In our implementation, we use the former one on two USRP devices.

The USRP sender generates discrete time signal in continuous time based on each input complex number $\tilde{c}[n]$. After that, it passes those time domain pulses to a low-pass filter to form OFDM baseband signal. In fact, low-pass filter is used to window the frequency domain spectrum in order to shape the pulses in time domain. The low-pass filter function is a window function in frequency domain as shown in Equation (4.2). It is equivalent to



**Channel Model**
**Noise Voltage:** 0
**Frequency Offset:** 0
**Epsilon:** 1
**Taps:** 750m, 120m
**Seed:** 0
**Block Tag Propagation:** Yes

Figure 4.9: AWGN Channel in GNU Radio

do the convolution between time domain signal and sinc function.

$$LP(\omega/2\pi W) = \begin{cases} 0 & |\omega| > \pi W \\ 1 & |\omega| < \pi W. \end{cases} \tag{4.2}$$

Finally, the real part and the imaginary part signal will be up-converted by 892 MHz cosine and sine carriers respectively.

## 4.4 Tests of OFDM Enc

This section describes the test procedures for OFDM Enc in detail. The tests of OFDM Enc in multipath AWGN channel model in GNU Radio are given in Section 4.4.1. Additionally, Section 4.4.2 demonstrates the test procedures in DART-3300 and laboratory environment.

### 4.4.1 Tests of OFDM Enc in Multipath Additive White Gaussian Noise (AWGN) Channel Model in GNU Radio

By replacing the two USRP blocks by a AWGN-channel-model block and combining the structures from Figures 4.6 and 4.8, we can implement the OFDM system with OFDM Enc in a simulated multipath AWGN channel. The AWGN-channel-model block is shown in Figure 4.9.

The AWGN-channel-model block has two useful parameters which are multipath FIR taps and AWGN noise voltage. The FIR taps are used to simulate the multipath delay, and the noise voltage is used to simulate AWGN. Other factors including frequency offset in Figure 4.9 are not used.

The implementation in this section contains three cases. The first case is multipath delay without AWGN. The second case is multipath delay with AWGN and adjust SNR to be 18.8 dB. The third case is multipath delay with AWGN and adjust SNR to be 20.1 dB. In the implementation, OFDM with and without OFDM Enc are both tested in order to compare the performance. The initial FIR taps for all three implementation are set to be $[\alpha_0, \alpha_1] = [0.799, 0.201]$ which are the normalized values of the first two taps of [0.74, 0.19, 0.07] given in [36]. The reason to use only two taps is that two taps [0.74, 0.19] has less effect on the system than that of using three taps [0.74, 0.19, 0.07].

The details of the three cases are shown as below.

(i) Case 1. We set the AWGN voltage to be 0 in the AWGN-channel-model block to investigate the pure multipath effect on the OFDM system with the OFDM Enc encryption scheme. By gradually increasing the taps ratio $\alpha_0/\alpha_1$, we measure and record the BER. After that, remove the OFDM Enc in the OFDM system and do the same process to collect those data points. Finally, the BER versus the taps ratio $\alpha_0/\alpha_1$ will be plotted in order to show the boundary of the multipath effect on OFDM Enc.

(ii) Case 2. We set the AWGN voltage to be $200u$ and adjust the gain-control block at the sender to meet $SNR = 18.8$ dB. Then we do the same procedure as in the first case to collect data points $(BER, \alpha_0/\alpha_1)$ from the system with and without the OFDM Enc encryption scheme. Finally, we plot those data in the same figure as in case one.

(iii) Case 3. We keep the same AWGN noise as in the second case and adjust the gain to meet SNR 20.1 dB. Then we do the same procedure as in the first case to collect data points $(BER, \alpha_0/\alpha_1)$ from the system with and without the OFDM Enc encryption scheme. Finally, we plot those data in the same figure as in case (i).

### 4.4.2 Tests in Microwave Anechoic Chamber DART-3300 and Lab Environment

The microwave anechoic chamber DART-3300 has two build-in polarized wideband antenna named ANT-3A which can transmit and receive signals with frequency from 700 MHz to 6 GHz. The overall setup demonstration is shown in Figure 4.11. The communication medium in DART-3300 has almost no noise. In other words, the transmitting signal in it will not suffer any significant channel effects like multipath delay. Furthermore, the radiation absorbent material is used to build the internal wall of the chamber, so that any RF signal propagate though the wall will be absorbed and no reflection. Additionally, the outside wall of the chamber is welded by multiple sheet metals in order to isolate the noise from outside.

We have following changes on the OFDM system with the OFDM Enc encryption scheme.

(i) The OFDM Enc encryption scheme in Figure 4.6 is moved to the place after the gain-control block.

(ii) The combination in Figure 4.10 is used to replace the two LFSR blocks in Figure 4.6 for the encryption.

(iii) The combinations in Figure 4.10 is used to replace the file-source block in Figure 4.8 for the decryption.

(iv) Use a filter sink to save sample data from the USRP receiver in Figure 4.8 to a file. After finished receiving, we replace the USRP-sink block in Figure 4.8 by a sources-file block. The sources-file block can output the saved data from the file. After that, we could use the same data many times for decryption and demodulation.

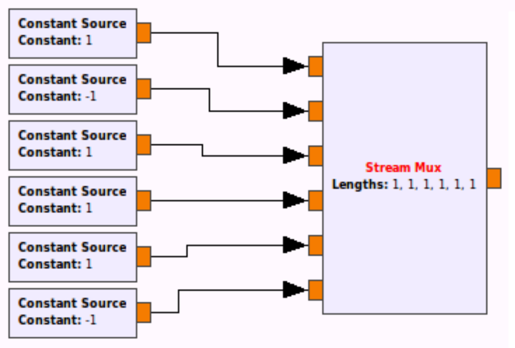


Figure 4.10: Customized Key Stream Generator: Constant Sources and Stream MUX

The combination of a stream-MUX block and multiple constant sources shown in Figure 4.10 forms a key stream generator. In detail, the stream-MUX block combines each input and repeat output. The number of input ports of the stream-MUX block can be defined in the setting. In Figure 4.10, the number of inputs is 6, then it repeatedly outputs its six inputs $(1, -1, 1, 1, 1, -1)$. Therefore, the file-sink block which is used to store the key stream in Figure 4.6 is not used in the implementation in this section.

The reason we made those changes is that we need to find the problems in the implementation. The lost sample data in the received samples at the beginning of the transmission will cause mismatch between sample data and key stream. Therefore, using simpler key bits and move the OFDM Enc after the CP is for the align in decryption. By using lower period of key, we can simply shift the received sample data to match the key stream. The delay block in Figure 4.8 is used to pad zeros in front of the saved data in order to solve the mismatch problem. The total number of possible shifts is the period of the key stream.

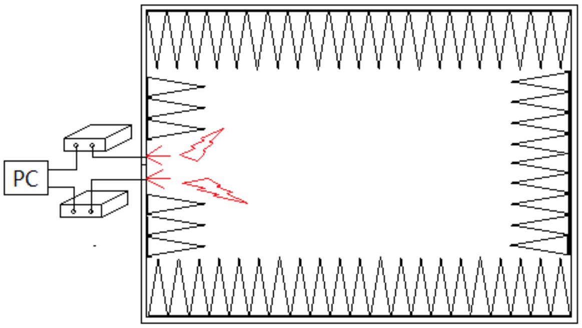


Figure 4.11: SDR Setup in Chamber DART-3300

The above procedure can be described in mathematical formula. Assume the received sample data are $y'_0, y'_1, y'_2, \cdots$. The delay block in GNU radio is used to pad complex number zeros before the data. In detail, $n$ delay means padding $n$ complex zeros before the data. Assume the key stream for the encryption has period $T$. Generally, if the indexes of the lost sample data at the beginning of transmission in the received file are

$$q + Tk, k = 0, 1, 2, \ldots, \text{ where } q \in \{0, 1, 2, \ldots, T-1\}.$$

Then the delay time in the delay block in Figure 4.8 should set to be $q$ in order to solve the mismatch. However, during the implementation in both lab and DART-3300, we do not know the value of $q$, so that the best way is to reduce the period of the key stream and put the OFDM Enc after the CP as discussed above. After that, the mismatch problem can be solved by doing a total of $q$ tests. Each test is done by setting $q = 0, 1, 2, \ldots, T-1$ in the delay block respectively. After that, the best BER in those $q$ tests is recorded.

For example, if the key period is 7, the seven tests will have following data streams after the delay block.

$$
\begin{aligned}
&y'_0, y'_1, y'_2, \ldots \\
&0+0i, y'_0, y'_1, y'_2, \ldots \\
&0+0i, 0+0i, y'_0, y'_1, y'_2, \ldots \\
&\vdots \\
&0+0i, 0+0i, 0+0i, 0+0i, 0+0i, 0+0i, y'_0, y'_1, y'_2, \ldots .
\end{aligned}
$$

The implementation in the DART-3300 and in the lab environment each has two experimental groups, and each group has 6 cases. The first experimental group for each test place has 6 cases as shown in each row below

Case 1: $k1 = k2 = (1, -1)$

Case 2: $k1 = k2 = (1, -1, 1)$

Case 3: $k1 = k2 = (1, -1, -1, 1)$

Case 4: $k1 = k2 = (1, -1, -1, 1, 1)$

Case 5: $k1 = k2 = (1, -1, 1, 1, 1, -1)$

Case 6: $k1 = k2 = (1, -1, 1, 1, 1, -1, -1)$

The second experimental group for each test place has 6 cases as shown in each row below

Case 1: $k1 = (-1, 1), k2 = (1, -1)$

Case 2: $k1 = (-1, -1, 1), k2 = (-1, 1, -1)$

Case 3: $k1 = (-1, -1, 1, -1), k2 = (-1, -1, 1, 1)$

Case 4: $k1 = (1, -1, -1, 1, 1), k2 = (-1, -1, -1, 1, 1)$

Case 5: $k1 = (1, -1, 1, 1, 1, -1), k2 = (1, -1, -1, 1, 1, -1)$

Case 6: $k1 = (1, -1, 1, 1, 1, -1, -1), k2 = (-1, 1, -1, 1, 1, 1, -1)$

The gain control coefficient is set from 0.01 to 0.03 with step 0.001. During the test, we found the OFDM system without OFDM Enc could demodulate correctly for the entire gain range. Implementations in the laboratory use the two USRP devices with VERT900 antennas. The two USRP devices are put on the same table and are one meter away. Afterwards, implementations in the DART-3300 use built-in ANT-3A antennas.

# Chapter 5

# Analysis and Implementation Results of OFDM Enc

This chapter provides the analysis and implementation results of OFDM Enc. The multipath boundary and the implementation results from the lab and the chamber are given and discussed in detail.

## 5.1 Multipath Delay Boundary in OFDM Enc

This section discusses the implementation results in GNU radio. It demonstrates the multipath delay boundary from the implementation of the OFDM system with OFDM Enc encryption scheme in detail.

### 5.1.1 Multipath Delay Analysis

The three FIR taps given in [36] demonstrated the three paths between the transmitter and receiver in their lab environment. Assume the three FIR taps are $[\alpha_0, \alpha_1, \alpha_2]$ and are fixed numbers. By setting $h$ to be 3 in Equation (3.6), we could get Equation (5.1).

$$\begin{aligned} y'_k &= \textstyle\sum_{i=0}^{2} \alpha_i x'_{k-i} + \beta_k, k \geq k-i \geq 0 \\ &= \textstyle\sum_{i=0}^{2} \alpha_i (a'_{k-i} + jb'_{k-i}) + \beta_k, k \geq k-i \geq 0. \end{aligned} \tag{5.1}$$

In detail, the expansion of Equation (5.1) is shown below

$$\begin{aligned} y'_0 &= \alpha_0 x'_0 + \beta_0 \\ y'_1 &= \alpha_0 x'_1 + \alpha_1 x'_0 + \beta_1 \\ y'_2 &= \alpha_0 x'_2 + \alpha_1 x'_1 + \alpha_2 x'_0 + \beta_2 \\ y'_3 &= \alpha_0 x'_3 + \alpha_1 x'_2 + \alpha_2 x'_1 + \beta_3 \\ &\vdots \\ y'_k &= \alpha_0 x'_k + \alpha_1 x'_{k-1} + \alpha_2 x'_{k-2} + \beta_k. \end{aligned} \tag{5.2}$$

At the receiver side, the OFDM Enc decryption yields that $y_k = Dec(y'_k)$. The $y_k$ is shown as

$$\begin{aligned} \tilde{y}_k &= Dec(y'_k) \\ &= Dec(\sum_{i=0}^{2} \alpha_i (a'_{k-i} + jb'_{k-i}) + \beta_k) \\ &= Dec(\alpha_0(a'_k + jb'_k) + \alpha_1(a'_{k-1} + jb'_{k-1}) + \alpha_2(a'_{k-2} + jb'_{k-2}) + \beta_k) \\ &= u_k(\alpha_0 a'_k + \alpha_1 a'_{k-1} + \alpha_2 a'_{k-2} + \beta_k) + v_k(j\alpha_0 b'_k + j\alpha_1 b'_{k-1} + j\alpha_2 b'_{k-2}) \\ &= \alpha_0(a_k + jb_k) + \beta'_k + u_k(\alpha_1 a'_{k-1} + \alpha_2 a'_{k-2}) + v_k(j\alpha_1 b'_{k-1} + j\alpha_2 b'_{k-2}) \end{aligned} \tag{5.3}$$

where $\beta'_k = u_k \beta_k$.

If there is no OFDM Enc encryption scheme in the OFDM system, the OFDM receiver demodulates the samples $\alpha_0(a_k + jb_k) + \alpha_1(a_{k-1} + jb_{k-1}) + \alpha_2(a_{k-2} + jb_{k-2}) + \beta_k$. However, if OFDM Enc is built in OFDM scheme, then the OFDM demodulator has to demodulate the result of Equation (5.3). The problem is we do not know whether the OFDM system can demodulate the part $u_k(\alpha_1 a'_{k-1} + \alpha_2 a'_{k-2}) + v_k(j\alpha_1 b'_{k-1} + j\alpha_2 b'_{k-2})$ or not. Therefore, it is necessary to compare the effect of multipath delay between the OFDM system with the OFDM Enc encryption and the system without the encryption scheme.

### 5.1.2 Results under Pure Multipath without AWGN

The multipath boundary on the IEEE 802.11a OFDM system with the OFDM Enc encryption scheme is shown in the dashed line marked as triangles in Figure 5.1, and the multipath boundary on the system without the encryption scheme is shown in the dashed line marked as diamonds at the bottom. Based on those two lines, we have the following observations.

(i) For the pure multipath effect without AWGN, the BER of the system without the encryption scheme is always zero, which means the multipath effect does not have any effect on it.

(ii) As the taps ratio $\alpha_0/\alpha_1$ increases, the BER of the system with the encryption scheme decreases quickly. After the ratio reaches 6.19, the corresponding BER is around $8.66 \times 10^{-7}$. The precise data is shown in Table A.1.

(iii) Once the ratio $\alpha_0/\alpha_1$ reaches the ratio of the first two taps of $[0.74, 0.19, 0.07]$ given by [36], the system with the encryption cannot deliver useful information.

Based on these observations, we found that if the multipath delay effect happens on the system in practice, it will dramatically decrease the performance of the OFDM system with the OFDM Enc encryption scheme.

### 5.1.3 Results under Multipath with AWGN

In this section, both multipath delay effect and AWGN in the channel model block are used in order to have more practical results. In detail, we adjust the SNR to be 18.8 dB. The plot of BER versus the FIR taps ratio for the OFDM system with the encryption scheme is the solid line marked as triangles in Figure 5.1. The plot of BER versus the FIR taps ratio for the OFDM system without the encryption is marked as rectangles in Figure 5.1.

When set the SNR to be 20.1 dB, the plots of BER versus FIR taps ratio are marked as rounds and stars in Figure 5.1 for the OFDM system with the encryption and the system without the encryption respectively.

From Figure 5.1, we have following observations

(i) As the increase of SNR, it pushes the line closer to the multipath boundary.

(ii) Under the same SNR, the system without the encryption always gets much better BER at the lower taps ratio $\alpha_0/\alpha_1$ then that of the system with the encryption.

(iii) Even with infinity signal power, the system with the encryption cannot get lower BER than that on the dashed line marked as triangles for the same taps ratio.

In summary, multipath delay creates a BER boundary in the OFDM system with the OFDM Enc encryption scheme. If we view the multipath parameters given by [36] as a reference in practice, it might be hard to get higher ratio $\alpha_0/\alpha_1$ in our lab environment than that in their lab.

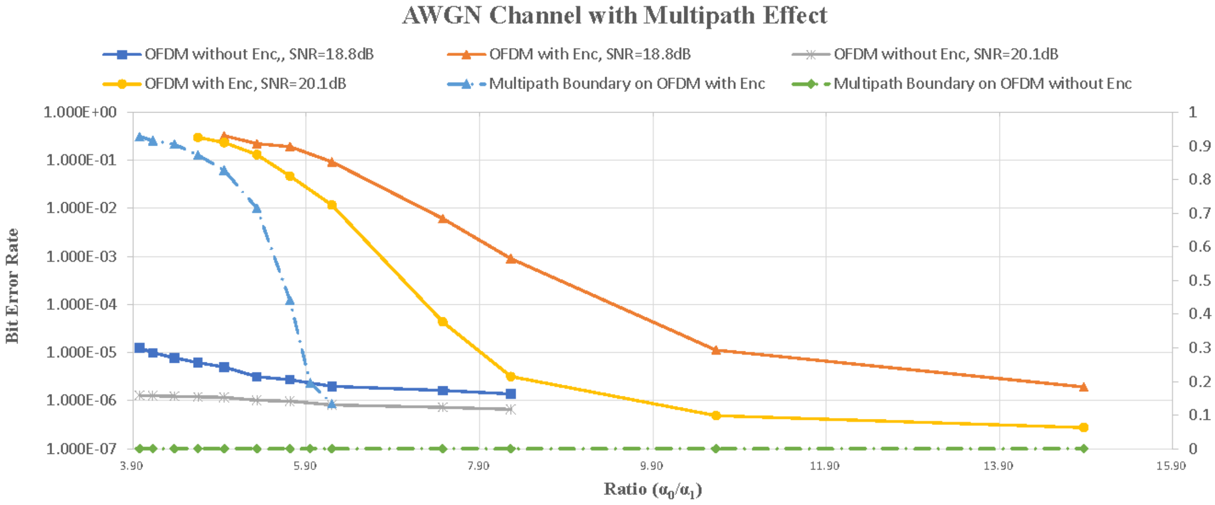


Figure 5.1: Multipath BER Versus Taps Ratio

## 5.2 Implementation Results

This section gives and discusses the test results from DART-3300 and the laboratory environment.

### 5.2.1 32-bit Data Flow of OFDM Enc from GNU Radio Implementation

The data flows of the OFDM Enc encryption from GNU radio are shown in Table 5.1. In detail, the 32-bit float data before the vector-to-stream block and the date after the stream-to-vector block have been captured by two file-sink blocks respectively. There are four columns in Table 5.1 which are input data from the vector-to-stream block, output data from the stream-to-vector block and two key streams from the first LFSR block and the second LFSR block. All data in the table have already been converted to decimal numbers from 32-bit float numbers and complex float numbers which are in the endianness of LSB. The real part of the output data is the result of multiplying the real part of input data by the output of the first LFSR block. Similarly, we can multiply the imaginary part of input data by the output of the second LFSR block to get the imaginary part of output data. Comparing to the data given in [17], we can see that the implementation results match the theory.

| OFDM Enc(All Data in Decimal) | | | | | |
|---|---|---|---|---|---|
| Input Data | | LFSR 1 | LFSR 2 | Output Data | |
| 32-bit float Real | 32-bit float Imag | 32-bit float | 32-bit float | 32-bit float Real | 32-bit float Imag |
| 2.828427 | 0 | 1 | −1 | 2.828427 | 0 |
| −4.123229 | 11.220899 | −1 | 1 | 4.123229 | 11.220899 |
| −2.351751 | 2.903550 | −1 | −1 | 2.351751 | −2.903550 |
| −1.698666 | 2.050345 | −1 | −1 | 1.698666 | −2.050345 |
| −6.308644 | 5.860302 | −1 | −1 | 6.308644 | −5.860302 |
| 3.649297 | 4.588861 | −1 | −1 | −3.649297 | −4.588861 |
| 0.551799 | 2.123189 | 1 | −1 | 0.551799 | −2.123189 |
| −2.760114 | −6.491563 | −1 | 1 | 2.760114 | −6.491563 |
| 6 | −4 | 1 | −1 | 6 | 4 |
| 7.482303 | 5.606011 | −1 | 1 | −7.482303 | 5.606011 |
| 2.774080 | −0.422328 | −1 | −1 | −2.774080 | 0.422328 |
| −4.531216 | −0.472989 | 1 | −1 | −4.531216 | 0.472989 |

Table 5.1: Data Flow of the OFDM Enc

### 5.2.2 Implementation Results of OFDM Enc in DART-3300

The implementation in DART-3300 indicates that the OFDM system with the OFDM Enc encryption scheme can only demodulate correctly for the gain coefficient at 0.017 for the 6 cases in experimental group 1. For all 6 cases in group 2, the file-sink block after the demodulation did not capture anything for the gain coefficient set from 0.01 to 0.03 with step 0.001.

The first and second columns in Figure 5.2 represent the spectrums obtained from two 1024-FFT blocks respectively before and after the OFDM Enc encryption at the transmitter side. The third and fourth column in Figure 5.2 indicates the spectrums obtained from two 1024-FFT blocks respectively before and after the OFDM Enc decryption at the receiver side.

Each row in Figure 5.2 provides the spectrum for a choice of two key streams. In detail, the two key streams used from row 1 to row 5 satisfy $k_1 = k_2$, which are $(1, -1)$,$(1, -1, 1)$, $(1, -1, -1, 1)$,$(1, -1, -1, 1, 1)$, $(1, -1, 1, 1, 1, -1)$,$(1, -1, 1, 1, 1, -1, -1)$ respectively. The two key streams for the last row are different, i.e., $k_1 \neq k_2$ where $k_1 = [1, -1, 1, 1, 1, -1, -1]$ and $k_2 = [-1, 1, -1, 1, 1, 1, -1]$.

For the implementation in DART-3300, the BER for the six rows in Figure 5.2 is

$(0, 0.143,\ 0.0409,\ 0.0265, 0.328, 0.123, 0.5)$ obtained by comparing the message before the modulation and the message after the demodulation. Actually, the message before the OFDM modulation and the demodulated message are captured in binary comparison mode in Appendix C.

Figure 5.2 indicates the spectrums' power before and after the OFDM Enc encryption are $-55$ dB, and the spectrums' power before and after the OFDM Enc decryption are $-65$ dB. From Figure 5.2, we have following observations.

(i) The second column of Figure 5.2 indicates that the spectrum after the OFDM Enc encryption becomes flat as the length of the key bits increases.

(ii) The third column indicates that the received spectrums before the OFDM Enc decryption are similar to the original sent spectrum, which is the second column, except that the received power dropped to around 10 dB due to the transmission loss.

(iii) Comparing the first column with the fourth column indicates that spectrums after the OFDM decryption are recovered back to the original spectrums before the encryption for the first five rows in Figure 5.2. In opposition, the last row of the fourth column is still flat, and the file sink block at the receiver side did not capture anything after the demodulator.

(iv) The second column verifies that each of the 64 subcarriers are occupied if the period of the key stream is long enough.

The left side messages of Figure C.2 in Appendix C are the fragments of transmitted messages before the OFDM modulation. The right side messages of Figure C.2 are fragments of the received messages after the demodulation. Additionally, the highlighted parts in those figures indicate that the transmitted messages are either lost or changed. In detail, if both sides have highlight parts at the same corresponding location, then it is defined as changed bytes. If the highlight part only occurs at one side and the corresponding same location at the other side is empty, then it is defined as the lost bytes or inserted bytes. Furthermore, if the receiver cannot recognize the header information of a received frame, then it might be discarded.

### 5.2.3 Implementation Results of OFDM Enc in Laboratory

The implementation in the laboratory indicates that the OFDM system with the OFDM Enc encryption scheme can only demodulate correctly for the first five cases in the experimental group 1 with the gain coefficient of 0.017. For the last case in the experimental

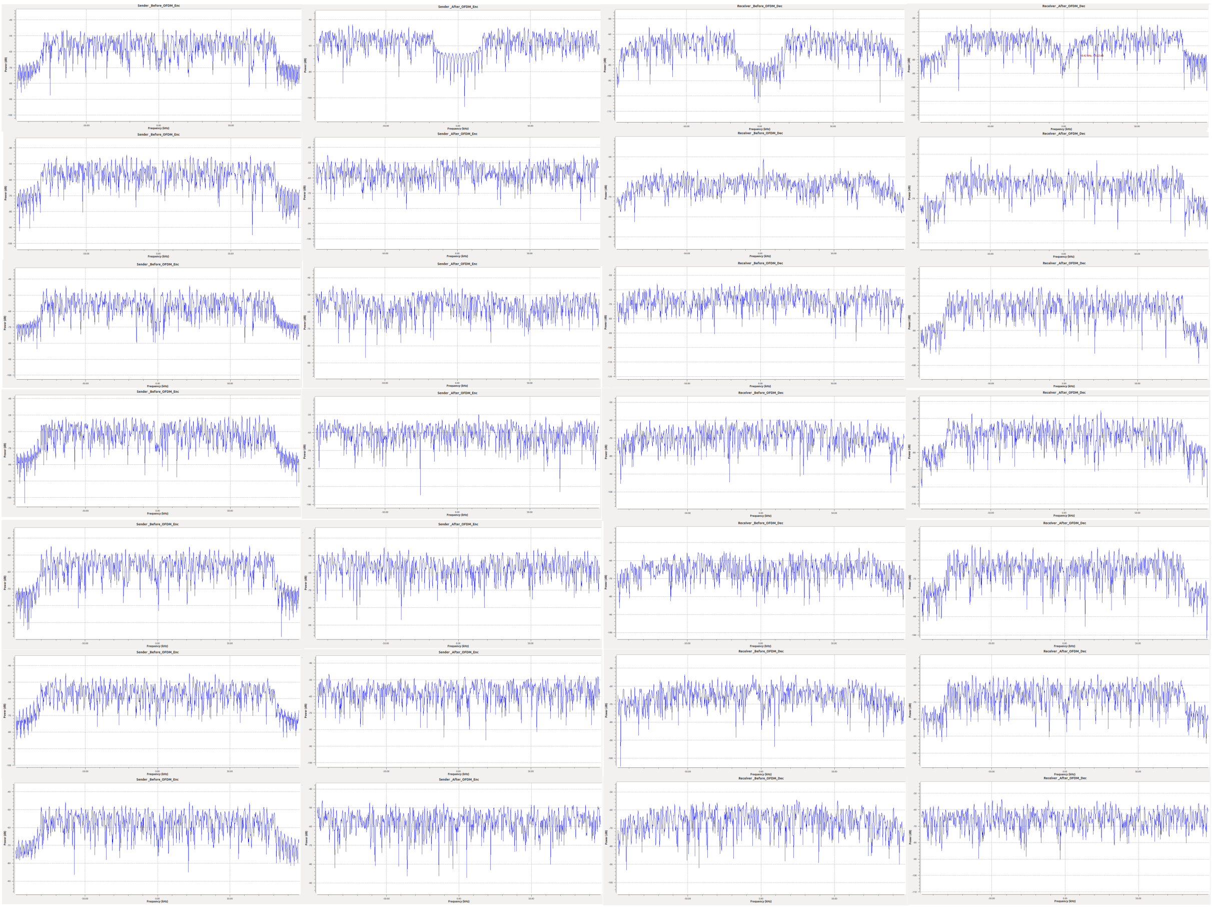


Figure 5.2: Spectrums of the OFDM System with OFDM Enc in the Chamber

group 1 and all cases in group 2, the file-sink block after the demodulation did not capture anything for the gain coefficient set from 0.01 to 0.03 with step 0.001.

The implementation results in the lab are shown in Figure 5.3 which has the same format as Figure 5.2 determined from the chamber, and keys are the same as the case in the chamber.

For the implementation in the lab, the best bit error rate for the six rows in Figure 5.3 are $(0, 0.189, 0.135, 0.0288, 0.3482, 0.5, 0.5)$ obtained by comparing the messages before the modulation and the received messages after the demodulation. Actually, the messages before the OFDM modulation and the demodulated messages are capture in binary comparison mode in Appendix C. From Figure 5.3 and the corresponding BER, we have the

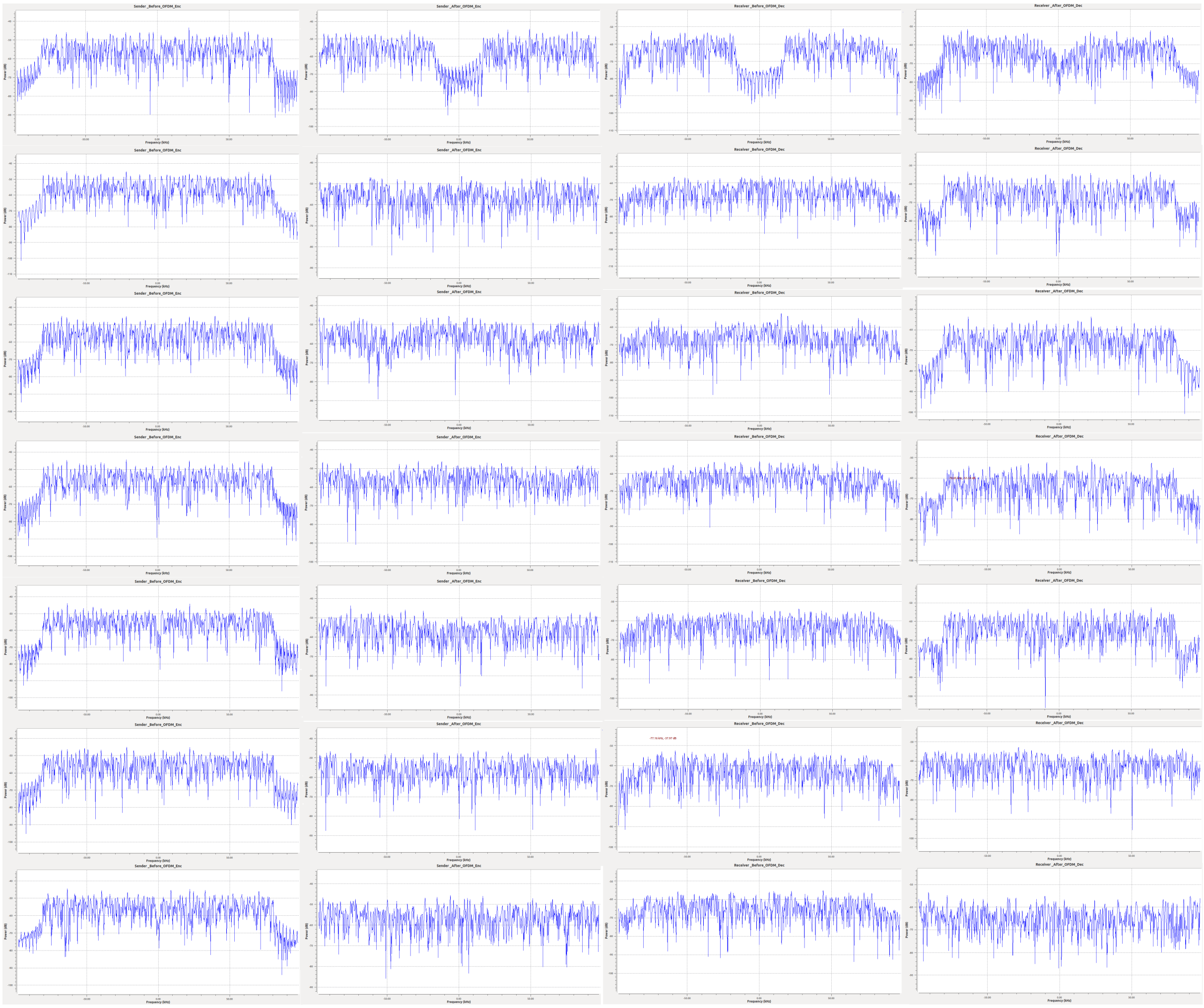


Figure 5.3: Spectrums of the OFDM System with OFDM Enc in the Lab

following observations.

(i) The spectrums' power before and after the OFDM Enc encryption are −55 dB, and the spectrums' power before and after the OFDM Enc decryption are −65 dB.

(ii) The spectrums after the OFDM Enc encryption become flat as the period of the key bits increases.

(iii) At the receiver side, the third column indicates the received spectrums before the

OFDM Enc decryption are similar to the original sent spectrum which is the second column except that the received power dropped to around 10 dB due to the transmission loss.

(iv) Comparing the first column and the fourth column, it indicates that spectrum after the OFDM decryption is recovered back to the original spectrums before the encryption for first four rows. In opposite, the last two rows of the fourth column are still flat, and the file sink block at the receiver side did not capture anything after the demodulator for these two cases.

(v) The second column verified that the entire 64 subcarriers are occupied if the randomness of the key stream is high enough, which agrees with the frequency mask property of the OFDM encryption scheme given in [17].

(vi) Case 6 in group 1 in the chamber has much better BER than that of Case 6 in the lab.

(vii) The BER is 0.5 for all 6 cases in experimental group 2 in the lab. From experimental group 1 and group 2, if the two key streams in the encryption are different, the BER will be 0.5.

(viii) The BER from the implementation of the OFDM without the OFDM Enc encryption scheme is significant low, and it does not have any bit errors in five minutes communication in both chamber and lab environment.

| Bit Error Rate from the Implementations | | |
|---|---|---|
| Cases | Chamber | Laboratory |
| *k1* = *k2* = (1,-1) | 0 | 0 |
| *k1* = *k2* = (1,-1,1) | 0.143 | 0.189 |
| *k1* = *k2* = (1,-1,-1,1) | 0.0409 | 0.135 |
| *k1* = *k2* = (1,-1,-1,1,1) | 0.265 | 0.0288 |
| *k1* = *k2* = (1,-1,1,1,1,-1) | 0.328 | 0.348 |
| *k1* = *k2* = (1,-1,1,1,1,-1,-1) | 0.123 | 0.5 |
| *k1* = (1,-1,1,1,1,-1,-1), *k2* = (-1,1,-1,1,1,1,-1) | 0.5 | 0.5 |

Table 5.2: Bit Error Rate from the Implementations in Both the Chamber and the Lab

### 5.2.4 Observation of OFDM Enc

Based on the tests results in both the lab and the chamber, the BER of the 7 cases discussed above is summarized in Table 5.2. The BER for each case in the lab is higher than the BER for each cases in the chamber respectively under the same SDR setting. In detail, the BER from Case 2 to Case 6 in group 1 are 0.189, 0.135,0.0288, 0.3482, 0.5, which are higher than those of 0.143, 0.0409, 0.0265,0.328,0.123 obtained from the chamber respectively. Additionally, results of using two different $m$-sequences in OFDM Enc always give 0.5 on BER in either lab or chamber. Finally, based on the simulations in GNU radio and implementations by USRP, the multipath boundary significantly decreases the performance of the OFDM Enc in practice. If the multipath ratio is lower than the desired BER point on the boundary, the OFDM system with OFDM Enc cannot achieve lower BER than that on the boundary even though the system has infinite SNR. The results also indicate that the OFDM system with OFDM Enc has much higher BER than that of the OFDM system without OFDM Enc if the multipath ratio is much lower than the boundary.

Since the chamber is an isolated environment without any channel effects, it is conjectured that there exist some unknown factors causing high BER in the chamber. One possible factor is the pilot symbols which are inserted in the subcarriers at [-7,-7,7,21]. For the tests in both the chamber and the lab, the OFDM Enc encrypted the pilot symbols at the sender side, then the pilot symbols may not contain proper channel information after the decryption at the receiver side. This causes the problem in the channel estimation. The second factor could be the noises in USRP deceives. If the OFDM Enc scheme is sensitive to phase noises or frequency offset generated by the USRP devices, then it could also cause high BER during the transmission. The third factor might be the synchronization issue between the transmitter and the receiver. The unsynchronized data at the receiver side may cause misalign between the received data and the key streams during the decryption process. Then the received encrypted data could not be decrypted properly, then it cause high BER after the demodulation.

# Chapter 6

# A New Frequency Hopping (FH) System

BLADES system was proposed in the middle of 1950s and successfully implemented in 1963 as the first working FH system in the world [5, 32, 34]. Based on the structure of BLADES given in Section 3.4.3, we propose a new frequency hopping system named *randomly selective m-sequence based BLADES (RSMB) system* in this chapter. Section 6.1 introduces the system model of the $m$-sequences based BLADES system and jammer. Section 6.2 gives the collision properties of two distinct binary primitive polynomials of the same degree in detail. Finally, Section 6.3 demonstrates the simulation results and two conjectures for the collision properties. In this chapter, we keep the notation introduced in Section 3.4 in Chapter 3.

## 6.1 System Model of M-sequences Based BLADES System and Jammer

Randomly selective $m$-sequence based BLADES system uses original BLADES system model given in [5, 32, 34], but it randomly selects two shift distinct m-sequences as key streams. Consider an FH system where $\Psi$ denotes the set of the available hopping frequencies. To simplify the notation, each available hopping frequency is represented by an integer value which belongs to the integer set $\Psi$. In detail, we denote $f_t \in \Psi$ as the hopping frequency at time slot $t, t \geq 0$, and the transmission starts from time slot 0. In Figure 3.3, use this notation we know that $\Psi = \{1, 2, 3, \ldots, 2^n - 1\}$. Before time slot 0, both the transmitter and the receiver know $f_t$ based on their pre-shared secret information. However, jammer does not know this information, so it cannot generate $f_t$; therefore, $f_t$ is a random variable for the jammer.

In order to jam the system, the jammer has two phases: discover phase and jamming phase. The jammer starts the discover phase by selecting a set $F$ ($F \subset \Psi$) of frequencies before time slot 0, and keeps monitoring $F$ starting from time slot 0. (Assume that the jammer can control the elements in $F$ while $|F|$ is fixed due to jammer's limited power.) Once $f_{t'}$ falls into $F$ (i.e., $f_{t'} \in F$) at a certain time slot $t'$, the jammer has successfully discovered the hopping frequency, and has been able to predict $f_t$ for $t > t'$. In this case, the jammer terminates the discover phase and starts the jamming phase by jamming the system from time slot $t' + 1$.

In RSMB system, assume that $\Psi = \{1, 2, \ldots, 2^n - 1\}$. There are two PRGs, which are $f(x)$ and $g(x)$ (randomly selected from $\mathcal{P}_n(x)$), used for generating two $m$-sequences respectively. Before starting the transmission at time slot 0, the transmitter and the receiver pre-share two $m$-sequences, say $\mathbf{a} \in G(f)$ and $\mathbf{b} \in G(g)$, for generating hopping frequencies. To be specific, at time slot $t, t \geq 0$, $f_t$ is determined by $\mathbf{a}[t, n]$ if the $t$-th sending bit is 0; otherwise, $f_t$ is determined by $\mathbf{b}[t, n]$.[1] Then, the transmitter sends some signal to the receiver at hopping frequency $f_t$.

As to the receiver, if any transmission is detected at hopping frequency $\mathbf{a}[t, n]$ but not at $\mathbf{b}[t, n]$ at time slot $t, t \geq 0$, the receiving bit will be identified as bit 0; if any transmission is detected at $\mathbf{b}[t, n]$ but not at $\mathbf{a}[t, n]$, the receiving bit will be identified as bit 1; however, if transmission is detected at both $\mathbf{a}[t, n]$ and $\mathbf{b}[t, n]$, the receiver is confused about the receiving bit, which is identified as a receiving failure. The receiving failure can be caused by either of two reasons:

(i) The jammer sends interference signal.

(ii) The collision happens between $\mathbf{a}$ and $\mathbf{b}$, where if $\mathbf{a}[t, n] = \mathbf{b}[t, n]$ for $t \geq 0$, $\mathbf{a}[t, n]$ is regarded as a collision between $\mathbf{a}$ and $\mathbf{b}$.

[1] As each $n$-tuple of bits in both $\mathbf{a}$ and $\mathbf{b}$ is one-to-one mapped to an element in $\Psi$, we also use $n$-tuple of bits, such as $\mathbf{a}[t, n]$, to refer to the hopping frequency.

## 6.2 Collision Properties of Two Distinct Binary Primitive Polynomials of the Same Degree

As discussed in Section 6.1, collisions between two $m$-sequences in the BLADES system will confuse the receiver. If two key streams generate the same bit at time moment $k$, then the receiver cannot figure out the sending bit based on the hopping frequency at the time slot $k$. The result is that the receiver has to randomly guess the bit, which increases the BER. Therefore, it is necessary to investigate the collision properties of two distinct binary primitive polynomials of the same degree.

**Definition 3.** *$\forall f(x) \neq g(x) \in \mathcal{P}_n(x)$, let*

$$\mathit{coll}(\mathbf{a}, \mathbf{b}) = \{\mathbf{a}[k, n] : 0 \leq k < N, \mathbf{a}[k, n] = \mathbf{b}[k, n]\}, \forall \mathbf{a} \in G(f), \mathbf{b} \in G(g)$$

*denote the set of collisions between $\mathbf{a}$ and $\mathbf{b}$. In addition, denote the set of collided sequence pairs between $G(f)^*$ and $G(g)^*$ as*

$$\mathit{coll}(f, g) = \{(\mathbf{a}, \mathbf{b}) : \mathbf{a} \in G(f)^*, \mathbf{b} \in G(g)^*, \mathit{coll}(\mathbf{a}, \mathbf{b}) \neq \emptyset\}$$

*and define the collision probability between $f(x)$ and $g(x)$ as*

$$P_{\mathit{coll}}(f, g) = \frac{|\mathit{coll}(f, g)|}{|G(f)^*| \cdot |G(g)^*|} = \frac{|\mathit{coll}(f, g)|}{N^2}.$$

### 6.2.1 Upper-Bound for the Collision Probability of Two Polynomials of $\mathcal{P}_n(x)$

In this subsection, the upper-bound for the collision probability of any two polynomials of $\mathcal{P}_n(x)$ is given.

**Lemma 1.** *$\forall f(x) \neq g(x) \in \mathcal{P}_n(x), \mathbf{a} \in G(f), \mathbf{b} \in G(g)$, let $\mathbf{z} = \mathbf{a}+\mathbf{b} = (a_0+b_0, a_1+b_1, \cdots)$. We have*

$$\mathit{coll}(\mathbf{a}, \mathbf{b}) = \{\mathbf{a}[k, n] : 0 \leq k < N, \mathbf{z}[k, n] = [0]^n\}$$

*where $[0]^n$ denotes a $n$-length zero-sequence.*

*Proof.* For $0 \leq k < N$, we have $\mathbf{a}[k, n] = \mathbf{b}[k, n] \iff \mathbf{z}[k, n] = [0]^n$. □

**Lemma 2.** *$\forall f(x) \neq g(x) \in \mathcal{P}_n(x)$, let $h(x) = f(x)g(x)$. We have*

$$G(h) = G(f) \oplus G(g) = \{\mathbf{a} + \mathbf{b} : \mathbf{a} \in G(f), \mathbf{b} \in G(g)\}.$$

*Moreover, $G(f)^* \oplus G(g)^*$ can be partitioned into $N$ shift-equivalent classes $G_0, G_1, \ldots, G_{2^n-2}$, where*

$$\begin{aligned} &G_i = \{L^j\mathbf{z} : j \geq 0\}, \forall \mathbf{z} \in G_i, 0 \leq i < N \\ &|G_0| = |G_1| = \cdots = |G_{2^n-2}| = N \\ &G_0 \cup G_1 \cup \cdots \cup G_{2^n-2} = G(f)^* \oplus G(g)^* \\ &G_i \cap G_j = \emptyset, 0 \leq i < j < N. \end{aligned}$$

*Proof.* This lemma comes from [11, Chapter 4]. □

**Theorem 1.** *$\forall f(x) \neq g(x) \in \mathcal{P}_n(x)$, we have*

$$P_{coll}(f, g) \leq 2^{n-1}/N.$$

*Proof.* See Appendix E. □

Based on Theorem 1, the upper-bound shows

$$\begin{aligned} 2^{n-1}/N &= 2^{n-1}/(2^n - 1) \\ &= 2^{n-1}/(2 \times 2^{n-1} - 1) \\ &= 0.5 \text{ as } n \to \infty. \end{aligned}$$

### 6.2.2 Upper-Bound for the Collision Probability of Reciprocal Polynomial Pairs of $\mathcal{P}_n(x)$

In this subsection, the upper-bound for the collision probability of reciprocal polynomial pairs of $\mathcal{P}_n(x)$ is given.

**Lemma 3.** *$\forall f(x) \in \mathcal{P}_n(x), \mathbf{a} \in G(f)^* \oplus G(f^{-1})^*$, there exists a unique integer $j, 0 \leq j < N$, satisfying*

$$L^j\mathbf{a} = (L^j\mathbf{a})^{-1}.$$

*Proof.* See Appendix F. □

**Theorem 2.** *$\forall f(x) \in \mathcal{P}_n(x)$, we have*

$$P_{coll}(f, f^{-1}) \leq (2^{n-2} - 1 + 2^{\lfloor n/2 \rfloor - 1} + 2^{\lceil n/2 \rceil - 1})/N.$$

*Proof.* See Appendix G. □

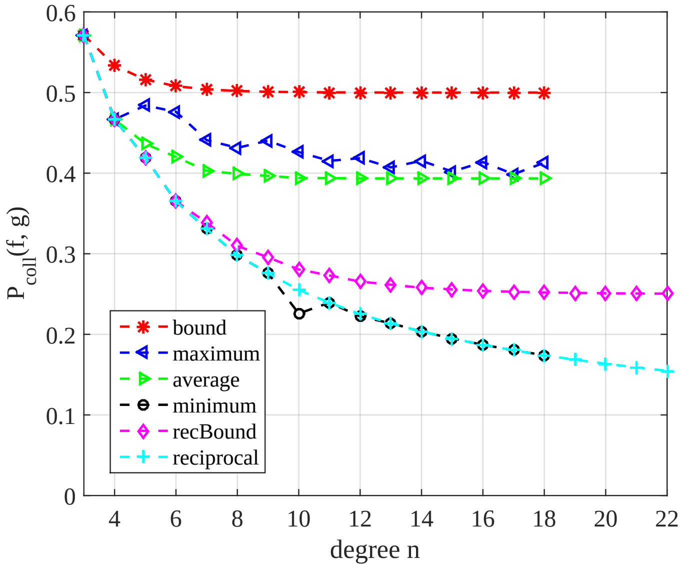


Figure 6.1: Collision Probabilities and Theoretical Upper-Bounds of Two Distinct Binary Primitive Polynomials of the Same Degree.

## 6.3 Simulations and Conjectures of the New Frequency Hopping System

Let

$$P_{coll}[n] = \{P_{coll}(f,g) : f(x) \neq g(x) \in \mathcal{P}_n(x)\}$$
$$P^{(r)}_{coll}[n] = \{P_{coll}(f,f^{-1}) : f(x) \in \mathcal{P}_n(x)\}.$$

For $f_1(x) \neq g_1(x) \in \mathcal{P}_n(x)$, $P_{coll}(f_1, f_1^{-1})$ and $P_{coll}(g_1, g_1^{-1})$ are regarded as two different elements in $P^{(r)}_{coll}[n]$; meanwhile, for $f_2(x) \neq g_2(x) \in \mathcal{P}_n(x)$, $P_{coll}(f_1, g_1)$ and $P_{coll}(f_2, g_2)$ are regarded as two different elements in $P_{coll}[n]$ if $f_1(x) \neq f_2(x)$ or $g_1(x) \neq g_2(x)$. Thus, we have $|P_{coll}[n]| = |\mathcal{P}_n(x)| \cdot (|\mathcal{P}_n(x)| - 1)$ and $|P^{(r)}_{coll}[n]| = |\mathcal{P}_n(x)|$.

Based on exhaustive simulation in Figure 6.1, we have $P_{coll}[n]$ for $3 \leq n \leq 18$ and $P^{(r)}_{coll}[n]$ for $3 \leq n \leq 22$. In Figure 6.1, the curves labeled as “bound”, “maximum”, “average”, and “minimum” display the theoretical upper-bound (see Theorem 1), maximum value, average value, and minimum value of $P_{coll}[n], 3 \leq n \leq 18$, respectively; meanwhile, the curves labeled as “recBound” and “reciprocal” display the theoretical upper-bound (see

Theorem 2) and the minimum value of $P_{coll}^{(r)}[n], 3 \leq n \leq 22$, respectively. Note that for $3 \leq n \leq 22$, the simulation results show that

$$\min P_{coll}^{(r)}[n] = \max P_{coll}^{(r)}[n].$$

In fact, we would like to give the following much stronger conjecture, which at least holds for $3 \leq n \leq 22$ according to the simulation results:

**Conjecture 1.** *$\forall f(x) \neq g(x) \in \mathcal{P}_n(x)$ and $\forall k \geq 0$, we have*

$$\begin{aligned} &|\{(\mathbf{a},\mathbf{b}) : \mathbf{a} \in G(f)^*, \mathbf{b} \in G(f^{-1})^*, |coll(\mathbf{a},\mathbf{b})| = k\}| \\ =&|\{(\mathbf{a},\mathbf{b}) : \mathbf{a} \in G(g)^*, \mathbf{b} \in G(g^{-1})^*, |coll(\mathbf{a},\mathbf{b})| = k\}|. \end{aligned}$$

Conjecture 1 indicates that the collision distribution in terms of the number of collisions versus the number of shifts of any two distinct reciprocal $m$-sequences of the same degree is the same.

Additionally, there are two assumptions based on the observation of the simulation results. One is that most elements of $P_{coll}[n] \setminus P_{coll}^{(r)}[n]$ may get close to 0.3935 as $n$ increases for $n \geq 10$ in general. From the simulation, the average value of $P_{coll}[n]$ gets close to 0.3935 as the degree $n$ increases from 10 to 18 and the variance in each degree becomes smaller and smaller as $n$ increases. For example, the average value and the variance of $P_{coll}[17]$ are 0.3935 and $8.3 \times 10^{-6}$, respectively, and the average value and the variance of $P_{coll}[18]$ are 0.3935 and $7.9 \times 10^{-6}$, respectively.

The other assumption is

$$\min P_{coll}[n] = \min P_{coll}^{(r)}[n], \forall n \geq 3, \text{ but not in } \setminus \{10, 12\}$$

based on the simulation which gives the above equation for $n \in \{3, 4, \cdots, 18\} \setminus \{10, 12\}$.

Note that the theoretical upper-bounds given by Theorems 1 and 2 converge to 0.5 and 0.25 respectively as $n$ increases to $+\infty$. Then, based on the two assumptions, we have the second conjecture shown below:

**Conjecture 2.**

$$\lim_{k \to +\infty} \frac{|\{i : 3 \leq i \leq k, \min P_{coll}[i] = \min P_{coll}^{(r)}[i]\}|}{k} = 1.$$

Conjecture 2 indicates that the collision probability of the reciprocal m-sequence pairs gives the minimum collision probability in most of primitive polynomial degrees.

*Note.* The detail of the new FH system in this chapter can be found in our draft [12].

# Chapter 7

# Conclusion and Future Work

This chapter demonstrates the contributions of this thesis and the future work.

## 7.1 Conclusion

In this thesis, our main contributions are in Chapter 4, 5 and 6. These are summarized below:

- **Implementations of the OFDM Enc by SDR:** In Chapter 4, we have implemented the OFDM system with OFDM Enc scheme under the IEEE802.11a standard in both microwave anechoic chamber and lab environment by SDR. Firstly, the spectrums at both sender side and receiver side are captured, and the best SDR has been counted for the OFDM encryption scheme. Secondly, we also used GNU radio to simulate the multipath AWGN channel in order to precisely check the influence of the OFDM Enc on the OFDM system. Lastly, the data of BER versus multipath ratio are also given by GNU radio, which is critical to show the multipath effect on OFDM Enc.

- **Found a multipath boundary in the OFDM Enc scheme:** Based on the implementation results in Chapter 5, if the two key streams are different in OFDM Enc, the OFDM decryption scheme cannot decrypt the received data under the multipath AWGN channel in practice. In detail, the implementation in GNU radio provides the multipath boundary which significantly decreases the performance of the OFDM Enc. For example, if the multipath ratio is fixed, the OFDM system with OFDM

Enc cannot achieve lower BER than that on the boundary even though the system has infinite SNR. The results also indicate that the OFDM system with OFDM Enc has much higher BER than that of the OFDM system without OFDM Enc if the multipath ratio is much lower than the boundary. Results of using two different $m$-sequences in OFDM Enc give significant high BER in either lab or chamber. Since the chamber is an isolated environment without any channel effects, it is conjectured that there exist some unknown factors causing the high BER in the chamber, such as pilot symbols, noises in USRP deceives and synchronization issues between the transmitter and the receiver.

- **Randomly selective *m*-sequence based BLADES system:** In chapter 6, we have proposed a new competitive FH system to overcome jamming attacks. The collision analysis and its exhaustive emulation on two distinct $m$-sequences of the same degree have been given. Based on the exhaustive emulation, we have proposed two conjectures. One indicates that all reciprocal $m$-sequence pairs of the same degree $n$ have the same collision distribution. The other one indicates that the collision probability of the reciprocal $m$-sequence pairs gives the minimum collision probability in most of primitive polynomial degrees. Additionally, the theoretical upper-bounds on the collision probability of two $m$-sequences of the same degree and the collision probability of two reciprocal $m$-sequences of the same degree are given to limit our conjectures.

## 7.2 Future Work

From the OFDM Enc encryption scheme given by [17], we found a multipath boundary in the scheme which significantly reduced the performance of the OFDM system. This finding is just one of significant channel effects on the system. Therefore, we will test other channel effects such as the doppler effect and the frequency selective fading effect on the OFDM system with the OFDM Enc encryption scheme. Also, the factors such as pilot symbols, synchronization issues and noises from USRPs will be investigated in order to reduce BER in OFDM Enc.

After obtaining those performance parameters of the OFDM Enc scheme, we will then work on removing those effects and improving the performance of the OFDM system with the OFDM Enc encryption scheme. The purpose would be to reduce the influence of the OFDM Enc encryption scheme on the performance of the OFDM system. Following successful improvement of the performance of the OFDM system with the OFDM encryption scheme, we plan to implement the OFDM Enc encryption scheme in LTE which has much more complex structure than that of the OFDM system under IEEE802.11a standard.

As to the randomly selective $m$-sequence based BLADES system, we will exam the jammer's expected discovery time in future. In detail, if the jammer can control the monitoring frequencies in order to achieve the lowest expected discovery time, it is necessary to investigate the jamming resistance of the randomly selective $m$-sequence based BLADES system.

# References

[1] A. Al-Dweik, M. Mirahmadi, A. Shami, B. Sharif, and R. Hamila. Joint secured and robust technique for ofdm systems, Dec 2013.

[2] A. Al-Dweik and A. Shami. Multitone jamming rejection of frequency hopped OFDM systems in wireless channels. In *Proc IEEE Vehicular Technology Conference*, pages 1–6, Quebec City, QC, Canada, Sep. 2012.

[3] J. B. Andersen, T. S. Rappaport, and S. Yoshida. Propagation measurements and models for wireless communications channels. *IEEE Communications Magazine*, 33(1):42–49, Jan 1995.

[4] R. W. Chang. Synthesis of band-limited orthogonal signals for multichannel data transmission. *The Bell System Technical Journal*, 45(10):1775–1796, Dec 1966.

[5] L. Chen and G. Gong. *Communication System Security*. CRC Press.

[6] S. Fang, Y. Liu, and P. Ning. Wireless communications under broadband reactive jamming attacks. *IEEE Transactions on Dependable and Secure Computing*, 13(3):394–408, May 2016.

[7] S.G. Glisic. *Adaptive WCDMA: Theory and Practice*. Wiley, 2003.

[8] Andrea Goldsmith. *Wireless Communications*. Cambridge University Press, 2005.

[9] S. Gollakota and D. Katabi. ijam: Jamming oneself for secure wireless communication, June 2010.

[10] Solomon W. Golomb. *Shift Register Sequences*. Aegean Park Press, Laguna Hills, CA, 1982.

[11] Solomon W. Golomb and Guang Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge University Press, 2005.

[12] G. Gong, X. He, and Y. Yi. Reactive jamming attacks on FH systems (in preparation for submission). July 2018.

[13] A. Gupta and R. K. Jha. A survey of 5G network: architecture and emerging technologies. *IEEE Access*, 3:1206–1232, Jul. 2015.

[14] F. He, H. Man, and W. Wang. Physical layer assisted security for mobile ofdm networks, Dec 2010.

[15] Y. Hou and T. Hase. New ofdm structure to smooth frequency notches of wireless channel. In *2009 Fourth International Conference on Communications and Networking in China*, pages 1–5, Aug 2009.

[16] X. Huang. Effect of dc offset on ofdm system with zero-padded suffix. In *2006 International Symposium on Communications and Information Technologies*, pages 503–506, Oct 2006.

[17] F. Huo and G. Gong. A new efficient physical layer ofdm encryption scheme. In *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pages 1024–1032, April 2014.

[18] Keysight Technologies Inc. Concepts of orthogonal frequency division multiplexing (ofdm) and 802.11 wlan. http://rfmw.em.keysight.com/wireless/helpfiles/89600b/webhelp/subsystems/wlan-ofdm/content/ofdm_basicprinciplesoverview.htm. Accessed: 2018-06-09.

[19] Keysight Technologies Inc. Lte physical layer overview. http://rfmw.em.keysight.com/wireless/helpfiles/89600b/webhelp/subsystems/lte/content/lte_overview.htm. Accessed: 2018-06-09.

[20] S. Kiambi, E. Mwangi, and G. Kamucha. Effect of ofdm signal structure and subcarrier modulation on the reduction of the signal peak power. In *2017 IEEE AFRICON*, pages 262–266, Sept 2017.

[21] An Liu, Peng Ning, Huaiyu Dai, Yao Liu, and Cliff Wang. Defending DSSS-based broadcast communication against insider jammers via delayed seed-disclosure. In *Proc. Annual Computer Security Application Conference*, pages 367–376, Dec. 2010.

[22] Chia-Yu Liu, Y. W. P. Hong, Pin-Hsun Lin, and E. A. Jorswieck. Jamming-resistant frequency hopping system with secret key generation from channel observations. In *Proc IEEE Information Theory Workshop*, pages 46–50, Cambridge, UK, Sep. 2016.

[23] N. N. N. A. Malik, N. Ngajikin, S. M. Idrus, and N. D. A. Latif. Peak to average power ratio (papr) reduction in ofdm system. In *2006 International RF and Microwave Conference*, pages 75–79, Sept 2006.

[24] M. S. Mohamad, M. H. A. Wahid, M. A. M. Azidin, N. A. Rahman, N. R. Yusof, and N. A. M. A. Hambali. Analysis of OTDM data for high speed all optical shift register. In *Proc International Conference on Electronic Design*, pages 335–338, Aug. 2014.

[25] T. Nawaz, L. Marcenaro, and C. S. Regazzoni. Defense against jamming attacks in wide-band radios using cyclic spectral analysis and compressed sensing. In *Proc International Conference on Ubiquitous and Future Networks*, pages 874–879, Milan, Italy, Jul. 2017.

[26] S. Ohno. Preamble and pilot symbol design for channel estimation in ofdm. In *2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07*, volume 3, pages III–281–III–284, April 2007.

[27] A.V. Oppenheim, R.W. Schafer, and J.R. Buck. *Discrete-time Signal Processing*. Prentice Hall international editions. Prentice Hall, 1999.

[28] A.V. Oppenheim, A.S. Willsky, and S.H. Nawab. *Signals and Systems*. Prentice-Hall signal processing series. Prentice Hall, 1997.

[29] R. Poisel. *Modern Communications Jamming: Principles and Techniques*. Artech House, 2011.

[30] R. Scholtz. Multiple access with time-hopping impulse modulation. In *Proc. IEEE Military Communications Conference*, volume 2, pages 447–450, Boston, MA, USA, Oct. 1993.

[31] J. L. Seoane, S. K. Wilson, and S. Gelfand. Analysis of intertone and interblock interference in ofdm when the length of the cyclic prefix is shorter than the length of the impulse response of the channel. In *GLOBECOM 97. IEEE Global Telecommunications Conference. Conference Record*, volume 1, pages 32–36 vol.1, Nov 1997.

[32] A. B. Shah. Software-based implementation of a frequency hopping two-way radio, May 1997.

[33] M. Simon, J. Omura, R. Scholtz, and B. Levitt. *Spread Spectrum Communications Handbook*. McGraw-Hill Professional, 2001.

[34] Marvin K. Simon, Jim K. Omura, Robert A. Scholtz, and Barry K. Levitt. *Spread Spectrum Communications: Vol. 1.* Rockville, Maryland: Computer Science Press.

[35] H. Steendam. How to select the pilot carrier positions in cp-ofdm? In *2013 IEEE International Conference on Communications (ICC)*, pages 3148–3153, June 2013.

[36] L. C. Tran, D. T. Nguyen, F. Safaei, and P. J. Vial. An experimental study of ofdm in software defined radio systems using gnu platform and usrp2 devices. In *2014 International Conference on Advanced Technologies for Communications (ATC 2014)*, pages 657–662, Oct 2014.

[37] J. Vlaović, S. Rimac-Drlje, and G. Horvat. Overview of ofdm channel estimation techniques for dvb-t2 systems. In *2016 International Conference on Smart Systems and Technologies (SST)*, pages 75–80, Oct 2016.

[38] X. Yang, R. J. Manning, and W. Hu. Simple 40 Gbit/s all-optical XOR gate. *Electronics Letters*, 46(3):229–230, Feb. 2010.

[39] C. H. Yih. Analysis and compensation of dc offset in ofdm systems over frequency-selective rayleigh fading channels. *IEEE Transactions on Vehicular Technology*, 58(7):3436–3446, Sept 2009.

[40] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong. Design of an ofdm physical layer encryption scheme, March 2017.

# APPENDICES

# Appendix A

# DATA: Multipath Channel Boundary

| Multipath Boundary | | | |
|---|---|---|---|
| Fir Filter Taps' Coeffecients | Ratio | Without Enc | With Enc |
| [0.799,0.201] | 3.98 | 0 | 5.000E-01 |
| [0.805,0.195] | 4.13 | 0 | 3.131E-01 |
| [0.814,0.186] | 4.38 | 0 | 2.579E-01 |
| [0.823,0.177] | 4.65 | 0 | 2.166E-01 |
| [0.832,0.168] | 4.95 | 0 | 1.282E-01 |
| [0.842,0.158] | 5.33 | 0 | 6.278E-02 |
| [0.851,0.149] | 5.71 | 0 | 1.007E-02 |
| [0.856,0.144] | 5.94 | 0 | 1.225E-04 |
| [0.861,0.139] | 6.19 | 0 | 2.350E-06 |
| [0.882,0.118] | 7.47 | 0 | 8.660E-07 |
| [0.892,0.108] | 8.26 | 0 | - |
| [0.914,0.086] | 10.63 | 0 | - |
| [0.937,0.063] | 14.87 | 0 | - |

Table A.1: Multipath Boundary

# Appendix B

# DATA: AWGN Multipath Channel with SNR

| AWGN Multipath Channel with SNR $\approx 18.8dB$ | | | |
|---|---|---|---|
| Fir Filter Taps' Coeffecients | Ratio | Without Enc | With Enc |
| [0.799,0.201] | 3.98 | 1.259E-05 | - |
| [0.805,0.195] | 4.13 | 9.931E-06 | - |
| [0.814,0.186] | 4.38 | 7.762E-06 | - |
| [0.823,0.177] | 4.65 | 6.166E-06 | - |
| [0.832,0.168] | 4.95 | 5.012E-06 | 3.253E-01 |
| [0.842,0.158] | 5.33 | 3.162E-06 | 2.212E-01 |
| [0.851,0.149] | 5.71 | 2.729E-06 | 1.919E-01 |
| [0.861,0.139] | 6.19 | 1.995E-06 | 9.303E-02 |
| [0.882,0.118] | 7.47 | 1.629E-06 | 6.141E-03 |
| [0.892,0.108] | 8.26 | 1.380E-06 | 9.041E-04 |
| [0.914,0.086] | 10.63 | - | 1.130E-05 |
| [0.937,0.063] | 14.87 | - | 1.928E-06 |

Table B.1: AWGN Multipath Channel with SNR $\approx 18.8dB$

| AWGN Multipath Channel with SNR $\approx 20.1dB$ | | | |
|---|---|---|---|
| Fir Filter Taps' Coeffecients | Ratio | Without Enc | With Enc |
| [0.799,0.201] | 3.98 | 1.28825E-06 | - |
| [0.805,0.195] | 4.13 | 1.25893E-06 | - |
| [0.814,0.186] | 4.38 | 1.23027E-06 | - |
| [0.823,0.177] | 4.65 | 1.20226E-06 | 2.999E-01 |
| [0.832,0.168] | 4.95 | 1.1695E-06 | 2.344E-01 |
| [0.842,0.158] | 5.33 | 1.02329E-06 | 1.315E-01 |
| [0.851,0.149] | 5.71 | 9.77237E-07 | 4.716E-02 |
| [0.861,0.139] | 6.19 | 8.12831E-07 | 1.178E-02 |
| [0.882,0.118] | 7.47 | 7.24436E-07 | 4.377E-05 |
| [0.892,0.108] | 8.26 | 6.60693E-07 | 3.184E-06 |
| [0.914,0.086] | 10.63 | - | 4.898E-07 |
| [0.937,0.063] | 14.87 | - | 2.754E-07 |

Table B.2: AWGN Multipath Channel with SNR $\approx 20.1dB$

# Appendix C

# Fragments of Sent and Received Messages for the Implementation in Chamber

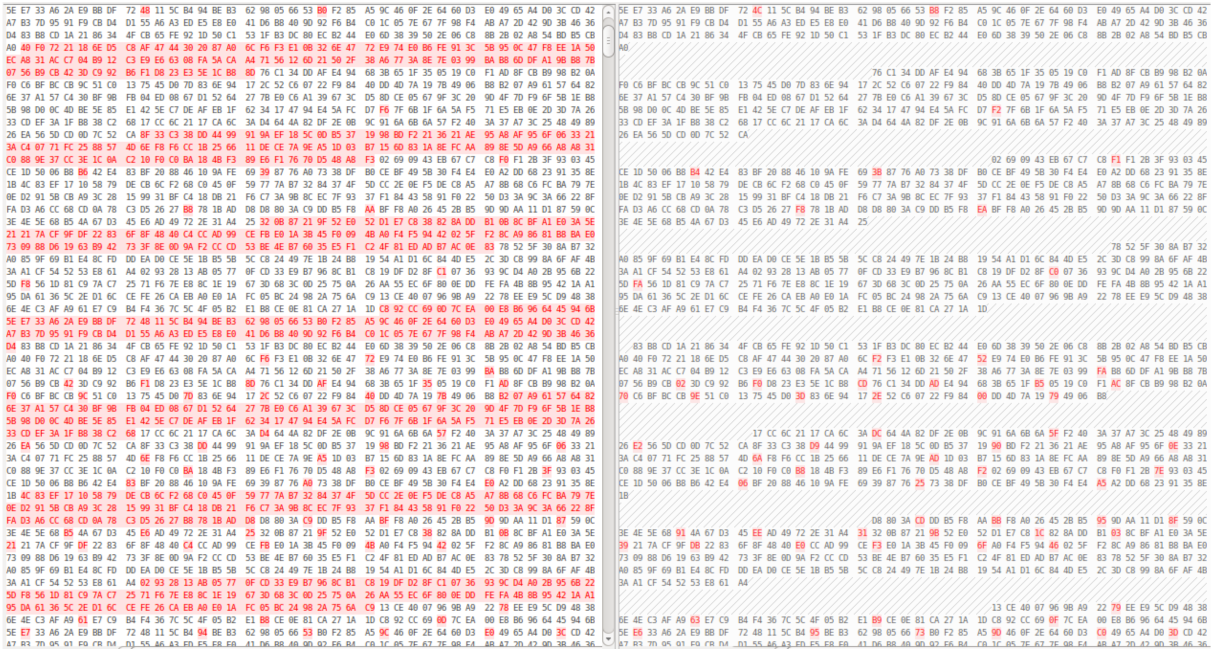


Figure C.1: Sent and Received Messages for the Case with $k1 = k2 = (1, -1, 1)$ in the Chamber

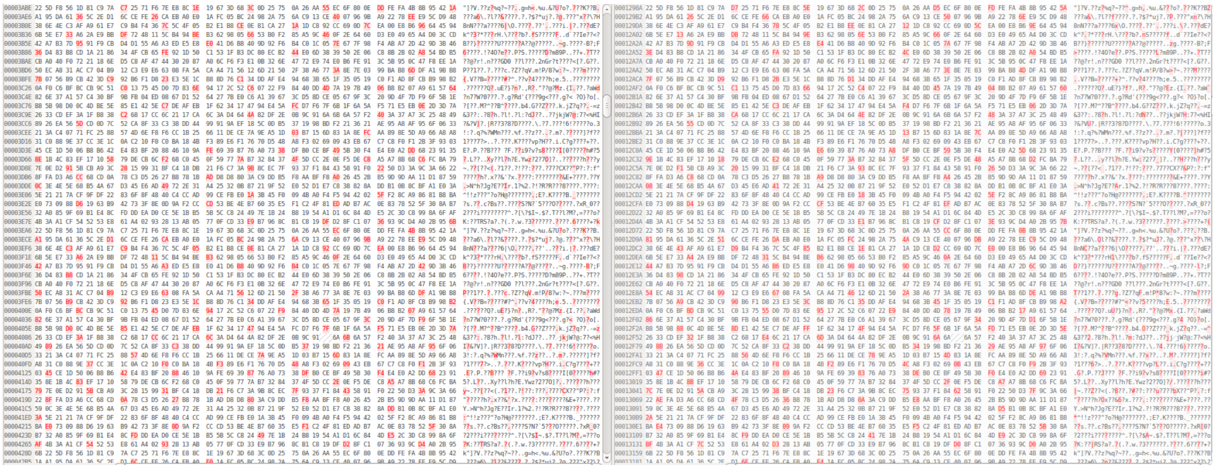
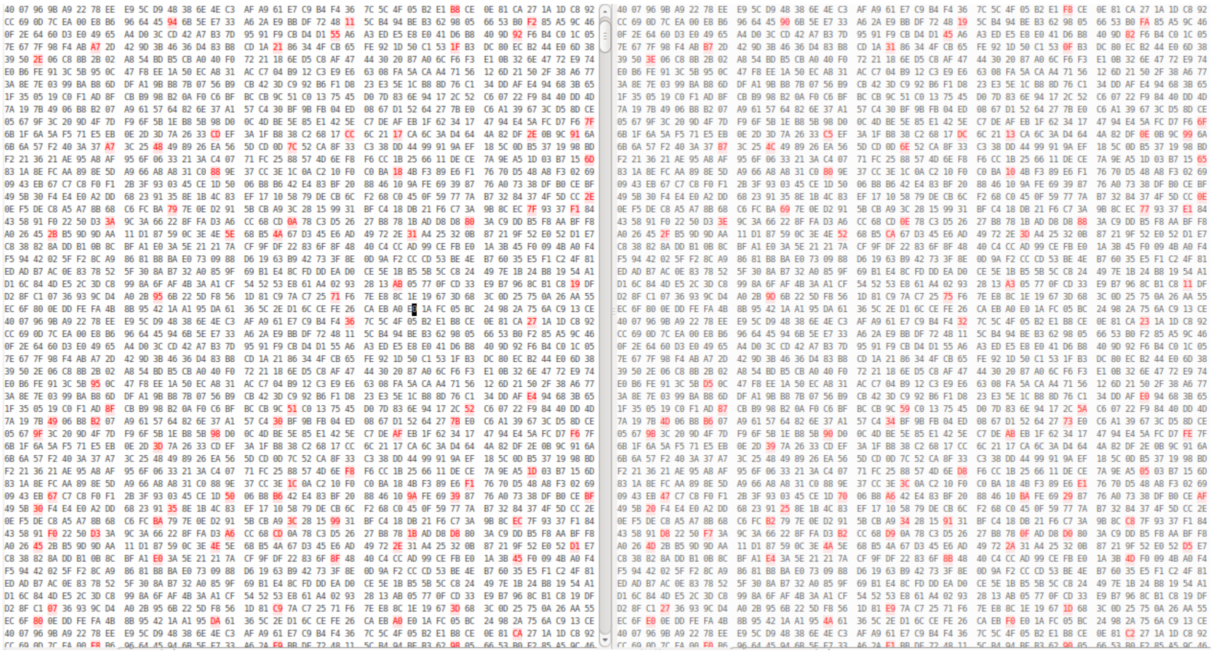
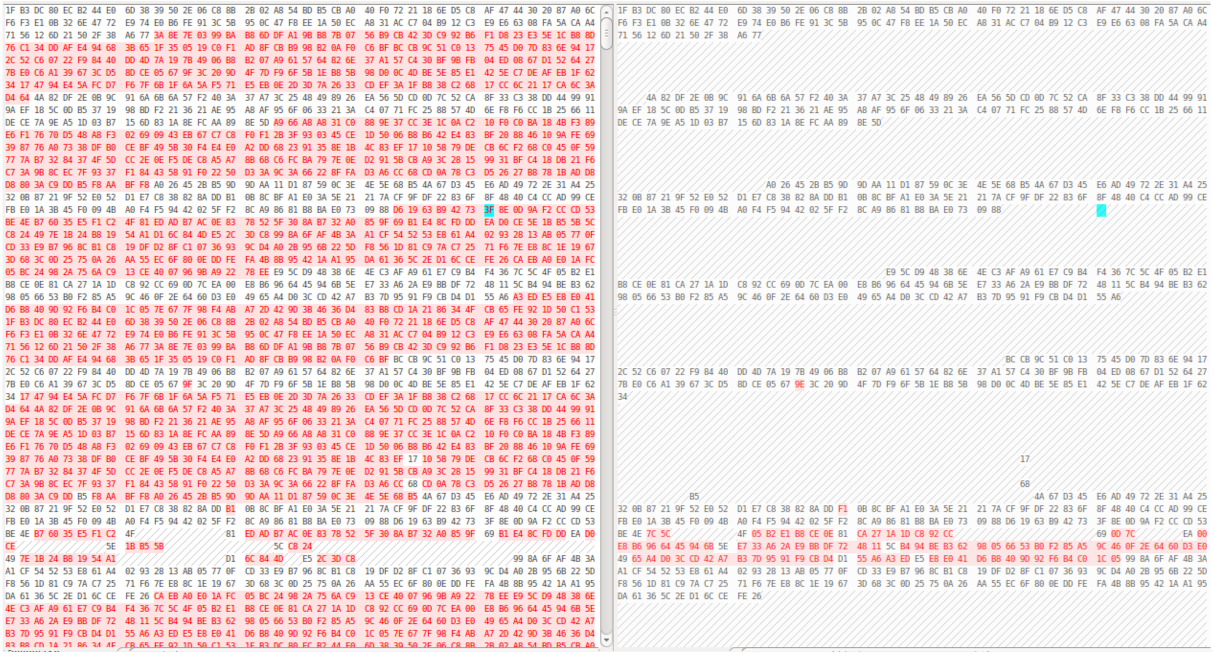


Figure C.2: Sent and Received Messages for the Case with $k1 = k2 = (1, -1, -1, 1)$ in the Chamber



```
40 07 96 9B A9 22 78 EE  E9 5C D9 48 38 6E 4E C3  AF A9 61 E7 C9 B4 F4 36  7C 5C 4F 05 B2 E1 B8 CE  0E 81 CA 27 1A 1D C8 92    40 07 96 9B A9 22 78 EE  E9 5C D9 48 38 6E 4E C3  AF A9 61 E7 C9 B4 F4 36  7C 5C 4F 05 B2 E1 F8 CE  0E 81 CA 27 1A 1D C8 92
CC 69 0D 7C EA 00 E8 B6  96 64 45 94 6B 5E E7 33  A6 2A E9 BB DF 72 48 11  5C B4 94 BE B3 62 98 05  66 53 B0 F2 85 A5 9C 46    CC 69 0D 7C EA 00 E8 B6  96 64 45 90 6B 5E E7 33  A6 2A E9 BB DF 72 48 19  5C B4 94 BE B3 62 98 05  66 53 B0 FA 85 A5 9C 46
0F 2E 64 60 D3 E0 49 65  A4 D0 3C CD 42 A7 B3 7D  95 91 F9 CB D4 D1 55 A6  A3 ED E5 E8 E0 41 D6 B8  40 9D 92 F6 B4 C0 1C 05    0F 2E 64 60 D3 E0 49 65  A4 D0 3C CD 42 A7 B3 7D  95 91 F9 CB D4 D1 45 A6  A3 ED E5 E8 E0 41 D6 B8  40 9D 82 F6 B4 C0 1C 05
7E 67 7F 98 F4 AB A7 2D  42 9D 3B 46 36 D4 83 B8  CD 1A 21 86 34 4F CB 65  FE 92 1D 50 C1 53 1F B3  DC 80 EC B2 44 E0 6D 38    7E 67 7F 98 F4 AB B7 2D  42 9D 3B 46 36 D4 83 B8  CD 1A 31 86 34 4F CB 65  FE 92 1D 50 C1 53 0F B3  DC 80 EC B2 44 E0 6D 38
39 50 2E 06 C8 8B 2B 02  A8 54 BD B5 CB A0 40 F0  72 21 18 6E D5 C8 AF 47  44 30 20 87 A0 6C F6 F3  E1 0B 32 6E 47 72 E9 74    39 50 3E 06 C8 8B 2B 02  A8 54 BD B5 CB A0 40 F0  72 21 18 6E D5 C8 AF 47  44 30 20 87 A0 6C F6 F3  E1 0B 32 6E 47 72 E9 74
E0 B6 FE 91 3C 5B 95 0C  47 F8 EE 1A 50 EC A8 31  AC C7 04 B9 12 C3 E9 E6  63 08 FA 5A CA A4 71 56  12 6D 21 50 2F 38 A6 77    E0 B6 FE 91 3C 5B 95 0C  47 F8 EE 1A 50 EC A8 31  AC C7 04 B9 12 C3 E9 E6  63 08 FA 5A CA A4 71 56  12 6D 21 50 2F 38 A6 77
3A 8E 7E 03 99 BA B8 6D  DF A1 9B B8 7B 07 56 B9  CB 42 3D C9 92 B6 F1 D8  23 E3 5E 1C B8 8D 76 C1  34 DD AF E4 94 68 3B 65    3A 8E 7E 03 99 BA B8 6D  DF A1 9B B8 7B 07 56 B9  CB 42 3D C9 92 B6 F1 D8  23 E3 5E 1C B8 8D 76 C1  34 DD AF E4 94 68 3B 65
1F 35 05 19 C0 F1 AD 8F  CB B9 98 B2 0A F0 C6 BF  BC CB 9C 51 C0 13 75 45  D0 7D 83 6E 94 17 2C 52  C6 07 22 F9 84 40 DD 4D    1F 35 05 19 C0 F1 AD 8F  CB B9 98 B2 0A F0 C6 BF  BC CB 9C 51 C0 13 75 45  D0 7D 83 6E 94 17 2C 52  C6 07 22 F9 84 40 DD 4D
7A 19 7B 49 06 B8 B2 07  A9 61 57 64 82 6E 37 A1  57 C4 30 BF 9B FB 04 ED  08 67 D1 52 64 27 7B E0  C6 A1 39 67 3C D5 8D CE    7A 19 7B 49 06 B8 B2 07  A9 61 57 64 82 6E 37 A1  57 C4 30 BF 9B FB 04 ED  08 67 D1 52 64 27 7B E0  C6 A1 39 67 3C D5 8D CE
05 67 9F 3C 20 9D 4F 7D  F9 6F 5B 1E B8 5B 98 D0  0C 4D BE 5E 85 E1 42 5E  C7 DE AF EB 1F 62 34 17  47 94 E4 5A FC D7 F6 7F    05 67 9F 3C 20 9D 4F 7D  F9 6F 5B 1E B8 5B 98 D0  0C 4D BE 5E 85 E1 42 5E  C7 DE AF EB 1F 62 34 17  47 94 E4 5A FC D7 F6 6F
6B 1F 6A 5A F5 71 E5 EB  0E 2D 3D 7A 26 33 CD EF  3A 1F B8 38 C2 68 17 CC  6C 21 17 CA 6C 3A D4 64  4A 82 DF 2E 0B 9C 91 6A    6B 1F 6A 5A F5 71 E5 EB  0E 2D 3D 7A 26 33 C5 EF  3A 1F B8 38 C2 68 17 DC  6C 21 13 CA 6C 3A D4 64  4A 82 DF 0E 0B 9C 99 6A
6B 6A 57 F2 40 3A 37 A7  3C 25 48 49 89 26 EA 56  5D CD 0D 7C 52 CA 8F 33  C3 38 DD 44 99 91 9A EF  18 5C 0D B5 37 19 98 BD    6B 6A 57 F2 40 3A 37 B7  3C 25 4C 49 89 26 EA 56  5D CD 0D 6E 52 CA 8F 33  C3 38 DD 44 99 91 9A EF  18 5C 0D B5 37 19 98 BD
F2 21 36 21 AE 95 A8 AF  95 6F 06 33 21 3A C4 07  71 FC 25 88 57 4D 6E F8  F6 CC 1B 25 66 11 DE CE  7A 9E A5 1D 03 B7 15 6D    F2 21 36 21 AE 95 A8 AF  95 6F 06 33 21 3A C4 07  71 FC 25 88 57 4D 6E F8  F6 CC 1B 25 66 11 DE CE  7A 9E A5 1D 03 B7 15 65
83 1A 8E FC AA 89 8E 5D  A9 66 A8 A8 31 C0 88 9E  37 CC 3E 1C 0A C2 10 F0  C0 BA 18 4B F3 89 E6 F1  76 70 D5 48 A8 F3 02 69    83 1A 8E FC AA 89 8E 5D  A9 66 A8 A8 31 C0 80 9E  37 CC 3E 1C 0A C2 10 F0  C0 BA 10 4B F3 89 E6 F1  76 70 D5 48 A8 F3 02 69
09 43 EB 67 C7 C8 F0 F1  2B 3F 93 03 45 CE 1D 50  06 B8 B6 42 E4 83 BF 20  88 46 10 9A FE 69 39 87  76 A0 73 38 DF B0 CE BF    09 43 EB 67 C7 C8 F0 F1  2B 3F 93 03 45 CE 1D 50  06 B8 B6 42 E4 83 BF 20  88 46 10 9A FE 69 39 87  76 A0 73 38 DF B0 CE BF
49 5B 30 F4 E4 E0 A2 DD  68 23 91 35 8E 1B 4C 83  EF 17 10 58 79 DE CB 6C  F2 68 C0 45 0F 59 77 7A  B7 32 84 37 4F 5D CC 2E    49 5B 30 F4 E4 E0 A2 DD  68 23 91 35 8E 1B 4C 83  EF 17 10 58 79 DE CB 6C  F2 68 C0 45 0F 59 77 7A  B7 32 84 37 4F 5D CC 0E
0E F5 DE C8 A5 A7 8B 68  C6 FC BA 79 7E 0E D2 91  5B CB A9 3C 28 15 99 31  BF C4 18 DB 21 F6 C7 3A  9B 8C EC 7F 93 37 F1 84    0E F5 DE C8 A5 A7 8B 68  C6 FC BA 69 7E 0E D2 91  5B CB A9 3C 28 15 99 31  BF C4 18 DB 21 F6 C7 3A  9B 8C EC 77 93 37 E1 84
43 58 91 F0 22 50 D3 3A  9C 3A 66 22 8F FA D3 A6  CC 68 CD 0A 78 C3 D5 26  27 B8 78 1B AD D8 D8 80  3A C9 DD B5 F8 AA BF F8    43 58 91 F0 22 50 D3 3E  9C 3A 66 22 8F FA D3 A6  CC 68 CD 0E 78 C3 D5 26  27 B8 78 1B AD D8 D8 88  3A C9 DD B5 F8 AA BF F8
A0 26 45 2B B5 9D 9D AA  11 D1 87 59 0C 3E 4E 5E  68 B5 4A 67 D3 45 E6 AD  49 72 2E 31 A4 25 32 0B  87 21 9F 52 E0 52 D1 E7    A0 26 45 2F B5 9D 9D AA  11 D1 87 59 0C 3E 4E 52  68 B5 CA 67 D3 45 E6 AD  49 72 2E 3D A4 25 32 0B  87 21 9F 52 E0 52 D1 E7
C8 38 82 8A DD B1 0B 8C  BF A1 E0 3A 5E 21 21 7A  CF 9F DF 22 83 6F 8F 48  40 C4 CC AD 99 CE FB E0  1A 3B 45 F0 09 4B A0 F4    C8 38 82 8A DD B1 0B 8C  BF A1 E0 3A 5E 21 21 7A  CF 9F DF 22 83 6F 8F 48  40 C4 CC AD 99 CE FB E0  1A 3B 45 F0 09 4B A0 F4
F5 94 42 02 5F F2 8C A9  86 81 B8 BA E0 73 09 88  D6 19 63 B9 42 73 3F 8E  0D 9A F2 CC CD 53 BE 4E  B7 60 35 E5 F1 C2 4F 81    F5 94 42 02 5F F2 8C A9  86 81 B8 BA E0 73 09 88  D6 19 63 B9 42 73 3F 8E  0D 9A F2 CC CD 53 BE 4E  B7 60 35 E5 F1 C2 4F 81
ED AD B7 AC 0E 83 78 52  5F 30 8A B7 32 A0 85 9F  69 B1 E4 8C FD DD EA D0  CE 5E 1B B5 5B 5C C8 24  49 7E 1B 24 B8 19 54 A1    ED AD B7 AC 0E 83 78 52  5F 30 8A B7 32 A0 85 9F  69 B1 E4 8C FD DD EA D0  CE 5E 1B B5 5B 5C C8 24  49 7E 1B 24 B8 19 54 A1
D1 6C 84 4D E5 2C 3D C8  99 8A 6F AF 4B 3A A1 CF  54 52 53 E8 61 A4 02 93  28 13 AB 05 77 0F CD 33  E9 B7 96 8C B1 C8 19 DF    D1 6C 84 4D E5 2C 3D C8  99 8A 6F AF 4B 3A A1 CF  54 52 53 E8 61 A4 02 93  28 13 A3 05 77 0F CD 33  E9 B7 96 8C B1 C8 11 DF
D2 8F C1 07 36 93 9C D4  A0 2B 95 6B 22 5D F8 56  1D 81 C9 7A C7 25 71 F6  7E E8 8C 1E 19 67 3D 68  3C 0D 25 75 0A 26 AA 55    D2 8F C1 07 36 93 9C D4  A0 2B 9D 6B 22 5D F8 56  1D 81 C9 7A C7 25 75 F6  7E E8 8C 1E 19 67 3D 68  3C 0D 25 75 0A 26 AA 55
EC 6F 80 0E DD FE FA 4B  8B 95 42 1A A1 95 DA 61  36 5C 2E D1 6C CE FE 26  CA EB A0 E0 1A FC 05 BC  24 98 2A 75 6A C9 13 CE    EC 6F 80 0E DD FE FA 4B  8B 95 42 1A A1 95 DA 61  36 5C 2E D1 6C CE FE 26  CA EB A0 E0 1A FC 05 BC  24 98 2A 75 6A C9 13 CE
40 07 96 9B A9 22 78 EE  E9 5C D9 48 38 6E 4E C3  AF A9 61 E7 C9 B4 F4 36  7C 5C 4F 05 B2 E1 B8 CE  0E 81 CA 27 1A 1D C8 92    40 07 96 9B A9 22 78 EE  E9 5C D9 48 38 6E 4E C3  AF A9 61 E7 C9 B4 F4 32  7C 5C 4F 05 B2 E1 B8 CE  0E 81 CA 23 1A 1D C8 92
CC 69 0D 7C EA 00 E8 B6  96 64 45 94 6B 5E E7 33  A6 2A E9 BB DF 72 48 11  5C B4 94 BE B3 62 98 05  66 53 B0 F2 85 A5 9C 46    CC 69 0D 7C EA 00 E8 B6  96 64 45 94 6B 5E E7 33  A6 2A E9 BB DF 72 48 11  5C B4 94 BE B3 62 98 05  66 53 B0 F2 85 A5 9C 46
0F 2E 64 60 D3 E0 49 65  A4 D0 3C CD 42 A7 B3 7D  95 91 F9 CB D4 D1 55 A6  A3 ED E5 E8 E0 41 D6 B8  40 9D 92 F6 B4 C0 1C 05    0F 2E 64 60 D3 E0 49 65  A4 D0 3C CD 42 A7 B3 7D  95 91 F9 CB D4 D1 55 A6  A3 ED E5 E8 E0 41 D6 B8  40 9D 92 F6 B4 C0 1C 05
7E 67 7F 98 F4 AB A7 2D  42 9D 3B 46 36 D4 83 B8  CD 1A 21 86 34 4F CB 65  FE 92 1D 50 C1 53 1F B3  DC 80 EC B2 44 E0 6D 38    7E 67 7F 98 F4 AB A7 2D  42 9D 3B 46 36 D4 83 B8  CD 1A 21 86 34 4F CB 65  FE 92 1D 50 C1 53 1F B3  DC 80 EC B2 44 E0 6D 38
39 50 2E 06 C8 8B 2B 02  A8 54 BD B5 CB A0 40 F0  72 21 18 6E D5 C8 AF 47  44 30 20 87 A0 6C F6 F3  E1 0B 32 6E 47 72 E9 74    39 50 2E 06 C8 8B 2B 02  A8 54 BD B5 CB A0 40 F0  72 21 18 6E D5 C8 AF 47  44 30 20 87 A0 6C F6 F3  E1 0B 32 6E 47 72 E9 74
E0 B6 FE 91 3C 5B 95 0C  47 F8 EE 1A 50 EC A8 31  AC C7 04 B9 12 C3 E9 E6  63 08 FA 5A CA A4 71 56  12 6D 21 50 2F 38 A6 77    E0 B6 FE 91 3C 5B D5 0C  47 F8 EE 1A 50 EC A8 31  AC C7 04 B9 12 C3 E9 E6  63 08 FA 5A CA A4 71 56  12 6D 21 50 2F 38 A6 77
3A 8E 7E 03 99 BA B8 6D  DF A1 9B B8 7B 07 56 B9  CB 42 3D C9 92 B6 F1 D8  23 E3 5E 1C B8 8D 76 C1  34 DD AF E4 94 68 3B 65    3A 8E 7E 03 99 BA B8 6D  DF A1 9B B8 7B 07 56 B9  CB 42 3D C9 92 B6 F1 D8  23 E3 5E 1C B8 8D 76 C1  34 DD AF E0 94 68 3B 65
1F 35 05 19 C0 F1 AD 8F  CB B9 98 B2 0A F0 C6 BF  BC CB 9C 51 C0 13 75 45  D0 7D 83 6E 94 17 2C 52  C6 07 22 F9 84 40 DD 4D    1F 35 05 19 C0 F1 AD 87  CB B9 98 B2 0A F0 C6 BF  BC CB 9C 59 C0 13 75 45  D0 7D 83 6E 94 17 2C 5A  C6 07 22 F9 84 40 DD 4D
7A 19 7B 49 06 B8 B2 07  A9 61 57 64 82 6E 37 A1  57 C4 30 BF 9B FB 04 ED  08 67 D1 52 64 27 7B E0  C6 A1 39 67 3C D5 8D CE    7A 19 7B 4D 06 B8 B6 07  A9 61 57 64 82 6E 37 A1  57 C4 34 BF 9B FB 04 ED  08 67 D1 52 64 27 73 E0  C6 A1 39 67 3C D5 8D CE
05 67 9F 3C 20 9D 4F 7D  F9 6F 5B 1E B8 5B 98 D0  0C 4D BE 5E 85 E1 42 5E  C7 DE AF EB 1F 62 34 17  47 94 E4 5A FC D7 F6 7F    05 67 9B 3C 20 9D 4F 7D  F9 6F 5B 1E B8 5B 90 D0  0C 4D BE 5E 85 E1 42 5E  C7 DE AB EB 1F 62 34 17  47 94 E4 5A FC D7 FE 7F
6B 1F 6A 5A F5 71 E5 EB  0E 2D 3D 7A 26 33 CD EF  3A 1F B8 38 C2 68 17 CC  6C 21 17 CA 6C 3A D4 64  4A 82 DF 2E 0B 9C 91 6A    6B 1F 6A 5A F5 71 E5 EB  0E 2D 39 7A 26 33 CD EF  3A 1F B8 38 C2 68 17 CC  6C 21 17 CA 6C 3A D4 64  4A 82 DF 2E 0B 9C 91 6A
6B 6A 57 F2 40 3A 37 A7  3C 25 48 49 89 26 EA 56  5D CD 0D 7C 52 CA 8F 33  C3 38 DD 44 99 91 9A EF  18 5C 0D B5 37 19 98 BD    6B 6A 57 F2 40 3A 37 A7  3C 25 48 49 89 26 EA 56  5D CD 0D 7C 52 CA 8F 33  C3 38 DD 44 99 91 9A EF  18 5C 0D B5 37 19 98 BD
F2 21 36 21 AE 95 A8 AF  95 6F 06 33 21 3A C4 07  71 FC 25 88 57 4D 6E F8  F6 CC 1B 25 66 11 DE CE  7A 9E A5 1D 03 B7 15 6D    F2 21 36 21 AE 95 A8 AF  95 6F 06 33 21 3A C4 07  71 FC 25 88 57 4D 6E D8  F6 CC 1B 25 66 11 DE CE  7A 9E A5 05 03 B7 15 6D
83 1A 8E FC AA 89 8E 5D  A9 66 A8 A8 31 C0 88 9E  37 CC 3E 1C 0A C2 10 F0  C0 BA 18 4B F3 89 E6 F1  76 70 D5 48 A8 F3 02 69    83 1A 8E FC AA 89 8E 5D  A9 66 A8 A8 31 C0 88 9E  37 CC 3E 3C 0A C2 10 F0  C0 BA 18 4B F3 89 E6 E1  76 70 D5 48 A8 F3 02 69
09 43 EB 67 C7 C8 F0 F1  2B 3F 93 03 45 CE 1D 50  06 B8 B6 42 E4 83 BF 20  88 46 10 9A FE 69 39 87  76 A0 73 38 DF B0 CE BF    09 43 EB 47 C7 C8 F0 F1  2B 3F 93 03 45 CE 1D 70  06 B8 A6 42 E4 83 BF 20  88 46 10 BA FE 69 29 87  76 A0 73 38 DF B0 CE AF
49 5B 30 F4 E4 E0 A2 DD  68 23 91 35 8E 1B 4C 83  EF 17 10 58 79 DE CB 6C  F2 68 C0 45 0F 59 77 7A  B7 32 84 37 4F 5D CC 2E    49 5B 20 F4 E4 E0 A2 DD  68 23 91 25 8E 1B 4C 83  EF 17 10 58 79 DE CB 6C  F2 68 C0 45 0F 59 77 7A  B7 32 84 37 4F 5D CC 2E
0E F5 DE C8 A5 A7 8B 68  C6 FC BA 79 7E 0E D2 91  5B CB A9 3C 28 15 99 31  BF C4 18 DB 21 F6 C7 3A  9B 8C EC 7F 93 37 F1 84    0E F5 DE C8 A5 A7 8B 68  C6 FC B2 79 7E 0E D2 91  5B CB A9 34 28 15 91 31  BF C4 18 DB 21 F6 C7 3A  9B 8C C8 7F 93 37 F1 84
43 58 91 F0 22 50 D3 3A  9C 3A 66 22 8F FA D3 A6  CC 68 CD 0A 78 C3 D5 26  27 B8 78 1B AD D8 D8 80  3A C9 DD B5 F8 AA BF F8    43 58 91 D8 22 50 F7 3A  9C 3A 66 22 8F FA D3 B2  CC 68 D9 0A 78 C3 D5 26  27 B8 78 0F AD D8 D0 80  3A C9 DD B5 F8 AA BF F8
A0 26 45 2B B5 9D 9D AA  11 D1 87 59 0C 3E 4E 5E  68 B5 4A 67 D3 45 E6 AD  49 72 2E 31 A4 25 32 0B  87 21 9F 52 E0 52 D1 E7    A0 26 4D 2B B5 9D 9D AA  11 D1 87 59 0C 3E 4A 5E  68 B5 4A 67 D3 45 E6 AD  49 72 2A 31 A4 25 32 0B  87 21 9F 52 E0 52 D5 E7
C8 38 82 8A DD B1 0B 8C  BF A1 E0 3A 5E 21 21 7A  CF 9F DF 22 83 6F 8F 48  40 C4 CC AD 99 CE FB E0  1A 3B 45 F0 09 4B A0 F4    C8 38 82 8A DD B1 0B 8C  BF A1 E4 3A 5E 21 21 7A  CF 9F DF 22 83 6F 8B 48  40 C4 CC AD 99 CE FB E0  1A 3B 4D F0 09 4B A0 F4
F5 94 42 02 5F F2 8C A9  86 81 B8 BA E0 73 09 88  D6 19 63 B9 42 73 3F 8E  0D 9A F2 CC CD 53 BE 4E  B7 60 35 E5 F1 C2 4F 81    F5 94 42 02 5F F2 8C A9  86 81 B8 BA E0 73 09 88  D6 19 63 B9 42 73 3F 8E  0D 9A F2 CC CD 53 BE 4E  B7 60 35 E5 F1 C2 4F 81
ED AD B7 AC 0E 83 78 52  5F 30 8A B7 32 A0 85 9F  69 B1 E4 8C FD DD EA D0  CE 5E 1B B5 5B 5C C8 24  49 7E 1B 24 B8 19 54 A1    ED AD B7 AC 0E 83 78 52  5F 30 8A B7 32 A0 85 9F  69 B1 E4 8C FD DD EA D0  CE 5E 1B B5 5B 5C C8 24  49 7E 1B 24 B8 19 54 A1
D1 6C 84 4D E5 2C 3D C8  99 8A 6F AF 4B 3A A1 CF  54 52 53 E8 61 A4 02 93  28 13 AB 05 77 0F CD 33  E9 B7 96 8C B1 C8 19 DF    D1 6C 84 4D E5 2C 3D C8  99 8A 6F AF 4B 3A A1 CF  54 52 53 E8 61 A4 02 93  28 13 AB 05 77 0F CD 33  E9 B7 96 8C B1 C8 19 DF
D2 8F C1 07 36 93 9C D4  A0 2B 95 6B 22 5D F8 56  1D 81 C9 7A C7 25 71 F6  7E E8 8C 1E 19 67 3D 68  3C 0D 25 75 0A 26 AA 55    D2 8F C1 27 36 93 9C D4  A0 2B 95 6B 22 5D F8 56  1D 81 E9 7A C7 25 71 F6  7E E8 8C 1E 19 67 1D 68  3C 0D 25 75 0A 26 AA 55
EC 6F 80 0E DD FE FA 4B  8B 95 42 1A A1 95 DA 61  36 5C 2E D1 6C CE FE 26  CA EB A0 E0 1A FC 05 BC  24 98 2A 75 6A C9 13 CE    EC 6F E0 0E DD FE FA 4B  8B 95 42 1A A1 95 4A 61  36 5C 2E D1 6C CE FE 26  CA EB F0 E0 1A FC 05 BC  24 98 2A 75 6A C9 13 CE
40 07 96 9B A9 22 78 EE  E9 5C D9 48 38 6E 4E C3  AF A9 61 E7 C9 B4 F4 36  7C 5C 4F 05 B2 E1 B8 CE  0E 81 CA 27 1A 1D C8 92    40 07 96 9B A9 22 78 EE  E9 5C D9 48 38 6E 4E C3  AF A9 61 E7 C9 B4 F4 36  7C 5C 4F 05 B2 E1 B8 CE  0E 81 C2 27 1A 1D C8 92
CC 69 0D 7C EA 00 E8 B6  96 64 45 94 6B 5E E7 33  A6 2A E9 BB DF 72 48 11  5C B4 94 BE B3 62 98 05  66 53 B0 F2 85 A5 9C 46    CC 69 0D 7C EA 00 F0 B6  96 64 45 94 6B 5E E7 33  A6 2A E1 BB DF 72 48 11  5C B4 94 BE B3 62 90 05  66 53 B0 F2 85 A5 9C 46
```

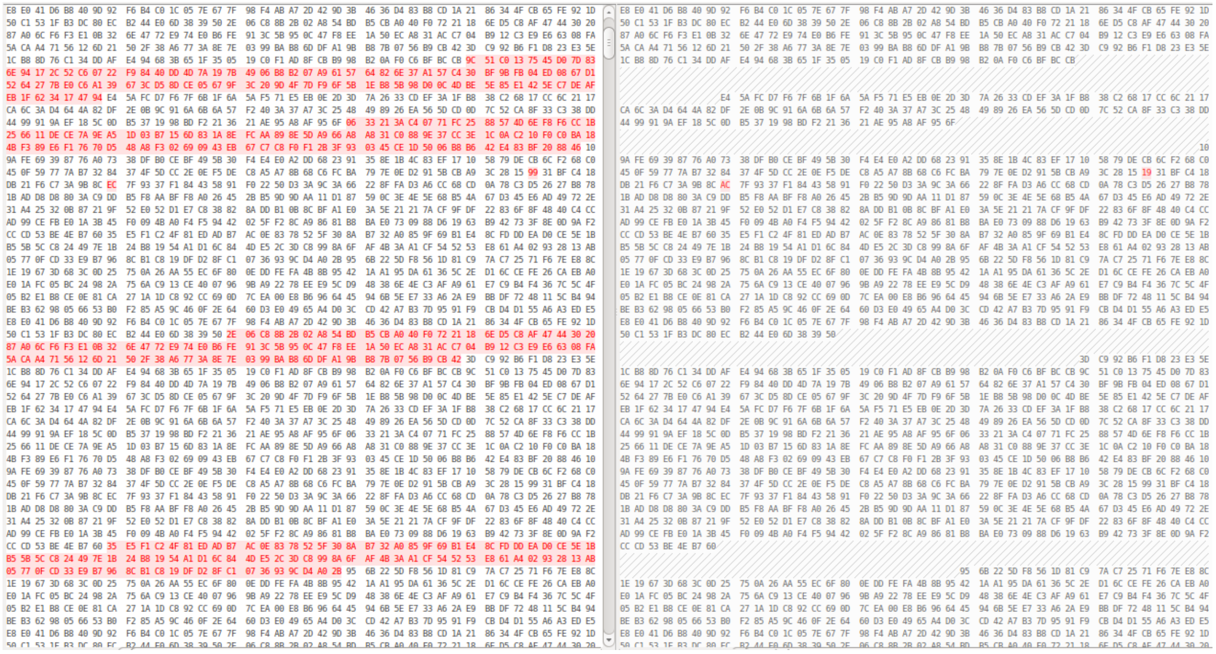
Figure C.3: Sent and Received Messages for the Case with $k1 = k2 = (1, -1, -1, 1, 1)$ in the Chamber



```
1F B3 DC 80 EC B2 44 E0  6D 38 39 50 2E 06 C8 8B  2B 02 A8 54 BD B5 CB A0  40 F0 72 21 18 6E D5 C8  AF 47 44 30 20 87 A0 6C
F6 F3 E1 0B 32 6E 47 72  E9 74 E0 B6 FE 91 3C 5B  95 0C 47 F8 EE 1A 50 EC  A8 31 AC C7 04 B9 12 C3  E9 E6 63 08 FA 5A CA A4
71 56 12 6D 21 50 2F 38  A6 77 3A 8E 7E 03 99 BA  BB 6D DF A1 9B B8 7B 07  56 B9 CB 42 3D C9 92 B6  F1 D8 23 E3 5E 1C BB 8D
76 C1 34 DD AF E4 94 6B  3B 65 1F 35 05 19 C0 F1  AD 8F CB B9 98 B2 0A F0  C6 BF BC CB 9C 51 C0 13  75 45 D0 7D 83 6E 94 17
2C 52 C6 07 22 F9 84 40  DD 4D 7A 19 7B 49 06 B8  B2 07 A9 61 57 64 82 6E  37 A1 57 C4 30 BF 9B FB  04 ED 08 67 D1 52 64 27
7B E0 C6 A1 39 67 3C D5  8D CE 05 67 9F 3C 20 9D  4F 7D F9 6F 5B 1E B8 5B  98 D0 0C 4D BE 5E 85 E1  42 5E C7 DE AF EB 1F 62
34 17 47 94 E4 5A FC D7  F6 7F 6B 1F 6A 5A F5 71  E5 EB 0E 2D 3D 7A 26 33  CD EF 3A 1F B8 38 C2 68  17 CC 6C 21 17 CA 6C 3A
D4 64 4A 82 DF 2E 0B 9C  91 6A 6B 6A 57 F2 40 3A  37 A7 3C 25 48 49 89 26  EA 56 5D CD 0D 7C 52 CA  8F 33 C3 38 DD 44 99 91
9A EF 18 5C 0D B5 37 19  98 BD F2 21 36 21 AE 95  A8 AF 95 6F 06 33 21 3A  C4 07 71 FC 25 88 57 4D  6E F8 F6 CC 1B 25 66 11
DE CE 7A 9E A5 1D 03 B7  15 6D 83 1A 8E FC AA 89  8E 5D A9 66 A8 A8 31 C0  88 9E 37 CC 3E 1C 0A C2  10 F0 C0 BA 18 4B F3 89
E6 F1 76 70 D5 48 A8 F3  02 69 09 43 EB 67 C7 C8  F0 F1 2B 3F 93 03 45 CE  1D 50 06 B8 B6 42 E4 83  BF 20 88 46 10 9A FE 69
39 87 76 A0 73 38 DF B0  CE BF 49 5B 30 F4 E4 E0  A2 DD 68 23 91 35 8E 1B  4C 83 EF 17 10 58 79 DE  CB 6C F2 68 C0 45 0F 59
77 7A B7 32 84 37 4F 5D  CC 2E 0E F5 DE C8 A5 A7  8B 68 C6 FC BA 79 7E 0E  D2 91 5B CB A9 3C 28 15  99 31 BF C4 18 DB 21 F6
C7 3A 9B 8C EC 7F 93 37  F1 84 43 58 91 F0 22 50  D3 3A 9C 3A 66 22 8F FA  D3 A6 CC 68 CD 0A 78 C3  D5 26 27 B8 78 1B AD D8
D8 80 3A C9 DD B5 F8 AA  BF F8 A0 26 45 2B B5 9D  9D AA 11 D1 87 59 0C 3E  4E 5E 68 B5 4A 67 D3 45  E6 AD 49 72 2E 31 A4 25
32 0B 87 21 9F 52 E0 52  D1 E7 C8 38 82 8A DD B1  0B 8C BF A1 E0 3A 5E 21  21 7A CF 9F DF 22 83 6F  8F 48 40 C4 CC AD 99 CE
FB E0 1A 3B 45 F0 09 4B  A0 F4 F5 94 42 02 5F F2  8C A9 86 81 B8 BA E0 73  09 88 D6 19 63 B9 42 73  3F 8E 0D 9A F2 CC CD 53
BE 4E B7 60 35 E5 F1 C2  4F 81 ED AD B7 AC 0E 83  78 52 5F 30 8A B7 32 A0  85 9F 69 B1 E4 8C FD DD  EA D0 CE 5E 1B B5 5B 5C
C8 24 49 7E 1B 24 B8 19  54 A1 D1 6C 84 4D E5 2C  3D C8 99 8A 6F AF 4B 3A  A1 CF 54 52 53 E8 61 A4  02 93 28 13 AB 05 77 0F
CD 33 E9 B7 96 8C B1 C8  19 DF D2 8F C1 07 36 93  9C D4 A0 2B 95 6B 22 5D  F8 56 1D 81 C9 7A C7 25  71 F6 7E E8 8C 1E 19 67
3D 68 3C 0D 25 75 0A 26  AA 55 EC 6F 80 0E DD FE  FA 4B 8B 95 42 1A A1 95  DA 61 36 5C 2E D1 6C CE  FE 26 CA EB A0 E0 1A FC
05 BC 24 9B 2A 75 6A C9  13 CE 40 07 96 9B A9 22  78 EE E9 5C D9 48 38 6E  4E C3 AF A9 61 E7 C9 B4  F4 36 7C 5C 4F 05 B2 E1
B8 CE 0E 81 CA 27 1A 1D  C8 92 CC 69 0D 7C EA 00  E8 B6 96 64 45 94 6B 5E  E7 33 A6 2A E9 BB DF 72  48 11 5C B4 94 BE B3 62
98 05 66 53 B0 F2 85 A5  9C 46 0F 2E 64 60 D3 E0  49 65 A4 D0 3C CD 42 A7  B3 7D 95 91 F9 CB D4 D1  55 A6 A3 ED E5 E8 E0 41
D6 B8 40 9D 92 F6 B4 C0  1C 05 7E 67 7F 98 F4 AB  A7 2D 42 9D 3B 46 36 D4  83 B8 CD 1A 21 86 34 4F  CB 65 FE 92 1D 50 C1 53
1F B3 DC 80 EC B2 44 E0  6D 38 39 50 2E 06 C8 8B  2B 02 A8 54 BD B5 CB A0  40 F0 72 21 18 6E D5 C8  AF 47 44 30 20 87 A0 6C
F6 F3 E1 0B 32 6E 47 72  E9 74 E0 B6 FE 91 3C 5B  95 0C 47 F8 EE 1A 50 EC  A8 31 AC C7 04 B9 12 C3  E9 E6 63 08 FA 5A CA A4
71 56 12 6D 21 50 2F 38  A6 77 3A 8E 7E 03 99 BA  BB 6D DF A1 9B B8 7B 07  56 B9 CB 42 3D C9 92 B6  F1 D8 23 E3 5E 1C BB 8D
76 C1 34 DD AF E4 94 6B  3B 65 1F 35 05 19 C0 F1  AD 8F CB B9 98 B2 0A F0  C6 BF BC CB 9C 51 C0 13  75 45 D0 7D 83 6E 94 17
2C 52 C6 07 22 F9 84 40  DD 4D 7A 19 7B 49 06 B8  B2 07 A9 61 57 64 82 6E  37 A1 57 C4 30 BF 9B FB  04 ED 08 67 D1 52 64 27
7B E0 C6 A1 39 67 3C D5  8D CE 05 67 9F 3C 20 9D  4F 7D F9 6F 5B 1E B8 5B  98 D0 0C 4D BE 5E 85 E1  42 5E C7 DE AF EB 1F 62
34 17 47 94 E4 5A FC D7  F6 7F 6B 1F 6A 5A F5 71  E5 EB 0E 2D 3D 7A 26 33  CD EF 3A 1F B8 38 C2 68  17 CC 6C 21 17 CA 6C 3A
D4 64 4A 82 DF 2E 0B 9C  91 6A 6B 6A 57 F2 40 3A  37 A7 3C 25 48 49 89 26  EA 56 5D CD 0D 7C 52 CA  8F 33 C3 38 DD 44 99 91
9A EF 18 5C 0D B5 37 19  98 BD F2 21 36 21 AE 95  A8 AF 95 6F 06 33 21 3A  C4 07 71 FC 25 88 57 4D  6E F8 F6 CC 1B 25 66 11
DE CE 7A 9E A5 1D 03 B7  15 6D 83 1A 8E FC AA 89  8E 5D A9 66 A8 A8 31 C0  88 9E 37 CC 3E 1C 0A C2  10 F0 C0 BA 18 4B F3 89
E6 F1 76 70 D5 48 A8 F3  02 69 09 43 EB 67 C7 C8  F0 F1 2B 3F 93 03 45 CE  1D 50 06 B8 B6 42 E4 83  BF 20 88 46 10 9A FE 69
39 87 76 A0 73 38 DF B0  CE BF 49 5B 30 F4 E4 E0  A2 DD 68 23 91 35 8E 1B  4C 83 EF 17 10 58 79 DE  CB 6C F2 68 C0 45 0F 59
77 7A B7 32 84 37 4F 5D  CC 2E 0E F5 DE C8 A5 A7  8B 68 C6 FC BA 79 7E 0E  D2 91 5B CB A9 3C 28 15  99 31 BF C4 18 DB 21 F6
C7 3A 9B 8C EC 7F 93 37  F1 84 43 58 91 F0 22 50  D3 3A 9C 3A 66 22 8F FA  D3 A6 CC 68 CD 0A 78 C3  D5 26 27 B8 78 1B AD D8
D8 80 3A C9 DD B5 F8 AA  BF F8 A0 26 45 2B B5 9D  9D AA 11 D1 87 59 0C 3E  4E 5E 68 B5 4A 67 D3 45  E6 AD 49 72 2E 31 A4 25
32 0B 87 21 9F 52 E0 52  D1 E7 C8 38 82 8A DD B1  0B 8C BF A1 E0 3A 5E 21  21 7A CF 9F DF 22 83 6F  8F 48 40 C4 CC AD 99 CE
FB E0 1A 3B 45 F0 09 4B  A0 F4 F5 94 42 02 5F F2  8C A9 86 81 B8 BA E0 73  09 88 D6 19 63 B9 42 73  3F 8E 0D 9A F2 CC CD 53
BE 4E B7 60 35 E5 F1 C2  4F                   81  ED AD B7 AC 0E 83 78 52  5F 30 8A B7 32 A0 85 9F  69 B1 E4 8C FD DD EA D0
CE                   5E  1B B5 5B                       5C C8 24
49 7E 1B 24 B8 19 54 A1                       D1  6C 84 4D    E5 2C 3D C8                                    99 8A 6F AF 4B 3A
A1 CF 54 52 53 E8 61 A4  02 93 28 13 AB 05 77 0F  CD 33 E9 B7 96 8C B1 C8  19 DF D2 8F C1 07 36 93  9C D4 A0 2B 95 6B 22 5D
F8 56 1D 81 C9 7A C7 25  71 F6 7E E8 8C 1E 19 67  3D 68 3C 0D 25 75 0A 26  AA 55 EC 6F 80 0E DD FE  FA 4B 8B 95 42 1A A1 95
DA 61 36 5C 2E D1 6C CE  FE 26 CA EB A0 E0 1A FC  05 BC 24 9B 2A 75 6A C9  13 CE 40 07 96 9B A9 22  78 EE E9 5C D9 48 38 6E
4E C3 AF A9 61 E7 C9 B4  F4 36 7C 5C 4F 05 B2 E1  B8 CE 0E 81 CA 27 1A 1D  C8 92 CC 69 0D 7C EA 00  E8 B6 96 64 45 94 6B 5E
E7 33 A6 2A E9 BB DF 72  48 11 5C B4 94 BE B3 62  98 05 66 53 B0 F2 85 A5  9C 46 0F 2E 64 60 D3 E0  49 65 A4 D0 3C CD 42 A7
B3 7D 95 91 F9 CB D4 D1  55 A6 A3 ED E5 E8 E0 41  D6 B8 40 9D 92 F6 B4 C0  1C 05 7E 67 7F 98 F4 AB  A7 2D 42 9D 3B 46 36 D4
83 B8 CD 1A 21 86 34 4F  CB 65 FE 92 1D 50 C1 53  1F B3 DC 80 EC B2 44 E0  6D 38 39 50 2E 06 C8 8B  2B 02 A8 54 BD B5 CB A0
```

```
1F B3 DC 80 EC B2 44 E0  6D 38 39 50 2E 06 C8 8B  2B 02 A8 54 BD B5 CB A0  40 F0 72 21 18 6E D5 C8  AF 47 44 30 20 87 A0 6C
F6 F3 E1 0B 32 6E 47 72  E9 74 E0 B6 FE 91 3C 5B  95 0C 47 F8 EE 1A 50 EC  A8 31 AC C7 04 B9 12 C3  E9 E6 63 08 FA 5A CA A4
71 56 12 6D 21 50 2F 38  A6 77




      4A 82 DF 2E 0B 9C  91 6A 6B 6A 57 F2 40 3A  37 A7 3C 25 48 49 89 26  EA 56 5D CD 0D 7C 52 CA  8F 33 C3 38 DD 44 99 91
9A EF 18 5C 0D B5 37 19  98 BD F2 21 36 21 AE 95  A8 AF 95 6F 06 33 21 3A  C4 07 71 FC 25 88 57 4D  6E F8 F6 CC 1B 25 66 11
DE CE 7A 9E A5 1D 03 B7  15 6D 83 1A 8E FC AA 89  8E 5D




                               A0 26 45 2B B5 9D  9D AA 11 D1 87 59 0C 3E  4E 5E 68 B5 4A 67 D3 45  E6 AD 49 72 2E 31 A4 25
32 0B 87 21 9F 52 E0 52  D1 E7 C8 38 82 8A DD B1  0B 8C BF A1 E0 3A 5E 21  21 7A CF 9F DF 22 83 6F  8F 48 40 C4 CC AD 99 CE
FB E0 1A 3B 45 F0 09 4B  A0 F4 F5 94 42 02 5F F2  8C A9 86 81 B8 BA E0 73  09 88




                                                        E9 5C D9 48 38 6E  4E C3 AF A9 61 E7 C9 B4  F4 36 7C 5C 4F 05 B2 E1
B8 CE 0E 81 CA 27 1A 1D  C8 92 CC 69 0D 7C EA 00  E8 B6 96 64 45 94 6B 5E  E7 33 A6 2A E9 BB DF 72  48 11 5C B4 94 BE B3 62
98 05 66 53 B0 F2 85 A5  9C 46 0F 2E 64 60 D3 E0  49 65 A4 D0 3C CD 42 A7  B3 7D 95 91 F9 CB D4 D1  55 A6




                                                                                 BC CB 9C 51 C0 13  75 45 D0 7D 83 6E 94 17
2C 52 C6 07 22 F9 84 40  DD 4D 7A 19 7B 49 06 B8  B2 07 A9 61 57 64 82 6E  37 A1 57 C4 30 BF 9B FB  04 ED 08 67 D1 52 64 27
7B E0 C6 A1 39 67 3C D5  8D CE 05 67 9E 3C 20 9D  4F 7D F9 6F 5B 1E B8 5B  98 D0 0C 4D BE 5E 85 E1  42 5E C7 DE AF EB 1F 62
34




                                                                                    17

                                                                                    68
               B5                                                                      4A 67 D3 45  E6 AD 49 72 2E 31 A4 25
32 0B 87 21 9F 52 E0 52  D1 E7 C8 38 82 8A DD F1  0B 8C BF A1 E0 3A 5E 21  21 7A CF 9F DF 22 83 6F  8F 48 40 C4 CC AD 99 CE
FB E0 1A 3B 45 F0 09 4B  A0 F4 F5 94 42 02 5F F2  8C A9 86 81 B8 BA E0 73  09 88 D6 19 63 B9 42 73  3F 8E 0D 9A F2 CC CD 53
BE 4E 7C 5C              4F 05 B2 E1 B8 CE 0E 81  CA 27 1A 1D C8 92 CC                              69 0D 7C          EA 00
E8 B6 96 64 45 94 6B 5E  E7 33 A6 2A E9 BB DF 72  48 11 5C B4 94 BE B3 62  98 05 66 53 B0 F2 85 A5  9C 46 0F 2E 64 60 D3 E0
49 65 A4 D0 3C CD 42 A7  B3 7D 95 91 F9 CB D4 D1  55 A6 A3 ED E5 E8 E0 41  D6 B8 40 9D 92 F6 B4 C0  1C 05 99 8A 6F AF 4B 3A
A1 CF 54 52 53 E8 61 A4  02 93 28 13 AB 05 77 0F  CD 33 E9 B7 96 8C B1 C8  19 DF D2 8F C1 07 36 93  9C D4 A0 2B 95 6B 22 5D
F8 56 1D 81 C9 7A C7 25  71 F6 7E E8 8C 1E 19 67  3D 68 3C 0D 25 75 0A 26  AA 55 EC 6F 80 0E DD FE  FA 4B 8B 95 42 1A A1 95
DA 61 36 5C 2E D1 6C CE  FE 26
```

Figure C.4: Sent and Received Messages for the Case with $k1 = k2 = (1, -1, 1, 1, 1, -1)$ in the Chamber



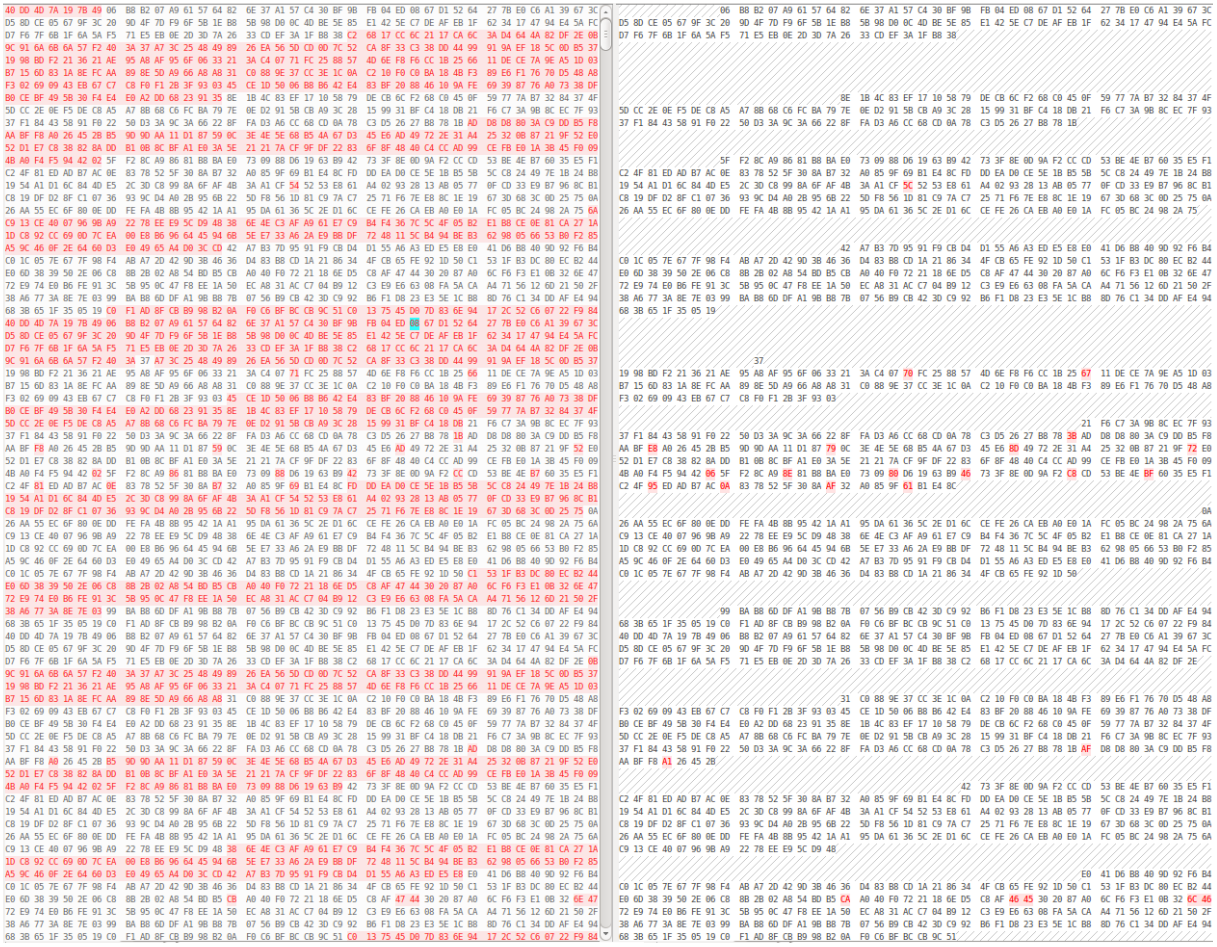
```
E8 E0 41 D6 B8 40 9D 92  F6 B4 C0 1C 05 7E 67 7F  98 F4 AB A7 2D 42 9D 3B  46 36 D4 83 B8 CD 1A 21  86 34 4F CB 65 FE 92 1D
50 C1 53 1F B3 DC 80 EC  B2 44 E0 6D 38 39 50 2E  06 C8 8B 2B 02 A8 54 BD  B5 CB A0 40 F0 72 21 18  6E D5 C8 AF 47 44 30 20
87 A0 6C F6 F3 E1 0B 32  6E 47 72 E9 74 E0 B6 FE  91 3C 5B 95 0C 47 F8 EE  1A 50 EC A8 31 AC C7 04  B9 12 C3 E9 E6 63 08 FA
5A CA A4 71 56 12 6D 21  50 2F 38 A6 77 3A 8E 7E  03 99 BA B8 6D DF A1 9B  B8 7B 07 56 B9 CB 42 3D  C9 92 B6 F1 D8 23 E3 5E
1C B8 8D 76 C1 34 DD AF  E4 94 68 3B 65 1F 35 05  19 C0 F1 AD 8F CB B9 98  B2 0A F0 C6 BF BC CB 9C  51 C0 13 75 45 D0 7D 83
6E 94 17 2C 52 C6 07 22  F9 84 40 DD 4D 7A 19 7B  49 06 B8 B2 07 A9 61 57  64 82 6E 37 A1 57 C4 30  BF 9B FB 04 ED 08 67 D1
52 64 27 7B E0 C6 A1 39  67 3C D5 8D CE 05 67 9F  3C 20 9D 4F 7D F9 6F 5B  1E B8 5B 98 D0 0C 4D BE  5E 85 E1 42 5E C7 DE AF
EB 1F 62 34 17 47 94 E4  5A FC D7 F6 7F 6B 1F 6A  5A F5 71 E5 EB 0E 2D 3D  7A 26 33 CD EF 3A 1F B8  38 C2 68 17 CC 6C 21 17
CA 6C 3A D4 64 4A 82 DF  2E 0B 9C 91 6A 6B 6A 57  F2 40 3A 37 A7 3C 25 48  49 89 26 EA 56 5D CD 0D  7C 52 CA 8F 33 C3 38 DD
44 99 91 9A EF 18 5C 0D  B5 37 19 98 BD F2 21 36  21 AE 95 A8 AF 95 6F 06  33 21 3A C4 07 71 FC 25  88 57 4D 6E F8 F6 CC 1B
25 66 11 DE CE 7A 9E A5  1D 03 B7 15 6D 83 1A 8E  FC AA 89 8E 5D A9 66 A8  A8 31 C0 88 9E 37 CC 3E  1C 0A C2 10 F0 C0 BA 18
4B F3 89 E6 F1 76 70 D5  48 A8 F3 02 69 09 43 EB  67 C7 C8 F0 F1 2B 3F 93  03 45 CE 1D 50 06 B8 B6  42 E4 83 BF 20 88 46 10
9A FE 69 39 87 76 A0 73  38 DF B0 CE BF 49 5B 30  F4 E4 E0 A2 DD 68 23 91  35 8E 1B 4C 83 EF 17 10  58 79 DE CB 6C F2 68 C0
45 0F 59 77 7A B7 32 84  37 4F 5D CC 2E 0E F5 DE  C8 A5 A7 8B 68 C6 FC BA  79 7E 0E D2 91 5B CB A9  3C 28 15 99 31 BF C4 18
DB 21 F6 C7 3A 9B 8C EC  7F 93 37 F1 84 43 58 91  F0 22 50 D3 3A 9C 3A 66  22 8F FA D3 A6 CC 68 CD  0A 78 C3 D5 26 27 B8 78
1B AD D8 D8 80 3A C9 DD  B5 F8 AA BF F8 A0 26 45  2B B5 9D 9D AA 11 D1 87  59 0C 3E 4E 5E 68 B5 4A  67 D3 45 E6 AD 49 72 2E
31 A4 25 32 0B 87 21 9F  52 E0 52 D1 E7 C8 38 82  8A DD B1 0B 8C BF A1 E0  3A 5E 21 21 7A CF 9F DF  22 83 6F 8F 48 40 C4 CC
AD 99 CE FB E0 1A 3B 45  F0 09 4B A0 F4 F5 94 42  02 5F F2 8C A9 86 81 B8  BA E0 73 09 88 D6 19 63  B9 42 73 3F 8E 0D 9A F2
CC CD 53 BE 4E B7 60 35  E5 F1 C2 4F 81 ED AD B7  AC 0E 83 78 52 5F 30 8A  B7 32 A0 85 9F 69 B1 E4  8C FD DD EA D0 CE 5E 1B
B5 5B 5C C8 24 49 7E 1B  24 B8 19 54 A1 D1 6C 84  4D E5 2C 3D C8 99 8A 6F  AF 4B 3A A1 CF 54 52 53  E8 61 A4 02 93 28 13 AB
05 77 0F CD 33 E9 B7 96  8C B1 C8 19 DF D2 8F C1  07 36 93 9C D4 A0 2B 95  6B 22 5D F8 56 1D 81 C9  7A C7 25 71 F6 7E E8 8C
1E 19 67 3D 68 3C 0D 25  75 0A 26 AA 55 EC 6F 80  0E DD FE FA 4B 8B 95 42  1A A1 95 DA 61 36 5C 2E  D1 6C CE FE 26 CA EB A0
E0 1A FC 05 BC 24 98 2A  75 6A C9 13 CE 40 07 96  9B A9 22 78 EE E9 5C D9  48 38 6E 4E C3 AF A9 61  E7 C9 B4 F4 36 7C 5C 4F
05 B2 E1 B8 CE 0E 81 CA  27 1A 1D C8 92 CC 69 0D  7C EA 00 E8 B6 96 64 45  94 6B 5E E7 33 A6 2A E9  BB DF 72 48 11 5C B4 94
BE B3 62 98 05 66 53 B0  F2 85 A5 9C 46 0F 2E 64  60 D3 E0 49 65 A4 D0 3C  CD 42 A7 B3 7D 95 91 F9  CB D4 D1 55 A6 A3 ED E5
E8 E0 41 D6 B8 40 9D 92  F6 B4 C0 1C 05 7E 67 7F  98 F4 AB A7 2D 42 9D 3B  46 36 D4 83 B8 CD 1A 21  86 34 4F CB 65 FE 92 1D
50 C1 53 1F B3 DC 80 EC  B2 44 E0 6D 38 39 50 2E  06 C8 8B 2B 02 A8 54 BD  B5 CB A0 40 F0 72 21 18  6E D5 C8 AF 47 44 30 20
87 A0 6C F6 F3 E1 0B 32  6E 47 72 E9 74 E0 B6 FE  91 3C 5B 95 0C 47 F8 EE  1A 50 EC A8 31 AC C7 04  B9 12 C3 E9 E6 63 08 FA
5A CA A4 71 56 12 6D 21  50 2F 38 A6 77 3A 8E 7E  03 99 BA B8 6D DF A1 9B  B8 7B 07 56 B9 CB 42 3D  C9 92 B6 F1 D8 23 E3 5E
1C B8 8D 76 C1 34 DD AF  E4 94 68 3B 65 1F 35 05  19 C0 F1 AD 8F CB B9 98  B2 0A F0 C6 BF BC CB 9C  51 C0 13 75 45 D0 7D 83
6E 94 17 2C 52 C6 07 22  F9 84 40 DD 4D 7A 19 7B  49 06 B8 B2 07 A9 61 57  64 82 6E 37 A1 57 C4 30  BF 9B FB 04 ED 08 67 D1
52 64 27 7B E0 C6 A1 39  67 3C D5 8D CE 05 67 9F  3C 20 9D 4F 7D F9 6F 5B  1E B8 5B 98 D0 0C 4D BE  5E 85 E1 42 5E C7 DE AF
EB 1F 62 34 17 47 94 E4  5A FC D7 F6 7F 6B 1F 6A  5A F5 71 E5 EB 0E 2D 3D  7A 26 33 CD EF 3A 1F B8  38 C2 68 17 CC 6C 21 17
CA 6C 3A D4 64 4A 82 DF  2E 0B 9C 91 6A 6B 6A 57  F2 40 3A 37 A7 3C 25 48  49 89 26 EA 56 5D CD 0D  7C 52 CA 8F 33 C3 38 DD
44 99 91 9A EF 18 5C 0D  B5 37 19 98 BD F2 21 36  21 AE 95 A8 AF 95 6F 06  33 21 3A C4 07 71 FC 25  88 57 4D 6E F8 F6 CC 1B
25 66 11 DE CE 7A 9E A5  1D 03 B7 15 6D 83 1A 8E  FC AA 89 8E 5D A9 66 A8  A8 31 C0 88 9E 37 CC 3E  1C 0A C2 10 F0 C0 BA 18
4B F3 89 E6 F1 76 70 D5  48 A8 F3 02 69 09 43 EB  67 C7 C8 F0 F1 2B 3F 93  03 45 CE 1D 50 06 B8 B6  42 E4 83 BF 20 88 46 10
9A FE 69 39 87 76 A0 73  38 DF B0 CE BF 49 5B 30  F4 E4 E0 A2 DD 68 23 91  35 8E 1B 4C 83 EF 17 10  58 79 DE CB 6C F2 68 C0
45 0F 59 77 7A B7 32 84  37 4F 5D CC 2E 0E F5 DE  C8 A5 A7 8B 68 C6 FC BA  79 7E 0E D2 91 5B CB A9  3C 28 15 99 31 BF C4 18
DB 21 F6 C7 3A 9B 8C EC  7F 93 37 F1 84 43 58 91  F0 22 50 D3 3A 9C 3A 66  22 8F FA D3 A6 CC 68 CD  0A 78 C3 D5 26 27 B8 78
1B AD D8 D8 80 3A C9 DD  B5 F8 AA BF F8 A0 26 45  2B B5 9D 9D AA 11 D1 87  59 0C 3E 4E 5E 68 B5 4A  67 D3 45 E6 AD 49 72 2E
31 A4 25 32 0B 87 21 9F  52 E0 52 D1 E7 C8 38 82  8A DD B1 0B 8C BF A1 E0  3A 5E 21 21 7A CF 9F DF  22 83 6F 8F 48 40 C4 CC
AD 99 CE FB E0 1A 3B 45  F0 09 4B A0 F4 F5 94 42  02 5F F2 8C A9 86 81 B8  BA E0 73 09 88 D6 19 63  B9 42 73 3F 8E 0D 9A F2
CC CD 53 BE 4E B7 60 35  E5 F1 C2 4F 81 ED AD B7  AC 0E 83 78 52 5F 30 8A  B7 32 A0 85 9F 69 B1 E4  8C FD DD EA D0 CE 5E 1B
B5 5B 5C C8 24 49 7E 1B  24 B8 19 54 A1 D1 6C 84  4D E5 2C 3D C8 99 8A 6F  AF 4B 3A A1 CF 54 52 53  E8 61 A4 02 93 28 13 AB
05 77 0F CD 33 E9 B7 96  8C B1 C8 19 DF D2 8F C1  07 36 93 9C D4 A0 2B 95  6B 22 5D F8 56 1D 81 C9  7A C7 25 71 F6 7E E8 8C
1E 19 67 3D 68 3C 0D 25  75 0A 26 AA 55 EC 6F 80  0E DD FE FA 4B 8B 95 42  1A A1 95 DA 61 36 5C 2E  D1 6C CE FE 26 CA EB A0
E0 1A FC 05 BC 24 98 2A  75 6A C9 13 CE 40 07 96  9B A9 22 78 EE E9 5C D9  48 38 6E 4E C3 AF A9 61  E7 C9 B4 F4 36 7C 5C 4F
05 B2 E1 B8 CE 0E 81 CA  27 1A 1D C8 92 CC 69 0D  7C EA 00 E8 B6 96 64 45  94 6B 5E E7 33 A6 2A E9  BB DF 72 48 11 5C B4 94
BE B3 62 98 05 66 53 B0  F2 85 A5 9C 46 0F 2E 64  60 D3 E0 49 65 A4 D0 3C  CD 42 A7 B3 7D 95 91 F9  CB D4 D1 55 A6 A3 ED E5
E8 E0 41 D6 B8 40 9D 92  F6 B4 C0 1C 05 7E 67 7F  98 F4 AB A7 2D 42 9D 3B  46 36 D4 83 B8 CD 1A 21  86 34 4F CB 65 FE 92 1D
50 C1 53 1F B3 DC 80 EC  B2 44 E0 6D 38 39 50 2E  06 C8 8B 2B 02 A8 54 BD  B5 CB A0 40 F0 72 21 18  6E D5 C8 AF 47 44 30 20
```

```
E8 E0 41 D6 B8 40 9D 92  F6 B4 C0 1C 05 7E 67 7F  98 F4 AB A7 2D 42 9D 3B  46 36 D4 83 B8 CD 1A 21  86 34 4F CB 65 FE 92 1D
50 C1 53 1F B3 DC 80 EC  B2 44 E0 6D 38 39 50 2E  06 C8 8B 2B 02 A8 54 BD  B5 CB A0 40 F0 72 21 18  6E D5 C8 AF 47 44 30 20
87 A0 6C F6 F3 E1 0B 32  6E 47 72 E9 74 E0 B6 FE  91 3C 5B 95 0C 47 F8 EE  1A 50 EC A8 31 AC C7 04  B9 12 C3 E9 E6 63 08 FA
5A CA A4 71 56 12 6D 21  50 2F 38 A6 77 3A 8E 7E  03 99 BA B8 6D DF A1 9B  B8 7B 07 56 B9 CB 42 3D  C9 92 B6 F1 D8 23 E3 5E
1C B8 8D 76 C1 34 DD AF  E4 94 68 3B 65 1F 35 05  19 C0 F1 AD 8F CB B9 98  B2 0A F0 C6 BF BC CB


                     E4  5A FC D7 F6 7F 6B 1F 6A  5A F5 71 E5 EB 0E 2D 3D  7A 26 33 CD EF 3A 1F B8  38 C2 68 17 CC 6C 21 17
CA 6C 3A D4 64 4A 82 DF  2E 0B 9C 91 6A 6B 6A 57  F2 40 3A 37 A7 3C 25 48  49 89 26 EA 56 5D CD 0D  7C 52 CA 8F 33 C3 38 DD
44 99 91 9A EF 18 5C 0D  B5 37 19 98 BD F2 21 36  21 AE 95 A8 AF 95 6F

                                                                                                                         10
9A FE 69 39 87 76 A0 73  38 DF B0 CE BF 49 5B 30  F4 E4 E0 A2 DD 68 23 91  35 8E 1B 4C 83 EF 17 10  58 79 DE CB 6C F2 68 C0
45 0F 59 77 7A B7 32 84  37 4F 5D CC 2E 0E F5 DE  C8 A5 A7 8B 68 C6 FC BA  79 7E 0E D2 91 5B CB A9  3C 28 15 19 31 BF C4 18
DB 21 F6 C7 3A 9B 8C AC  7F 93 37 F1 84 43 58 91  F0 22 50 D3 3A 9C 3A 66  22 8F FA D3 A6 CC 68 CD  0A 78 C3 D5 26 27 B8 78
1B AD D8 D8 80 3A C9 DD  B5 F8 AA BF F8 A0 26 45  2B B5 9D 9D AA 11 D1 87  59 0C 3E 4E 5E 68 B5 4A  67 D3 45 E6 AD 49 72 2E
31 A4 25 32 0B 87 21 9F  52 E0 52 D1 E7 C8 38 82  8A DD B1 0B 8C BF A1 E0  3A 5E 21 21 7A CF 9F DF  22 83 6F 8F 48 40 C4 CC
AD 99 CE FB E0 1A 3B 45  F0 09 4B A0 F4 F5 94 42  02 5F F2 8C A9 86 81 B8  BA E0 73 09 88 D6 19 63  B9 42 73 3F 8E 0D 9A F2
CC CD 53 BE 4E B7 60 35  E5 F1 C2 4F 81 ED AD B7  AC 0E 83 78 52 5F 30 8A  B7 32 A0 85 9F 69 B1 E4  8C FD DD EA D0 CE 5E 1B
B5 5B 5C C8 24 49 7E 1B  24 B8 19 54 A1 D1 6C 84  4D E5 2C 3D C8 99 8A 6F  AF 4B 3A A1 CF 54 52 53  E8 61 A4 02 93 28 13 AB
05 77 0F CD 33 E9 B7 96  8C B1 C8 19 DF D2 8F C1  07 36 93 9C D4 A0 2B 95  6B 22 5D F8 56 1D 81 C9  7A C7 25 71 F6 7E E8 8C
1E 19 67 3D 68 3C 0D 25  75 0A 26 AA 55 EC 6F 80  0E DD FE FA 4B 8B 95 42  1A A1 95 DA 61 36 5C 2E  D1 6C CE FE 26 CA EB A0
E0 1A FC 05 BC 24 98 2A  75 6A C9 13 CE 40 07 96  9B A9 22 78 EE E9 5C D9  48 38 6E 4E C3 AF A9 61  E7 C9 B4 F4 36 7C 5C 4F
05 B2 E1 B8 CE 0E 81 CA  27 1A 1D C8 92 CC 69 0D  7C EA 00 E8 B6 96 64 45  94 6B 5E E7 33 A6 2A E9  BB DF 72 48 11 5C B4 94
BE B3 62 98 05 66 53 B0  F2 85 A5 9C 46 0F 2E 64  60 D3 E0 49 65 A4 D0 3C  CD 42 A7 B3 7D 95 91 F9  CB D4 D1 55 A6 A3 ED E5
E8 E0 41 D6 B8 40 9D 92  F6 B4 C0 1C 05 7E 67 7F  98 F4 AB A7 2D 42 9D 3B  46 36 D4 83 B8 CD 1A 21  86 34 4F CB 65 FE 92 1D
50 C1 53 1F B3 DC 80 EC  B2 44 E0 6D 38 39 50

                                                                                                3D  C9 92 B6 F1 D8 23 E3 5E
1C B8 8D 76 C1 34 DD AF  E4 94 68 3B 65 1F 35 05  19 C0 F1 AD 8F CB B9 98  B2 0A F0 C6 BF BC CB 9C  51 C0 13 75 45 D0 7D 83
6E 94 17 2C 52 C6 07 22  F9 84 40 DD 4D 7A 19 7B  49 06 B8 B2 07 A9 61 57  64 82 6E 37 A1 57 C4 30  BF 9B FB 04 ED 08 67 D1
52 64 27 7B E0 C6 A1 39  67 3C D5 8D CE 05 67 9F  3C 20 9D 4F 7D F9 6F 5B  1E B8 5B 98 D0 0C 4D BE  5E 85 E1 42 5E C7 DE AF
EB 1F 62 34 17 47 94 E4  5A FC D7 F6 7F 6B 1F 6A  5A F5 71 E5 EB 0E 2D 3D  7A 26 33 CD EF 3A 1F B8  38 C2 68 17 CC 6C 21 17
CA 6C 3A D4 64 4A 82 DF  2E 0B 9C 91 6A 6B 6A 57  F2 40 3A 37 A7 3C 25 48  49 89 26 EA 56 5D CD 0D  7C 52 CA 8F 33 C3 38 DD
44 99 91 9A EF 18 5C 0D  B5 37 19 98 BD F2 21 36  21 AE 95 A8 AF 95 6F 06  33 21 3A C4 07 71 FC 25  88 57 4D 6E F8 F6 CC 1B
25 66 11 DE CE 7A 9E A5  1D 03 B7 15 6D 83 1A 8E  FC AA 89 8E 5D A9 66 A8  A8 31 C0 88 9E 37 CC 3E  1C 0A C2 10 F0 C0 BA 18
4B F3 89 E6 F1 76 70 D5  48 A8 F3 02 69 09 43 EB  67 C7 C8 F0 F1 2B 3F 93  03 45 CE 1D 50 06 B8 B6  42 E4 83 BF 20 88 46 10
9A FE 69 39 87 76 A0 73  38 DF B0 CE BF 49 5B 30  F4 E4 E0 A2 DD 68 23 91  35 8E 1B 4C 83 EF 17 10  58 79 DE CB 6C F2 68 C0
45 0F 59 77 7A B7 32 84  37 4F 5D CC 2E 0E F5 DE  C8 A5 A7 8B 68 C6 FC BA  79 7E 0E D2 91 5B CB A9  3C 28 15 99 31 BF C4 18
DB 21 F6 C7 3A 9B 8C EC  7F 93 37 F1 84 43 58 91  F0 22 50 D3 3A 9C 3A 66  22 8F FA D3 A6 CC 68 CD  0A 78 C3 D5 26 27 B8 78
1B AD D8 D8 80 3A C9 DD  B5 F8 AA BF F8 A0 26 45  2B B5 9D 9D AA 11 D1 87  59 0C 3E 4E 5E 68 B5 4A  67 D3 45 E6 AD 49 72 2E
31 A4 25 32 0B 87 21 9F  52 E0 52 D1 E7 C8 38 82  8A DD B1 0B 8C BF A1 E0  3A 5E 21 21 7A CF 9F DF  22 83 6F 8F 48 40 C4 CC
AD 99 CE FB E0 1A 3B 45  F0 09 4B A0 F4 F5 94 42  02 5F F2 8C A9 86 81 B8  BA E0 73 09 88 D6 19 63  B9 42 73 3F 8E 0D 9A F2
CC CD 53 BE 4E B7 60

                                                                       95  6B 22 5D F8 56 1D 81 C9  7A C7 25 71 F6 7E E8 8C
1E 19 67 3D 68 3C 0D 25  75 0A 26 AA 55 EC 6F 80  0E DD FE FA 4B 8B 95 42  1A A1 95 DA 61 36 5C 2E  D1 6C CE FE 26 CA EB A0
E0 1A FC 05 BC 24 98 2A  75 6A C9 13 CE 40 07 96  9B A9 22 78 EE E9 5C D9  48 38 6E 4E C3 AF A9 61  E7 C9 B4 F4 36 7C 5C 4F
05 B2 E1 B8 CE 0E 81 CA  27 1A 1D C8 92 CC 69 0D  7C EA 00 E8 B6 96 64 45  94 6B 5E E7 33 A6 2A E9  BB DF 72 48 11 5C B4 94
BE B3 62 98 05 66 53 B0  F2 85 A5 9C 46 0F 2E 64  60 D3 E0 49 65 A4 D0 3C  CD 42 A7 B3 7D 95 91 F9  CB D4 D1 55 A6 A3 ED E5
E8 E0 41 D6 B8 40 9D 92  F6 B4 C0 1C 05 7E 67 7F  98 F4 AB A7 2D 42 9D 3B  46 36 D4 83 B8 CD 1A 21  86 34 4F CB 65 FE 92 1D
50 C1 53 1F B3 DC 80 EC  B2 44 E0 6D 38 39 50 2E  06 C8 8B 2B 02 A8 54 BD  B5 CB A0 40 F0 72 21 18  6E D5 C8 AF 47 44 30 20
```

Figure C.5: Sent and Received Messages for the Case with $k1 = k2 = (1, -1, 1, 1, 1, -1, -1)$ in the Chamber

# Appendix D

# Fragments of Sent and Received Messages for the Implementation in Laboratory



```
40 DD 4D 7A 19 7B 49 06  B8 B2 07 A9 61 57 64 82  6E 37 A1 57 C4 30 BF 9B  FB 04 ED 08 67 D1 52 64  27 7B E0 C6 A1 39 67 3C
D5 8D CE 05 67 9F 3C 20  9D 4F 7D F9 6F 5B 1E B8  5B 98 D0 0C 4D BE 5E 85  E1 42 5E C7 DE AF EB 1F  62 34 17 47 94 E4 5A FC
D7 F6 7F 6B 1F 6A 5A F5  71 E5 EB 0E 2D 3D 7A 26  33 CD EF 3A 1F B8 38 C2  68 17 CC 6C 21 17 CA 6C  3A D4 64 4A 82 DF 2E 0B
9C 91 6A 6B 6A 57 F2 40  3A 37 A7 3C 25 48 49 89  26 EA 56 5D CD 0D 7C 52  CA 8F 33 C3 38 DD 44 99  91 9A EF 18 5C 0D B5 37
19 98 BD F2 21 36 21 AE  95 A8 AF 95 6F 06 33 21  3A C4 07 71 FC 25 88 57  4D 6E F8 F6 CC 1B 25 66  11 DE CE 7A 9E A5 1D 03
B7 15 6D 83 1A 8E FC AA  89 8E 5D A9 66 A8 A8 31  C0 88 9E 37 CC 3E 1C 0A  C2 10 F0 C0 BA 18 4B F3  89 E6 F1 76 70 D5 48 A8
F3 02 69 09 43 EB 67 C7  C8 F0 F1 2B 3F 93 03 45  CE 1D 50 06 B8 B6 42 E4  83 BF 20 88 46 10 9A FE  69 39 87 76 A0 73 38 DF
B0 CE BF 49 5B 30 F4 E4  E0 A2 DD 68 23 91 35 8E  1B 4C 83 EF 17 10 58 79  DE CB 6C F2 68 C0 45 0F  59 77 7A B7 32 84 37 4F
5D CC 2E 0E F5 DE C8 A5  A7 8B 68 C6 FC BA 79 7E  0E D2 91 5B CB A9 3C 28  15 99 31 BF C4 18 DB 21  F6 C7 3A 9B 8C EC 7F 93
37 F1 84 43 58 91 F0 22  50 D3 3A 9C 3A 66 22 8F  FA D3 A6 CC 68 CD 0A 78  C3 D5 26 27 B8 78 1B AD  D8 D8 80 3A C9 DD B5 F8
AA BF F8 A0 26 45 2B B5  9D 9D AA 11 D1 87 59 0C  3E 4E 5E 68 B5 4A 67 D3  45 E6 AD 49 72 2E 31 A4  25 32 0B 87 21 9F 52 E0
52 D1 E7 C8 38 82 8A DD  B1 0B 8C BF A1 E0 3A 5E  21 21 7A CF 9F DF 22 83  6F 8F 48 40 C4 CC AD 99  CE FB E0 1A 3B 45 F0 09
4B A0 F4 F5 94 42 02 5F  F2 8C A9 86 81 B8 BA E0  73 09 88 D6 19 63 B9 42  73 3F 8E 0D 9A F2 CC CD  53 BE 4E B7 60 35 E5 F1
C2 4F 81 ED AD B7 AC 0E  83 78 52 5F 30 8A B7 32  A0 85 9F 69 B1 E4 8C FD  DD EA D0 CE 5E 1B B5 5B  5C C8 24 49 7E 1B 24 B8
19 54 A1 D1 6C 84 4D E5  2C 3D C8 99 8A 6F AF 4B  3A A1 CF 54 52 53 E8 61  A4 02 93 28 13 AB 05 77  0F CD 33 E9 B7 96 8C B1
C8 19 DF D2 8F C1 07 36  93 9C D4 A0 2B 95 6B 22  5D F8 56 1D 81 C9 7A C7  25 71 F6 7E E8 8C 1E 19  67 3D 68 3C 0D 25 75 0A
26 AA 55 EC 6F 80 0E DD  FE FA 4B 8B 95 42 1A A1  95 DA 61 36 5C 2E D1 6C  CE FE 26 CA EB A0 E0 1A  FC 05 BC 24 98 2A 75 6A
C9 13 CE 40 07 96 9B A9  22 78 EE E9 5C D9 48 38  6E 4E C3 AF A9 61 E7 C9  B4 F4 36 7C 5C 4F 05 B2  E1 B8 CE 0E 81 CA 27 1A
1D C8 92 CC 69 0D 7C EA  00 E8 B6 96 64 45 94 6B  5E E7 33 A6 2A E9 BB DF  72 48 11 5C B4 94 BE B3  62 98 05 66 53 B0 F2 85
A5 9C 46 0F 2E 64 60 D3  E0 49 65 A4 D0 3C CD 42  A7 B3 7D 95 91 F9 CB D4  D1 55 A6 A3 ED E5 E8 E0  41 D6 B8 40 9D 92 F6 B4
C0 1C 05 7E 67 7F 98 F4  AB A7 2D 42 9D 3B 46 36  D4 83 B8 CD 1A 21 86 34  4F CB 65 FE 92 1D 50 C1  53 1F B3 DC 80 EC B2 44
E0 6D 38 39 50 2E 06 C8  8B 2B 02 A8 54 BD B5 CB  A0 40 F0 72 21 18 6E D5  C8 AF 47 44 30 20 87 A0  6C F6 F3 E1 0B 32 6E 47
72 E9 74 E0 B6 FE 91 3C  5B 95 0C 47 F8 EE 1A 50  EC A8 31 AC C7 04 B9 12  C3 E9 E6 63 08 FA 5A CA  A4 71 56 12 6D 21 50 2F
38 A6 77 3A 8E 7E 03 99  BA B8 6D DF A1 9B B8 7B  07 56 B9 CB 42 3D C9 92  B6 F1 D8 23 E3 5E 1C B8  8D 76 C1 34 DD AF E4 94
68 3B 65 1F 35 05 19 C0  F1 AD 8F CB B9 98 B2 0A  F0 C6 BF BC CB 9C 51 C0  13 75 45 D0 7D 83 6E 94  17 2C 52 C6 07 22 F9 84
40 DD 4D 7A 19 7B 49 06  B8 B2 07 A9 61 57 64 82  6E 37 A1 57 C4 30 BF 9B  FB 04 ED 08 67 D1 52 64  27 7B E0 C6 A1 39 67 3C
D5 8D CE 05 67 9F 3C 20  9D 4F 7D F9 6F 5B 1E B8  5B 98 D0 0C 4D BE 5E 85  E1 42 5E C7 DE AF EB 1F  62 34 17 47 94 E4 5A FC
D7 F6 7F 6B 1F 6A 5A F5  71 E5 EB 0E 2D 3D 7A 26  33 CD EF 3A 1F B8 38 C2  68 17 CC 6C 21 17 CA 6C  3A D4 64 4A 82 DF 2E 0B
9C 91 6A 6B 6A 57 F2 40  3A 37 A7 3C 25 48 49 89  26 EA 56 5D CD 0D 7C 52  CA 8F 33 C3 38 DD 44 99  91 9A EF 18 5C 0D B5 37
19 98 BD F2 21 36 21 AE  95 A8 AF 95 6F 06 33 21  3A C4 07 71 FC 25 88 57  4D 6E F8 F6 CC 1B 25 66  11 DE CE 7A 9E A5 1D 03
B7 15 6D 83 1A 8E FC AA  89 8E 5D A9 66 A8 A8 31  C0 88 9E 37 CC 3E 1C 0A  C2 10 F0 C0 BA 18 4B F3  89 E6 F1 76 70 D5 48 A8
F3 02 69 09 43 EB 67 C7  C8 F0 F1 2B 3F 93 03 45  CE 1D 50 06 B8 B6 42 E4  83 BF 20 88 46 10 9A FE  69 39 87 76 A0 73 38 DF
B0 CE BF 49 5B 30 F4 E4  E0 A2 DD 68 23 91 35 8E  1B 4C 83 EF 17 10 58 79  DE CB 6C F2 68 C0 45 0F  59 77 7A B7 32 84 37 4F
5D CC 2E 0E F5 DE C8 A5  A7 8B 68 C6 FC BA 79 7E  0E D2 91 5B CB A9 3C 28  15 99 31 BF C4 18 DB 21  F6 C7 3A 9B 8C EC 7F 93
37 F1 84 43 58 91 F0 22  50 D3 3A 9C 3A 66 22 8F  FA D3 A6 CC 68 CD 0A 78  C3 D5 26 27 B8 78 1B AD  D8 D8 80 3A C9 DD B5 F8
AA BF F8 A0 26 45 2B B5  9D 9D AA 11 D1 87 59 0C  3E 4E 5E 68 B5 4A 67 D3  45 E6 AD 49 72 2E 31 A4  25 32 0B 87 21 9F 52 E0
52 D1 E7 C8 38 82 8A DD  B1 0B 8C BF A1 E0 3A 5E  21 21 7A CF 9F DF 22 83  6F 8F 48 40 C4 CC AD 99  CE FB E0 1A 3B 45 F0 09
4B A0 F4 F5 94 42 02 5F  F2 8C A9 86 81 B8 BA E0  73 09 88 D6 19 63 B9 42  73 3F 8E 0D 9A F2 CC CD  53 BE 4E B7 60 35 E5 F1
C2 4F 81 ED AD B7 AC 0E  83 78 52 5F 30 8A B7 32  A0 85 9F 69 B1 E4 8C FD  DD EA D0 CE 5E 1B B5 5B  5C C8 24 49 7E 1B 24 B8
19 54 A1 D1 6C 84 4D E5  2C 3D C8 99 8A 6F AF 4B  3A A1 CF 54 52 53 E8 61  A4 02 93 28 13 AB 05 77  0F CD 33 E9 B7 96 8C B1
C8 19 DF D2 8F C1 07 36  93 9C D4 A0 2B 95 6B 22  5D F8 56 1D 81 C9 7A C7  25 71 F6 7E E8 8C 1E 19  67 3D 68 3C 0D 25 75 0A
26 AA 55 EC 6F 80 0E DD  FE FA 4B 8B 95 42 1A A1  95 DA 61 36 5C 2E D1 6C  CE FE 26 CA EB A0 E0 1A  FC 05 BC 24 98 2A 75 6A
C9 13 CE 40 07 96 9B A9  22 78 EE E9 5C D9 48 38  6E 4E C3 AF A9 61 E7 C9  B4 F4 36 7C 5C 4F 05 B2  E1 B8 CE 0E 81 CA 27 1A
1D C8 92 CC 69 0D 7C EA  00 E8 B6 96 64 45 94 6B  5E E7 33 A6 2A E9 BB DF  72 48 11 5C B4 94 BE B3  62 98 05 66 53 B0 F2 85
A5 9C 46 0F 2E 64 60 D3  E0 49 65 A4 D0 3C CD 42  A7 B3 7D 95 91 F9 CB D4  D1 55 A6 A3 ED E5 E8 E0  41 D6 B8 40 9D 92 F6 B4
C0 1C 05 7E 67 7F 98 F4  AB A7 2D 42 9D 3B 46 36  D4 83 B8 CD 1A 21 86 34  4F CB 65 FE 92 1D 50 C1  53 1F B3 DC 80 EC B2 44
E0 6D 38 39 50 2E 06 C8  8B 2B 02 A8 54 BD B5 CB  A0 40 F0 72 21 18 6E D5  C8 AF 47 44 30 20 87 A0  6C F6 F3 E1 0B 32 6E 47
72 E9 74 E0 B6 FE 91 3C  5B 95 0C 47 F8 EE 1A 50  EC A8 31 AC C7 04 B9 12  C3 E9 E6 63 08 FA 5A CA  A4 71 56 12 6D 21 50 2F
38 A6 77 3A 8E 7E 03 99  BA B8 6D DF A1 9B B8 7B  07 56 B9 CB 42 3D C9 92  B6 F1 D8 23 E3 5E 1C B8  8D 76 C1 34 DD AF E4 94
68 3B 65 1F 35 05 19 C0  F1 AD 8F CB B9 98 B2 0A  F0 C6 BF BC CB 9C 51 C0  13 75 45 D0 7D 83 6E 94  17 2C 52 C6 07 22 F9 84
40 DD 4D 7A 19 7B 49 06  B8 B2 07 A9 61 57 64 82  6E 37 A1 57 C4 30 BF 9B  FB 04 ED 08 67 D1 52 64  27 7B E0 C6 A1 39 67 3C
D5 8D CE 05 67 9F 3C 20  9D 4F 7D F9 6F 5B 1E B8  5B 98 D0 0C 4D BE 5E 85  E1 42 5E C7 DE AF EB 1F  62 34 17 47 94 E4 5A FC
D7 F6 7F 6B 1F 6A 5A F5  71 E5 EB 0E 2D 3D 7A 26  33 CD EF 3A 1F B8 38 C2  68 17 CC 6C 21 17 CA 6C  3A D4 64 4A 82 DF 2E 0B
9C 91 6A 6B 6A 57 F2 40  3A 37 A7 3C 25 48 49 89  26 EA 56 5D CD 0D 7C 52  CA 8F 33 C3 38 DD 44 99  91 9A EF 18 5C 0D B5 37
19 98 BD F2 21 36 21 AE  95 A8 AF 95 6F 06 33 21  3A C4 07 71 FC 25 88 57  4D 6E F8 F6 CC 1B 25 66  11 DE CE 7A 9E A5 1D 03
B7 15 6D 83 1A 8E FC AA  89 8E 5D A9 66 A8 A8 31  C0 88 9E 37 CC 3E 1C 0A  C2 10 F0 C0 BA 18 4B F3  89 E6 F1 76 70 D5 48 A8
F3 02 69 09 43 EB 67 C7  C8 F0 F1 2B 3F 93 03 45  CE 1D 50 06 B8 B6 42 E4  83 BF 20 88 46 10 9A FE  69 39 87 76 A0 73 38 DF
B0 CE BF 49 5B 30 F4 E4  E0 A2 DD 68 23 91 35 8E  1B 4C 83 EF 17 10 58 79  DE CB 6C F2 68 C0 45 0F  59 77 7A B7 32 84 37 4F
5D CC 2E 0E F5 DE C8 A5  A7 8B 68 C6 FC BA 79 7E  0E D2 91 5B CB A9 3C 28  15 99 31 BF C4 18 DB 21  F6 C7 3A 9B 8C EC 7F 93
37 F1 84 43 58 91 F0 22  50 D3 3A 9C 3A 66 22 8F  FA D3 A6 CC 68 CD 0A 78  C3 D5 26 27 B8 78 1B AD  D8 D8 80 3A C9 DD B5 F8
AA BF F8 A0 26 45 2B B5  9D 9D AA 11 D1 87 59 0C  3E 4E 5E 68 B5 4A 67 D3  45 E6 AD 49 72 2E 31 A4  25 32 0B 87 21 9F 52 E0
52 D1 E7 C8 38 82 8A DD  B1 0B 8C BF A1 E0 3A 5E  21 21 7A CF 9F DF 22 83  6F 8F 48 40 C4 CC AD 99  CE FB E0 1A 3B 45 F0 09
4B A0 F4 F5 94 42 02 5F  F2 8C A9 86 81 B8 BA E0  73 09 88 D6 19 63 B9 42  73 3F 8E 0D 9A F2 CC CD  53 BE 4E B7 60 35 E5 F1
C2 4F 81 ED AD B7 AC 0E  83 78 52 5F 30 8A B7 32  A0 85 9F 69 B1 E4 8C FD  DD EA D0 CE 5E 1B B5 5B  5C C8 24 49 7E 1B 24 B8
19 54 A1 D1 6C 84 4D E5  2C 3D C8 99 8A 6F AF 4B  3A A1 CF 54 52 53 E8 61  A4 02 93 28 13 AB 05 77  0F CD 33 E9 B7 96 8C B1
C8 19 DF D2 8F C1 07 36  93 9C D4 A0 2B 95 6B 22  5D F8 56 1D 81 C9 7A C7  25 71 F6 7E E8 8C 1E 19  67 3D 68 3C 0D 25 75 0A
26 AA 55 EC 6F 80 0E DD  FE FA 4B 8B 95 42 1A A1  95 DA 61 36 5C 2E D1 6C  CE FE 26 CA EB A0 E0 1A  FC 05 BC 24 98 2A 75 6A
C9 13 CE 40 07 96 9B A9  22 78 EE E9 5C D9 48 38  6E 4E C3 AF A9 61 E7 C9  B4 F4 36 7C 5C 4F 05 B2  E1 B8 CE 0E 81 CA 27 1A
1D C8 92 CC 69 0D 7C EA  00 E8 B6 96 64 45 94 6B  5E E7 33 A6 2A E9 BB DF  72 48 11 5C B4 94 BE B3  62 98 05 66 53 B0 F2 85
A5 9C 46 0F 2E 64 60 D3  E0 49 65 A4 D0 3C CD 42  A7 B3 7D 95 91 F9 CB D4  D1 55 A6 A3 ED E5 E8 E0  41 D6 B8 40 9D 92 F6 B4
C0 1C 05 7E 67 7F 98 F4  AB A7 2D 42 9D 3B 46 36  D4 83 B8 CD 1A 21 86 34  4F CB 65 FE 92 1D 50 C1  53 1F B3 DC 80 EC B2 44
E0 6D 38 39 50 2E 06 C8  8B 2B 02 A8 54 BD B5 CB  A0 40 F0 72 21 18 6E D5  C8 AF 47 44 30 20 87 A0  6C F6 F3 E1 0B 32 6E 47
72 E9 74 E0 B6 FE 91 3C  5B 95 0C 47 F8 EE 1A 50  EC A8 31 AC C7 04 B9 12  C3 E9 E6 63 08 FA 5A CA  A4 71 56 12 6D 21 50 2F
38 A6 77 3A 8E 7E 03 99  BA B8 6D DF A1 9B B8 7B  07 56 B9 CB 42 3D C9 92  B6 F1 D8 23 E3 5E 1C B8  8D 76 C1 34 DD AF E4 94
68 3B 65 1F 35 05 19 C0  F1 AD 8F CB B9 98 B2 0A  F0 C6 BF BC CB 9C 51 C0  13 75 45 D0 7D 83 6E 94  17 2C 52 C6 07 22 F9 84
```

```
                     06  B8 B2 07 A9 61 57 64 82  6E 37 A1 57 C4 30 BF 9B  FB 04 ED 08 67 D1 52 64  27 7B E0 C6 A1 39 67 3C
D5 8D CE 05 67 9F 3C 20  9D 4F 7D F9 6F 5B 1E B8  5B 98 D0 0C 4D BE 5E 85  E1 42 5E C7 DE AF EB 1F  62 34 17 47 94 E4 5A FC
D7 F6 7F 6B 1F 6A 5A F5  71 E5 EB 0E 2D 3D 7A 26  33 CD EF 3A 1F B8 38




                                              8E  1B 4C 83 EF 17 10 58 79  DE CB 6C F2 68 C0 45 0F  59 77 7A B7 32 84 37 4F
5D CC 2E 0E F5 DE C8 A5  A7 8B 68 C6 FC BA 79 7E  0E D2 91 5B CB A9 3C 28  15 99 31 BF C4 18 DB 21  F6 C7 3A 9B 8C EC 7F 93
37 F1 84 43 58 91 F0 22  50 D3 3A 9C 3A 66 22 8F  FA D3 A6 CC 68 CD 0A 78  C3 D5 26 27 B8 78 1B


                     5F  F2 8C A9 86 81 B8 BA E0  73 09 88 D6 19 63 B9 42  73 3F 8E 0D 9A F2 CC CD  53 BE 4E B7 60 35 E5 F1
C2 4F 81 ED AD B7 AC 0E  83 78 52 5F 30 8A B7 32  A0 85 9F 69 B1 E4 8C FD  DD EA D0 CE 5E 1B B5 5B  5C C8 24 49 7E 1B 24 B8
19 54 A1 D1 6C 84 4D E5  2C 3D C8 99 8A 6F AF 4B  3A A1 CF 5C 52 53 E8 61  A4 02 93 28 13 AB 05 77  0F CD 33 E9 B7 96 8C B1
C8 19 DF D2 8F C1 07 36  93 9C D4 A0 2B 95 6B 22  5D F8 56 1D 81 C9 7A C7  25 71 F6 7E E8 8C 1E 19  67 3D 68 3C 0D 25 75 0A
26 AA 55 EC 6F 80 0E DD  FE FA 4B 8B 95 42 1A A1  95 DA 61 36 5C 2E D1 6C  CE FE 26 CA EB A0 E0 1A  FC 05 BC 24 98 2A 75


                                              42  A7 B3 7D 95 91 F9 CB D4  D1 55 A6 A3 ED E5 E8 E0  41 D6 B8 40 9D 92 F6 B4
C0 1C 05 7E 67 7F 98 F4  AB A7 2D 42 9D 3B 46 36  D4 83 B8 CD 1A 21 86 34  4F CB 65 FE 92 1D 50 C1  53 1F B3 DC 80 EC B2 44
E0 6D 38 39 50 2E 06 C8  8B 2B 02 A8 54 BD B5 CB  A0 40 F0 72 21 18 6E D5  C8 AF 47 44 30 20 87 A0  6C F6 F3 E1 0B 32 6E 47
72 E9 74 E0 B6 FE 91 3C  5B 95 0C 47 F8 EE 1A 50  EC A8 31 AC C7 04 B9 12  C3 E9 E6 63 08 FA 5A CA  A4 71 56 12 6D 21 50 2F
38 A6 77 3A 8E 7E 03 99  BA B8 6D DF A1 9B B8 7B  07 56 B9 CB 42 3D C9 92  B6 F1 D8 23 E3 5E 1C B8  8D 76 C1 34 DD AF E4 94
68 3B 65 1F 35 05 19



                            37
19 98 BD F2 21 36 21 AE  95 A8 AF 95 6F 06 33 21  3A C4 07 70 FC 25 88 57  4D 6E F8 F6 CC 1B 25 67  11 DE CE 7A 9E A5 1D 03
B7 15 6D 83 1A 8E FC AA  89 8E 5D A9 66 A8 A8 31  C0 88 9E 37 CC 3E 1C 0A  C2 10 F0 C0 BA 18 4B F3  89 E6 F1 76 70 D5 48 A8
F3 02 69 09 43 EB 67 C7  C8 F0 F1 2B 3F 93 03

                                                                       21  F6 C7 3A 9B 8C EC 7F 93
37 F1 84 43 58 91 F0 22  50 D3 3A 9C 3A 66 22 8F  FA D3 A6 CC 68 CD 0A 78  C3 D5 26 27 B8 78 3B AD  D8 D8 80 3A C9 DD B5 F8
AA BF E8 A0 26 45 2B B5  9D 9D AA 11 D1 87 79 0C  3E 4E 5E 68 B5 4A 67 D3  45 E6 8D 49 72 2E 31 A4  25 32 0B 87 21 9F 72 E0
52 D1 E7 C8 38 82 8A DD  B1 0B 8C BF A1 E0 3A 5E  21 21 7A CF 9F DF 22 83  6F 8F 48 40 C4 CC AD 99  CE FB E0 1A 3B 45 F0 09
4B A0 F4 F5 94 42 06 5F  F2 8C A9 8E 81 B8 BA E0  73 09 80 D6 19 63 B9 46  73 3F 8E 0D 9A F2 C8 CD  53 BE 4E BF 60 35 E5 F1
C2 4F 95 ED AD B7 AC 0A  83 78 52 5F 30 8A AF 32  A0 85 9F 61 B1 E4 8C

                                                                                                                         0A
26 AA 55 EC 6F 80 0E DD  FE FA 4B 8B 95 42 1A A1  95 DA 61 36 5C 2E D1 6C  CE FE 26 CA EB A0 E0 1A  FC 05 BC 24 98 2A 75 6A
C9 13 CE 40 07 96 9B A9  22 78 EE E9 5C D9 48 38  6E 4E C3 AF A9 61 E7 C9  B4 F4 36 7C 5C 4F 05 B2  E1 B8 CE 0E 81 CA 27 1A
1D C8 92 CC 69 0D 7C EA  00 E8 B6 96 64 45 94 6B  5E E7 33 A6 2A E9 BB DF  72 48 11 5C B4 94 BE B3  62 98 05 66 53 B0 F2 85
A5 9C 46 0F 2E 64 60 D3  E0 49 65 A4 D0 3C CD 42  A7 B3 7D 95 91 F9 CB D4  D1 55 A6 A3 ED E5 E8 E0  41 D6 B8 40 9D 92 F6 B4
C0 1C 05 7E 67 7F 98 F4  AB A7 2D 42 9D 3B 46 36  D4 83 B8 CD 1A 21 86 34  4F CB 65 FE 92 1D 50


                     99  BA B8 6D DF A1 9B B8 7B  07 56 B9 CB 42 3D C9 92  B6 F1 D8 23 E3 5E 1C B8  8D 76 C1 34 DD AF E4 94
68 3B 65 1F 35 05 19 C0  F1 AD 8F CB B9 98 B2 0A  F0 C6 BF BC CB 9C 51 C0  13 75 45 D0 7D 83 6E 94  17 2C 52 C6 07 22 F9 84
40 DD 4D 7A 19 7B 49 06  B8 B2 07 A9 61 57 64 82  6E 37 A1 57 C4 30 BF 9B  FB 04 ED 08 67 D1 52 64  27 7B E0 C6 A1 39 67 3C
D5 8D CE 05 67 9F 3C 20  9D 4F 7D F9 6F 5B 1E B8  5B 98 D0 0C 4D BE 5E 85  E1 42 5E C7 DE AF EB 1F  62 34 17 47 94 E4 5A FC
D7 F6 7F 6B 1F 6A 5A F5  71 E5 EB 0E 2D 3D 7A 26  33 CD EF 3A 1F B8 38 C2  68 17 CC 6C 21 17 CA 6C  3A D4 64 4A 82 DF 2E


                                              31  C0 88 9E 37 CC 3E 1C 0A  C2 10 F0 C0 BA 18 4B F3  89 E6 F1 76 70 D5 48 A8
F3 02 69 09 43 EB 67 C7  C8 F0 F1 2B 3F 93 03 45  CE 1D 50 06 B8 B6 42 E4  83 BF 20 88 46 10 9A FE  69 39 87 76 A0 73 38 DF
B0 CE BF 49 5B 30 F4 E4  E0 A2 DD 68 23 91 35 8E  1B 4C 83 EF 17 10 58 79  DE CB 6C F2 68 C0 45 0F  59 77 7A B7 32 84 37 4F
5D CC 2E 0E F5 DE C8 A5  A7 8B 68 C6 FC BA 79 7E  0E D2 91 5B CB A9 3C 28  15 99 31 BF C4 18 DB 21  F6 C7 3A 9B 8C EC 7F 93
37 F1 84 43 58 91 F0 22  50 D3 3A 9C 3A 66 22 8F  FA D3 A6 CC 68 CD 0A 78  C3 D5 26 27 B8 78 1B AF  D8 D8 80 3A C9 DD B5 F8
AA BF F8 A1 26 45 2B

                                                                       42  73 3F 8E 0D 9A F2 CC CD  53 BE 4E B7 60 35 E5 F1
C2 4F 81 ED AD B7 AC 0E  83 78 52 5F 30 8A B7 32  A0 85 9F 69 B1 E4 8C FD  DD EA D0 CE 5E 1B B5 5B  5C C8 24 49 7E 1B 24 B8
19 54 A1 D1 6C 84 4D E5  2C 3D C8 99 8A 6F AF 4B  3A A1 CF 54 52 53 E8 61  A4 02 93 28 13 AB 05 77  0F CD 33 E9 B7 96 8C B1
C8 19 DF D2 8F C1 07 36  93 9C D4 A0 2B 95 6B 22  5D F8 56 1D 81 C9 7A C7  25 71 F6 7E E8 8C 1E 19  67 3D 68 3C 0D 25 75 0A
26 AA 55 EC 6F 80 0E DD  FE FA 4B 8B 95 42 1A A1  95 DA 61 36 5C 2E D1 6C  CE FE 26 CA EB A0 E0 1A  FC 05 BC 24 98 2A 75 6A
C9 13 CE 40 07 96 9B A9  22 78 EE E9 5C D9 48

                                                                                               E0  41 D6 B8 40 9D 92 F6 B4
C0 1C 05 7E 67 7F 98 F4  AB A7 2D 42 9D 3B 46 36  D4 83 B8 CD 1A 21 86 34  4F CB 65 FE 92 1D 50 C1  53 1F B3 DC 80 EC B2 44
E0 6D 38 39 50 2E 06 C8  8B 2B 02 A8 54 BD B5 CA  A0 40 F0 72 21 18 6E D5  C8 AF 46 45 30 20 87 A0  6C F6 F3 E1 0B 32 6C 46
72 E9 74 E0 B6 FE 91 3C  5B 95 0C 47 F8 EE 1A 50  EC A8 31 AC C7 04 B9 12  C3 E9 E6 63 08 FA 5A CA  A4 71 56 12 6D 21 50 2F
38 A6 77 3A 8E 7E 03 99  BA B8 6D DF A1 9B B8 7B  07 56 B9 CB 42 3D C9 92  B6 F1 D8 23 E3 5E 1C B8  8D 76 C1 34 DD AF E4 94
68 3B 65 1F 35 05 19 C0  F1 AD 8F CB B9 98 B2 0A  F0 C6 BF BC CB 9C 51
```

Figure D.1: Sent and Received Messages for the Case with $k1 = k2 = (1, -1, 1)$ in the Laboratory

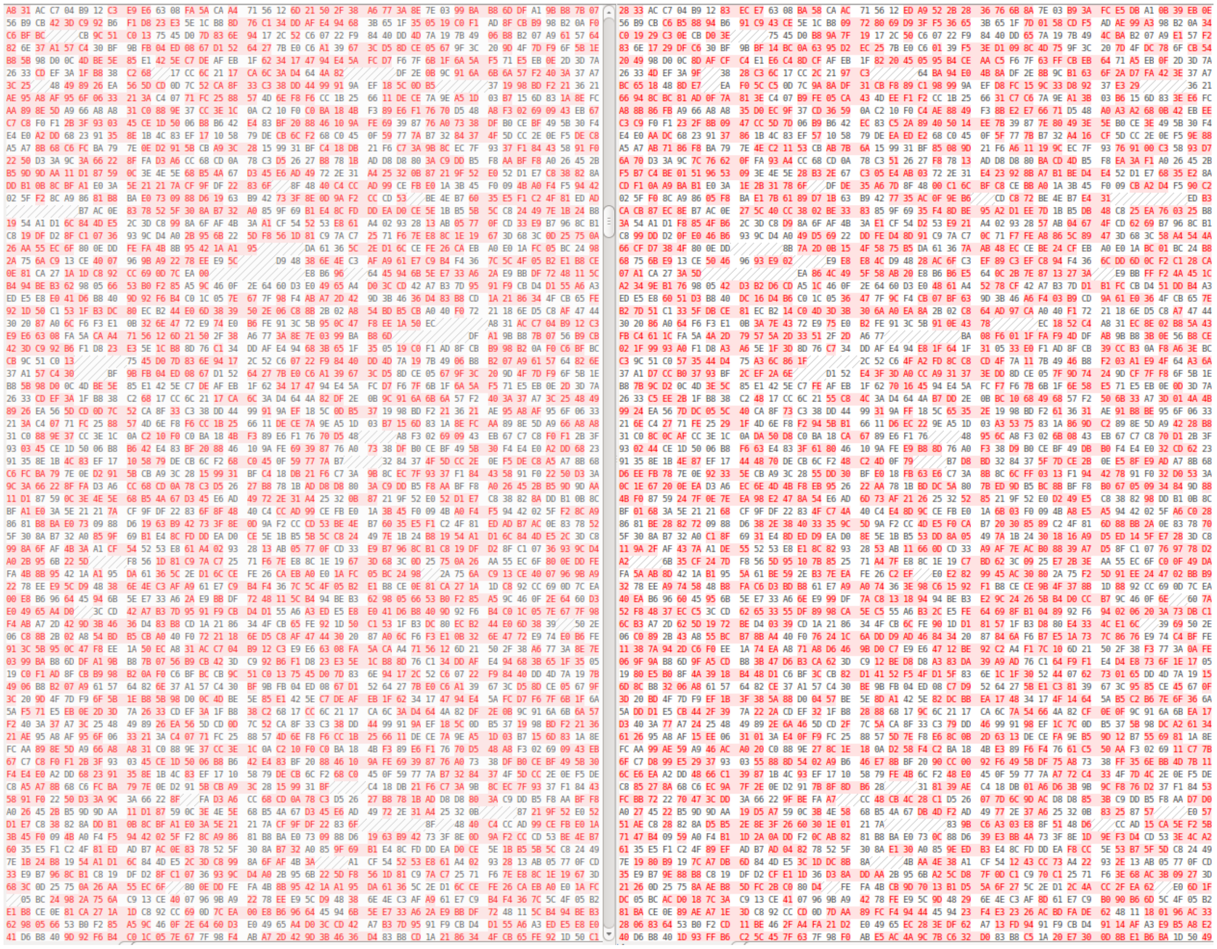
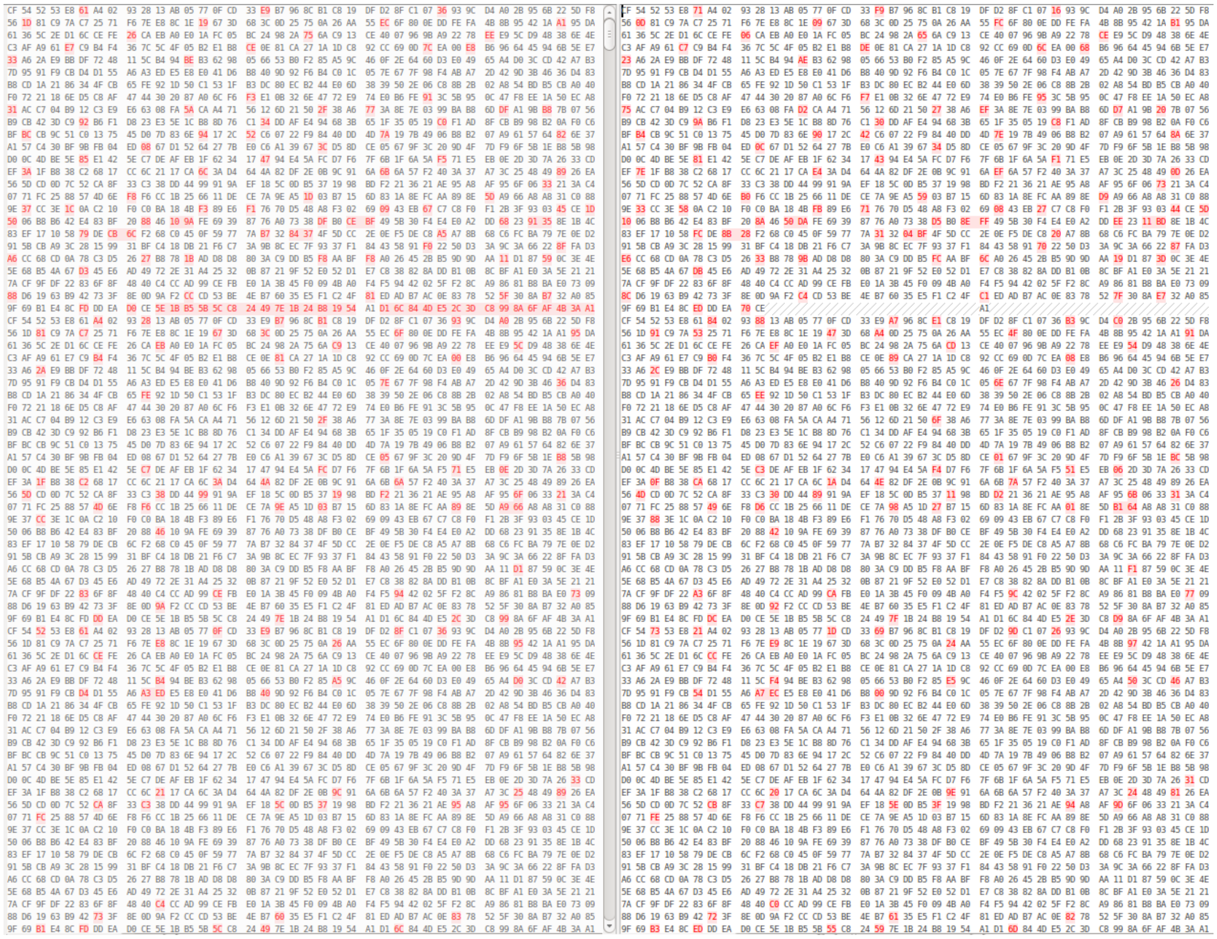


Figure D.2: Sent and Received Messages for the Case with $k1 = k2 = (1, -1, -1, 1)$ in the Laboratory



```
CF 54 52 53 E8 61 A4 02  93 28 13 AB 05 77 0F CD  33 E9 B7 96 8C B1 C8 19  DF D2 8F C1 07 36 93 9C  D4 A0 2B 95 6B 22 5D F8
56 1D 81 C9 7A C7 25 71  F6 7E E8 8C 1E 19 67 3D  68 3C 0D 25 75 0A 26 AA  55 EC 6F 80 0E DD FE FA  4B 8B 95 42 1A A1 95 DA
61 36 5C 2E D1 6C CE FE  26 CA EB A0 E0 1A FC 05  BC 24 98 2A 75 6A C9 13  CE 40 07 96 9B A9 22 78  EE E9 5C D9 48 38 6E 4E
C3 AF A9 61 E7 C9 B4 F4  36 7C 5C 4F 05 B2 E1 B8  CE 0E 81 CA 27 1A 1D C8  92 CC 69 0D 7C EA 00 E8  B6 96 64 45 94 6B 5E E7
33 A6 2A E9 BB DF 72 48  11 5C B4 94 BE B3 62 98  05 66 53 B0 F2 85 A5 9C  46 0F 2E 64 60 D3 E0 49  65 A4 D0 3C CD 42 A7 B3
7D 95 91 F9 CB D4 D1 55  A6 A3 ED E5 E8 E0 41 D6  B8 40 9D 92 F6 B4 C0 1C  05 7E 67 7F 98 F4 AB A7  2D 42 9D 3B 46 36 D4 83
B8 CD 1A 21 86 34 4F CB  65 FE 92 1D 50 C1 53 1F  B3 DC 80 EC B2 44 E0 6D  38 39 50 2E 06 C8 8B 2B  02 A8 54 BD B5 CB A0 40
F0 72 21 18 6E D5 C8 AF  47 44 30 20 87 A0 6C F6  F3 E1 0B 32 6E 47 72 E9  74 E0 B6 FE 91 3C 5B 95  0C 47 F8 EE 1A 50 EC A8
31 AC C7 04 B9 12 C3 E9  E6 63 08 FA 5A CA A4 71  56 12 6D 21 50 2F 38 A6  77 3A 8E 7E 03 99 BA B8  6D DF A1 9B B8 7B 07 56
B9 CB 42 3D C9 92 B6 F1  D8 23 E3 5E 1C B8 8D 76  C1 34 DD AF E4 94 68 3B  65 1F 35 05 19 C0 F1 AD  8F CB B9 98 B2 0A F0 C6
BF BC CB 9C 51 C0 13 75  45 D0 7D 83 6E 94 17 2C  52 C6 07 22 F9 84 40 DD  4D 7A 19 7B 49 06 B8 B2  07 A9 61 57 64 82 6E 37
A1 57 C4 30 BF 9B FB 04  ED 08 67 D1 52 64 27 7B  E0 C6 A1 39 67 3C D5 8D  CE 05 67 9F 3C 20 9D 4F  7D F9 6F 5B 1E B8 5B 98
D0 0C 4D BE 5E 85 E1 42  5E C7 DE AF EB 1F 62 34  17 47 94 E4 5A FC D7 F6  7F 6B 1F 6A 5A F5 71 E5  EB 0E 2D 3D 7A 26 33 CD
EF 3A 1F B8 38 C2 68 17  CC 6C 21 17 CA 6C 3A D4  64 4A 82 DF 2E 0B 9C 91  6A 6B 6A 57 F2 40 3A 37  A7 3C 25 48 49 89 26 EA
56 5D CD 0D 7C 52 CA 8F  33 C3 38 DD 44 99 91 9A  EF 18 5C 0D B5 37 19 98  BD F2 21 36 21 AE 95 A8  AF 95 6F 06 33 21 3A C4
07 71 FC 25 88 57 4D 6E  F8 F6 CC 1B 25 66 11 DE  CE 7A 9E A5 1D 03 B7 15  6D 83 1A 8E FC AA 89 8E  5D A9 66 A8 A8 31 C0 88
9E 37 CC 3E 1C 0A C2 10  F0 C0 BA 18 4B F3 89 E6  F1 76 70 D5 48 A8 F3 02  69 09 43 EB 67 C7 C8 F0  F1 2B 3F 93 03 45 CE 1D
50 06 B8 B6 42 E4 83 BF  20 88 46 10 9A FE 69 39  87 76 A0 73 38 DF B0 CE  BF 49 5B 30 F4 E4 E0 A2  DD 68 23 91 35 8E 1B 4C
83 EF 17 10 58 79 DE CB  6C F2 68 C0 45 0F 59 77  7A B7 32 84 37 4F 5D CC  2E 0E F5 DE C8 A5 A7 8B  68 C6 FC BA 79 7E 0E D2
91 5B CB A9 3C 28 15 99  31 BF C4 18 DB 21 F6 C7  3A 9B 8C EC 7F 93 37 F1  84 43 58 91 F0 22 50 D3  3A 9C 3A 66 22 8F FA D3
A6 CC 68 CD 0A 78 C3 D5  26 27 B8 78 1B AD D8 D8  80 3A C9 DD B5 F8 AA BF  F8 A0 26 45 2B B5 9D 9D  AA 11 D1 87 59 0C 3E 4E
5E 68 B5 4A 67 D3 45 E6  AD 49 72 2E 31 A4 25 32  0B 87 21 9F 52 E0 52 D1  E7 C8 38 82 8A DD B1 0B  8C BF A1 E0 3A 5E 21 21
7A CF 9F DF 22 83 6F 8F  48 40 C4 CC AD 99 CE FB  E0 1A 3B 45 F0 09 4B A0  F4 F5 94 42 02 5F F2 8C  A9 86 81 B8 BA E0 73 09
88 D6 19 63 B9 42 73 3F  8E 0D 9A F2 CC CD 53 BE  4E B7 60 35 E5 F1 C2 4F  81 ED AD B7 AC 0E 83 78  52 5F 30 8A B7 32 A0 85
9F 69 B1 E4 8C FD DD EA  D0 CE 5E 1B B5 5B 5C C8  24 49 7E 1B 24 B8 19 54  A1 D1 6C 84 4D E5 2C 3D  C8 99 8A 6F AF 4B 3A A1
CF 54 52 53 E8 61 A4 02  93 28 13 AB 05 77 0F CD  33 E9 B7 96 8C B1 C8 19  DF D2 8F C1 07 36 93 9C  D4 A0 2B 95 6B 22 5D F8
56 1D 81 C9 7A C7 25 71  F6 7E E8 8C 1E 19 67 3D  68 3C 0D 25 75 0A 26 AA  55 EC 6F 80 0E DD FE FA  4B 8B 95 42 1A A1 95 DA
61 36 5C 2E D1 6C CE FE  26 CA EB A0 E0 1A FC 05  BC 24 98 2A 75 6A C9 13  CE 40 07 96 9B A9 22 78  EE E9 5C D9 48 38 6E 4E
C3 AF A9 61 E7 C9 B4 F4  36 7C 5C 4F 05 B2 E1 B8  CE 0E 81 CA 27 1A 1D C8  92 CC 69 0D 7C EA 00 E8  B6 96 64 45 94 6B 5E E7
33 A6 2A E9 BB DF 72 48  11 5C B4 94 BE B3 62 98  05 66 53 B0 F2 85 A5 9C  46 0F 2E 64 60 D3 E0 49  65 A4 D0 3C CD 42 A7 B3
7D 95 91 F9 CB D4 D1 55  A6 A3 ED E5 E8 E0 41 D6  B8 40 9D 92 F6 B4 C0 1C  05 7E 67 7F 98 F4 AB A7  2D 42 9D 3B 46 36 D4 83
B8 CD 1A 21 86 34 4F CB  65 FE 92 1D 50 C1 53 1F  B3 DC 80 EC B2 44 E0 6D  38 39 50 2E 06 C8 8B 2B  02 A8 54 BD B5 CB A0 40
F0 72 21 18 6E D5 C8 AF  47 44 30 20 87 A0 6C F6  F3 E1 0B 32 6E 47 72 E9  74 E0 B6 FE 91 3C 5B 95  0C 47 F8 EE 1A 50 EC A8
31 AC C7 04 B9 12 C3 E9  E6 63 08 FA 5A CA A4 71  56 12 6D 21 50 2F 38 A6  77 3A 8E 7E 03 99 BA B8  6D DF A1 9B B8 7B 07 56
B9 CB 42 3D C9 92 B6 F1  D8 23 E3 5E 1C B8 8D 76  C1 34 DD AF E4 94 68 3B  65 1F 35 05 19 C0 F1 AD  8F CB B9 98 B2 0A F0 C6
BF BC CB 9C 51 C0 13 75  45 D0 7D 83 6E 94 17 2C  52 C6 07 22 F9 84 40 DD  4D 7A 19 7B 49 06 B8 B2  07 A9 61 57 64 82 6E 37
A1 57 C4 30 BF 9B FB 04  ED 08 67 D1 52 64 27 7B  E0 C6 A1 39 67 3C D5 8D  CE 05 67 9F 3C 20 9D 4F  7D F9 6F 5B 1E B8 5B 98
D0 0C 4D BE 5E 85 E1 42  5E C7 DE AF EB 1F 62 34  17 47 94 E4 5A FC D7 F6  7F 6B 1F 6A 5A F5 71 E5  EB 0E 2D 3D 7A 26 33 CD
EF 3A 1F B8 38 C2 68 17  CC 6C 21 17 CA 6C 3A D4  64 4A 82 DF 2E 0B 9C 91  6A 6B 6A 57 F2 40 3A 37  A7 3C 25 48 49 89 26 EA
56 5D CD 0D 7C 52 CA 8F  33 C3 38 DD 44 99 91 9A  EF 18 5C 0D B5 37 19 98  BD F2 21 36 21 AE 95 A8  AF 95 6F 06 33 21 3A C4
07 71 FC 25 88 57 4D 6E  F8 F6 CC 1B 25 66 11 DE  CE 7A 9E A5 1D 03 B7 15  6D 83 1A 8E FC AA 89 8E  5D A9 66 A8 A8 31 C0 88
9E 37 CC 3E 1C 0A C2 10  F0 C0 BA 18 4B F3 89 E6  F1 76 70 D5 48 A8 F3 02  69 09 43 EB 67 C7 C8 F0  F1 2B 3F 93 03 45 CE 1D
50 06 B8 B6 42 E4 83 BF  20 88 46 10 9A FE 69 39  87 76 A0 73 38 DF B0 CE  BF 49 5B 30 F4 E4 E0 A2  DD 68 23 91 35 8E 1B 4C
83 EF 17 10 58 79 DE CB  6C F2 68 C0 45 0F 59 77  7A B7 32 84 37 4F 5D CC  2E 0E F5 DE C8 A5 A7 8B  68 C6 FC BA 79 7E 0E D2
91 5B CB A9 3C 28 15 99  31 BF C4 18 DB 21 F6 C7  3A 9B 8C EC 7F 93 37 F1  84 43 58 91 F0 22 50 D3  3A 9C 3A 66 22 8F FA D3
A6 CC 68 CD 0A 78 C3 D5  26 27 B8 78 1B AD D8 D8  80 3A C9 DD B5 F8 AA BF  F8 A0 26 45 2B B5 9D 9D  AA 11 D1 87 59 0C 3E 4E
5E 68 B5 4A 67 D3 45 E6  AD 49 72 2E 31 A4 25 32  0B 87 21 9F 52 E0 52 D1  E7 C8 38 82 8A DD B1 0B  8C BF A1 E0 3A 5E 21 21
7A CF 9F DF 22 83 6F 8F  48 40 C4 CC AD 99 CE FB  E0 1A 3B 45 F0 09 4B A0  F4 F5 94 42 02 5F F2 8C  A9 86 81 B8 BA E0 73 09
88 D6 19 63 B9 42 73 3F  8E 0D 9A F2 CC CD 53 BE  4E B7 60 35 E5 F1 C2 4F  81 ED AD B7 AC 0E 83 78  52 5F 30 8A B7 32 A0 85
9F 69 B1 E4 8C FD DD EA  D0 CE 5E 1B B5 5B 5C C8  24 49 7E 1B 24 B8 19 54  A1 D1 6C 84 4D E5 2C 3D  C8 99 8A 6F AF 4B 3A A1
CF 54 52 53 E8 61 A4 02  93 28 13 AB 05 77 0F CD  33 E9 B7 96 8C B1 C8 19  DF D2 8F C1 07 36 93 9C  D4 A0 2B 95 6B 22 5D F8
56 1D 81 C9 7A C7 25 71  F6 7E E8 8C 1E 19 67 3D  68 3C 0D 25 75 0A 26 AA  55 EC 6F 80 0E DD FE FA  4B 8B 95 42 1A A1 95 DA
61 36 5C 2E D1 6C CE FE  26 CA EB A0 E0 1A FC 05  BC 24 98 2A 75 6A C9 13  CE 40 07 96 9B A9 22 78  EE E9 5C D9 48 38 6E 4E
C3 AF A9 61 E7 C9 B4 F4  36 7C 5C 4F 05 B2 E1 B8  CE 0E 81 CA 27 1A 1D C8  92 CC 69 0D 7C EA 00 E8  B6 96 64 45 94 6B 5E E7
33 A6 2A E9 BB DF 72 48  11 5C B4 94 BE B3 62 98  05 66 53 B0 F2 85 A5 9C  46 0F 2E 64 60 D3 E0 49  65 A4 D0 3C CD 42 A7 B3
7D 95 91 F9 CB D4 D1 55  A6 A3 ED E5 E8 E0 41 D6  B8 40 9D 92 F6 B4 C0 1C  05 7E 67 7F 98 F4 AB A7  2D 42 9D 3B 46 36 D4 83
B8 CD 1A 21 86 34 4F CB  65 FE 92 1D 50 C1 53 1F  B3 DC 80 EC B2 44 E0 6D  38 39 50 2E 06 C8 8B 2B  02 A8 54 BD B5 CB A0 40
F0 72 21 18 6E D5 C8 AF  47 44 30 20 87 A0 6C F6  F3 E1 0B 32 6E 47 72 E9  74 E0 B6 FE 91 3C 5B 95  0C 47 F8 EE 1A 50 EC A8
31 AC C7 04 B9 12 C3 E9  E6 63 08 FA 5A CA A4 71  56 12 6D 21 50 2F 38 A6  77 3A 8E 7E 03 99 BA B8  6D DF A1 9B B8 7B 07 56
B9 CB 42 3D C9 92 B6 F1  D8 23 E3 5E 1C B8 8D 76  C1 34 DD AF E4 94 68 3B  65 1F 35 05 19 C0 F1 AD  8F CB B9 98 B2 0A F0 C6
BF BC CB 9C 51 C0 13 75  45 D0 7D 83 6E 94 17 2C  52 C6 07 22 F9 84 40 DD  4D 7A 19 7B 49 06 B8 B2  07 A9 61 57 64 82 6E 37
A1 57 C4 30 BF 9B FB 04  ED 08 67 D1 52 64 27 7B  E0 C6 A1 39 67 3C D5 8D  CE 05 67 9F 3C 20 9D 4F  7D F9 6F 5B 1E B8 5B 98
D0 0C 4D BE 5E 85 E1 42  5E C7 DE AF EB 1F 62 34  17 47 94 E4 5A FC D7 F6  7F 6B 1F 6A 5A F5 71 E5  EB 0E 2D 3D 7A 26 33 CD
EF 3A 1F B8 38 C2 68 17  CC 6C 21 17 CA 6C 3A D4  64 4A 82 DF 2E 0B 9C 91  6A 6B 6A 57 F2 40 3A 37  A7 3C 25 48 49 89 26 EA
56 5D CD 0D 7C 52 CA 8F  33 C3 38 DD 44 99 91 9A  EF 18 5C 0D B5 37 19 98  BD F2 21 36 21 AE 95 A8  AF 95 6F 06 33 21 3A C4
07 71 FC 25 88 57 4D 6E  F8 F6 CC 1B 25 66 11 DE  CE 7A 9E A5 1D 03 B7 15  6D 83 1A 8E FC AA 89 8E  5D A9 66 A8 A8 31 C0 88
9E 37 CC 3E 1C 0A C2 10  F0 C0 BA 18 4B F3 89 E6  F1 76 70 D5 48 A8 F3 02  69 09 43 EB 67 C7 C8 F0  F1 2B 3F 93 03 45 CE 1D
50 06 B8 B6 42 E4 83 BF  20 88 46 10 9A FE 69 39  87 76 A0 73 38 DF B0 CE  BF 49 5B 30 F4 E4 E0 A2  DD 68 23 91 35 8E 1B 4C
83 EF 17 10 58 79 DE CB  6C F2 68 C0 45 0F 59 77  7A B7 32 84 37 4F 5D CC  2E 0E F5 DE C8 A5 A7 8B  68 C6 FC BA 79 7E 0E D2
91 5B CB A9 3C 28 15 99  31 BF C4 18 DB 21 F6 C7  3A 9B 8C EC 7F 93 37 F1  84 43 58 91 F0 22 50 D3  3A 9C 3A 66 22 8F FA D3
A6 CC 68 CD 0A 78 C3 D5  26 27 B8 78 1B AD D8 D8  80 3A C9 DD B5 F8 AA BF  F8 A0 26 45 2B B5 9D 9D  AA 11 D1 87 59 0C 3E 4E
5E 68 B5 4A 67 D3 45 E6  AD 49 72 2E 31 A4 25 32  0B 87 21 9F 52 E0 52 D1  E7 C8 38 82 8A DD B1 0B  8C BF A1 E0 3A 5E 21 21
7A CF 9F DF 22 83 6F 8F  48 40 C4 CC AD 99 CE FB  E0 1A 3B 45 F0 09 4B A0  F4 F5 94 42 02 5F F2 8C  A9 86 81 B8 BA E0 73 09
88 D6 19 63 B9 42 73 3F  8E 0D 9A F2 CC CD 53 BE  4E B7 60 35 E5 F1 C2 4F  81 ED AD B7 AC 0E 83 78  52 5F 30 8A B7 32 A0 85
9F 69 B1 E4 8C FD DD EA  D0 CE 5E 1B B5 5B 5C C8  24 49 7E 1B 24 B8 19 54  A1 D1 6C 84 4D E5 2C 3D  C8 99 8A 6F AF 4B 3A A1
```

```
CF 54 52 53 E8 71 A4 02  93 28 13 AB 05 77 0F CD  33 F9 B7 96 8C B1 C8 19  DF D2 8F C1 07 16 93 9C  D4 A0 2B 95 6B 22 5D F8
56 0D 81 C9 7A C7 25 71  F6 7E E8 8C 1E 09 67 3D  68 3C 0D 25 75 0A 26 AA  55 FC 6F 80 0E DD FE FA  4B 8B 95 42 1A B1 95 DA
61 36 5C 2E D1 6C CE FE  06 CA EB A0 E0 1A FC 05  BC 24 98 2A 65 6A C9 13  CE 40 07 96 9B A9 22 78  CE E9 5C D9 48 38 6E 4E
C3 AF A9 61 C7 C9 B4 F4  36 7C 5C 4F 05 B2 E1 B8  DE 0E 81 CA 27 1A 1D C8  92 CC 69 0D 6C EA 00 68  B6 96 64 45 94 6B 5E E7
23 A6 2A E9 BB DF 72 48  11 5C B4 94 AE B3 62 98  05 66 53 B0 F2 85 A5 9C  46 0F 2E 64 60 D3 E0 49  65 A4 D0 3C CD 42 A7 B3
7D 95 91 F9 CB D4 D1 55  A6 A3 ED E5 E8 E0 41 D6  B8 40 9D 92 F6 B4 C0 1C  05 7E 67 7F 98 F4 AB A7  2D 42 9D 3B 46 36 D4 83
B8 CD 1A 21 86 34 4F CB  65 FE 92 1D 50 C1 53 1F  B3 DC 80 EC B2 44 E0 6D  38 39 50 2E 06 C8 8B 2B  02 A8 54 BD B5 CB A0 40
F0 72 21 18 6E D5 C8 AF  47 44 30 20 87 A0 6C F6  F7 E1 0B 32 6E 47 72 E9  74 E0 B6 FE 95 3C 5B 95  0C 47 F8 EE 1A 50 EC A8
75 AC C7 04 B9 12 C3 E9  E6 63 08 FA D2 CA A4 71  56 12 6D 21 50 27 38 A6  EF 3A 8E 7E 03 99 BA B8  6D D7 A1 9B 20 7B 07 56
B9 CB 42 3D C9 9A B6 F1  D8 23 E3 5E 1C B8 8D 76  C1 30 DD AF E4 94 68 3B  65 1F 35 05 19 C8 F1 AD  8F CB B9 98 B2 0A F0 C6
BF B4 CB 9C 51 C0 13 75  45 D0 7D 83 6E 90 17 2C  42 C6 07 22 F9 84 40 DD  4D 7E 19 7B 49 06 B8 B2  07 A9 61 57 64 8A 6E 37
A1 57 C4 30 BF 9B FB 04  ED 0C 67 D1 52 64 27 7B  E0 C6 A1 39 67 34 D5 8D  CE 05 67 9F 3C 20 9D 4F  7D F9 6F 5B 1E B8 5B 98
D0 0C 4D BE 5E 81 E1 42  5E C7 DE AF EB 1F 62 34  17 43 94 E4 5A FC D7 F6  7F 6B 1F 6A 5A F1 71 E5  EB 0E 2D 3D 7A 26 33 CD
EF 7E 1F B8 38 C2 68 17  CC 6C 21 17 CA E4 3A D4  64 4A 82 DF 2E 0B 9C 91  6A EF 6A 57 F2 40 3A 37  A7 3C 25 48 49 0D 26 EA
56 5D CD 0D 7C 52 CA 8F  33 C3 38 DD 44 99 91 9A  EF 18 5C 0D B5 37 19 98  BD F2 21 36 21 AE 95 A8  AF 95 6F 06 73 21 3A C4
07 71 FC 25 88 57 4D 6E  B0 F6 CC 1B 25 66 11 DE  CE 7A 9E A5 59 03 B7 15  6D 83 1A 8E FC AA 89 8E  D9 A9 66 A8 A8 31 C0 88
9E 33 CC 3E 58 0A C2 10  F0 C0 BA 18 4B FB 89 E6  71 76 70 D5 48 A8 F3 02  69 08 43 EB 27 C7 C8 F0  F1 2B 3F 93 03 44 CE 5D
10 06 B8 B6 42 E4 83 BF  20 8A 46 50 DA FE 69 39  87 76 A0 73 38 D5 B0 8E  FF 49 5B 30 F4 E4 E0 A2  DD EE 23 11 BD 8E 1B 4C
83 EF 17 10 58 FC DE 8B  28 F2 68 C0 45 0F 59 77  7A 31 32 04 BF 4F 5D CC  2E 0E F5 DE C8 20 A7 8B  68 C6 FC BA 79 7E 0E D2
91 5B CB A9 3C 28 15 99  31 BF C4 18 DB 21 F6 C7  3A 9B 8C EC 7F 93 37 F1  84 43 58 91 70 22 50 D3  3A 9C 3A 66 22 87 FA D3
E6 CC 68 CD 0A 78 C3 D5  26 33 B8 78 9B AD D8 D8  80 3A C9 DD B5 FC AA BF  6C A0 26 45 2B B5 9D 9D  AA 19 D1 87 3D 0C 3E 4E
5E 68 B5 4A 67 DB 45 E6  AD 49 72 2E 31 A4 25 32  0B 87 21 9F 52 E0 52 D1  E7 C8 38 82 8A DD B1 0B  8C BF A1 E0 3A 5E 21 21
7A CF 9F DF 22 83 6F 8F  48 40 C4 CC AD 99 CE FB  E0 1A 3B 45 F0 09 4B A0  F4 F5 94 42 02 5F F2 8C  A9 86 81 B8 BA E0 73 09
8C D6 19 63 B9 42 73 3F  8E 0D 9A F2 C4 CD 53 BE  4E B7 60 35 E5 F1 C2 4F  C1 ED AD B7 AC 0E 83 78  52 7F 30 8A E7 32 A0 85
9F 69 B1 E4 8C ED DD EA  70 CE                                             A1
CF 54 52 53 E8 61 84 02  93 88 13 AB 05 77 0F CD  33 E9 A7 96 8C E1 C8 19  DF D2 8F C1 07 36 B3 9C  D4 C0 2B 95 6B 22 5D F8
56 1D 91 C9 7A 53 25 71  F6 7E E8 8C 1E 19 47 3D  68 A4 0D 25 75 0A 26 AA  55 EC 4F 80 0E DD FE FA  4B 8B 95 42 1A A1 91 DA
61 36 5C 2E D1 6C CE FE  26 CA EF A0 E0 1A FC 05  BC 24 98 2A 75 6A CD 13  CE 40 07 96 9B A9 22 78  EE E9 54 D9 48 38 6E 4E
C3 AF A9 61 E7 C9 B0 F4  36 7C 5C 4F 05 B2 E1 B8  CE 0E 89 CA 27 1A 1D C8  92 CC 69 0D 7C EA 08 E8  B6 96 64 45 94 6B 5E E7
33 A6 2C E9 BB DF 72 48  11 5C B4 94 BE B3 62 98  05 66 53 B0 F2 85 A5 9C  46 0F 2E 64 60 D3 E0 49  65 A4 D0 3C CD 42 A7 B3
7D 95 91 F9 CB D4 D1 55  A6 A3 ED E5 E8 E0 41 D6  B8 40 9D 92 F6 B4 C0 1C  05 6E 67 7F 98 F4 AB A7  2D 42 9D 3B 46 26 D4 83
B8 CD 1A 21 86 34 4F CB  65 EE 92 1D 50 C1 53 1F  B3 DC 80 EC B2 44 E0 6D  38 39 50 2E 06 C8 8B 2B  02 A8 54 BD B5 CB A0 40
F0 72 21 18 6E D5 C8 AF  47 44 30 20 87 A0 6C F6  F3 E1 0B 32 6E 47 72 E9  74 E0 B6 FE 91 3C 5B 95  0C 47 F8 EE 1A 50 EC A8
31 AC C7 04 B9 12 C3 E9  E6 63 08 FA 5A CA A4 71  56 12 6D 21 50 6F 38 A6  77 3A 8E 7E 03 99 BA B8  6D DF A1 9B B8 7B 07 56
B9 CB 42 3D C9 92 B6 F1  D8 23 E3 5E 1C B8 8D 76  C1 34 DD AF E4 94 68 3B  65 1F 35 05 19 C0 F1 AD  8F CB B9 98 B2 0A F0 C6
BF BC CB 9C 51 C0 13 75  45 D0 7D 83 6E 94 17 2C  52 C6 07 22 F9 84 40 DD  4D 7A 19 7B 49 06 B8 B2  07 A9 61 57 64 82 6E 37
A1 57 C4 30 BF 9B FB 04  ED 08 67 D1 52 64 27 7B  E0 C6 A1 39 67 3C D5 8D  CE 01 67 9F 3C 20 9D 4F  7D F9 6F 5B 1E BC 5B 98
D0 0C 4D BE 5E 85 E1 42  5E C3 DE AF EB 1F 62 34  17 47 94 E4 5A F4 D7 F6  7F 6B 1F 6A 5A F5 51 E5  EB 06 2D 3D 7A 26 33 CD
EF 3A 0F B8 38 CA 68 17  CC 6C 21 17 CA 6C 1A D4  64 4E 82 DF 2E 0B 9C 91  6A 6B 7A 57 F2 40 3A 37  A7 3C 25 48 49 89 26 EA
56 4D CD 0D 7C 52 CA 8F  33 C3 30 DD 44 89 91 9A  EF 18 5C 0D B5 37 11 98  BD D2 21 36 21 AE 95 A8  AF 95 6B 06 33 31 3A C4
07 71 FC 25 88 57 49 6E  F8 D6 CC 1B 25 66 11 DE  CE 7A 98 A5 1D 27 B7 15  6D 83 1A 8E FC AA 01 8E  5D B1 64 A8 A8 31 C0 88
9E 37 88 3E 1C 0A C2 10  F0 C0 BA 18 4B F3 89 E6  F1 76 70 D5 48 A8 F3 02  69 09 43 EB 67 C7 C8 F0  F1 2B 3F 93 03 45 CE 1D
50 06 B8 B6 42 E4 83 BF  20 88 42 10 9A FE 69 39  87 76 A0 73 38 DF B0 CE  BF 49 5B 30 F4 E4 E0 A2  DD 68 23 91 35 8E 1B 4C
83 EF 17 10 58 79 DE CB  6C F2 68 C0 45 0F 59 77  7A B7 32 84 37 4F 5D CC  2E 0E F5 DE C8 A5 A7 8B  68 C6 FC BA 79 7E 0E D2
91 5B CB A9 3C 28 15 99  31 BF C4 18 DB 21 F6 C7  3A 9B 8C EC 7F 93 37 F1  84 43 58 91 F0 22 50 D3  3A 9C 3A 66 22 8F FA D3
A6 CC 68 CD 0A 78 C3 D5  26 27 B8 78 1B AD D8 D8  80 3A C9 DD B5 F8 AA BF  F8 A0 26 45 2B B5 9D 9D  AA 11 F1 87 59 0C 3E 4E
5E 68 B5 4A 67 D3 45 E6  AD 49 72 2E 31 A4 25 32  0B 87 21 9F 52 E0 52 D1  E7 C8 38 82 8A DD B1 0B  8C BF A1 E0 3A 5E 21 21
7A CF 9F DF 22 A3 6F 8F  48 40 C4 CC AD 99 CA FB  E0 1A 3B 45 F0 09 4B A0  F4 F5 9C 42 02 5F F2 8C  A9 86 81 B8 BA E0 77 09
88 D6 19 63 B9 42 73 3F  8E 0D 92 F2 CC CD 53 BE  4E B7 60 35 E5 F1 C2 4F  81 ED AD B7 AC 0E 83 78  52 5F 30 8A B7 32 A0 85
9F 69 B1 E4 8C FD DC EA  D0 CE 5E 1B B5 5B 5C C8  24 49 7F 1B 24 B8 19 54  A1 D1 6C 84 4D E5 2E 3D  C8 D9 8A 6F AF 4B 3A A1
CF 54 73 53 E8 21 A4 02  93 28 13 AB 05 77 1D CD  33 69 B7 96 8C B1 C8 19  DF D2 9D C1 07 26 93 9C  D4 A0 2B 95 6B 22 5D F8
56 1D 81 C9 7A C7 25 71  F6 7E E9 8C 1E 19 67 3D  68 3C 0D 25 75 0A 24 AA  55 EC 6F 80 0E DD FE FA  4B 8B 97 42 1A A1 95 DA
61 36 5C 2E D1 6C CC FE  26 CA EB A0 E0 1A FC 05  BC 24 98 2A 75 6A C9 13  CE 40 07 96 9B A9 22 78  EE E9 5C D9 48 38 6E 4E
C3 AF A9 61 E7 C9 B4 F4  36 7C 5C 4F 05 B2 E1 B8  CE 0E 81 CA 27 1A 1D C8  92 CC 69 0D 7C EA 00 E8  B6 96 64 45 94 6B 5E E7
33 A6 2A E9 BB DF 72 48  11 5C F4 94 BE B3 62 98  05 66 53 B0 F2 85 E5 9C  46 0F 2E 64 60 D3 E0 49  65 A4 50 3C CD 46 A7 B3
7D 95 91 F9 CB 54 D1 55  A6 A7 EC E5 E8 E0 41 D6  B8 00 9D 92 F6 B4 C0 1C  05 7E 67 7F 98 F4 AB A7  2D 42 9D 3B 46 36 D4 83
B8 CD 1A 21 86 34 4F CB  65 FE 92 1D 50 C1 53 1F  B3 DC 80 EC B2 44 E0 6D  38 39 50 2E 06 C8 8B 2B  02 A8 54 BD B5 CB A0 40
F0 72 21 18 6E D5 C8 AF  47 44 30 20 87 A0 6C F6  F3 E1 0B 32 6E 47 72 E9  74 E0 B6 FE 91 3C 5B 95  0C 47 F8 EE 1A 50 EC A8
31 AC C7 04 B9 12 C3 E9  E6 63 08 FA 5A CA A4 71  56 12 6D 21 50 2F 38 A6  77 3A 8E 7E 03 99 BA B8  6D DF A1 9B B8 7B 07 56
B9 CB 42 3D C9 92 B6 F1  D8 23 E3 5E 1C B8 8D 76  C1 34 DD AF E4 94 68 3B  65 1F 35 05 19 C0 F1 AD  8F CB B9 98 B2 0A F0 C6
BF BC CB 9C 51 C0 13 75  45 D0 7D 83 6E 94 17 2C  52 C6 07 22 F9 84 40 DD  4D 7A 19 7B 49 06 B8 B2  07 A9 61 57 64 82 6E 37
A1 57 C4 30 BF 9B FB 04  ED 08 67 D1 52 64 27 7B  E0 C6 A1 39 67 3C D5 8D  CE 05 67 9F 3C 20 9D 4F  7D F9 6F 5B 1E B8 5B 98
D0 0C 4D BE 5E 85 E1 42  5E C7 DE AF EB 1F 62 34  17 47 94 E4 5A FC D7 F6  7F 6B 1F 6A 5A F5 71 E5  EB 0E 2D 3D 7A 26 31 CD
EF 3A 1F B8 38 C2 68 17  CC 6C 20 17 CA 6C 3A D4  64 4A 82 DF 2E 0B 9E 91  6A 6B 6A 57 F2 40 3A 37  A7 3C 24 48 49 81 26 EA
56 5D CD 0D 7C 52 CB 8F  33 C7 38 DD 44 99 91 9A  EF 18 5E 0D B5 3F 19 98  BD F2 21 36 21 AE 94 A8  AF 9D 6F 06 33 21 3A C4
07 71 FE 25 88 57 4D 6E  F8 F6 CC 1B 25 66 11 DE  CE 7A 9E A5 1D 03 B7 15  6D 83 1A 8E FC AA 89 8E  5D A9 66 A8 A8 31 C0 88
9E 37 CC 3E 1C 0A C2 10  F0 C0 BA 18 4B F3 89 E6  F1 76 70 D5 48 A8 F3 02  69 09 43 EB 67 C7 C8 F0  F1 2B 3F 93 03 45 CE 1D
50 06 B8 B6 42 E4 83 BF  20 88 46 10 9A FE 69 39  87 76 A0 73 38 DF B0 CE  BF 49 5B 30 F4 E4 E0 A2  DD 68 23 91 35 8E 1B 4C
83 EF 17 10 58 79 DE CB  6C F2 68 C0 45 0F 59 77  7A B7 32 84 37 4F 5D CC  2E 0E F5 DE C8 A5 A7 8B  68 C6 FC BA 79 7E 0E D2
91 5B CB A9 3C 28 15 99  31 BF C4 18 DB 21 F6 C7  3A 9B 8C EC 7F 93 37 F1  84 43 58 91 F0 22 50 D3  3A 9C 3A 66 22 8F FA D3
A6 CC 68 CD 0A 78 C3 D5  26 27 B8 78 1B AD D8 D8  80 3A C9 DD B5 F8 AA BF  F8 A0 26 45 2B B5 9D 9D  AA 11 D1 87 59 0C 3E 4E
5E 68 B5 4A 67 D3 45 E6  AD 49 72 2E 31 A4 25 32  0B 87 21 9F 52 E0 52 D1  E7 C8 38 82 8A DD B1 0B  8C BF A1 E0 3A 5E 21 21
7A CF 9F DF 22 83 6F 8F  48 40 C0 CC AD 99 CE FB  E0 1A 3B 45 F0 09 4B A0  F4 F5 94 42 02 5F F2 8C  A9 86 81 B8 BA E0 73 09
88 D6 19 63 B9 42 72 3F  8E 0D 9A F2 CC CD 53 BE  4E B7 61 35 E5 F1 C2 4F  81 ED AD B7 AC 0E 82 78  52 5F 30 8A B7 32 A0 85
9F 69 B3 E4 8C ED DD EA  D0 CE 5E 1B B5 5B 55 C8  24 59 7E 1B 24 B8 19 54  A1 D1 6D 84 4D E5 2C 3D  C8 99 8A 6F AF 4B 3A A1
```

Figure D.3: Sent and Received Messages for the Case with $k1 = k2 = (1, -1, -1, 1, 1)$ in the Laboratory

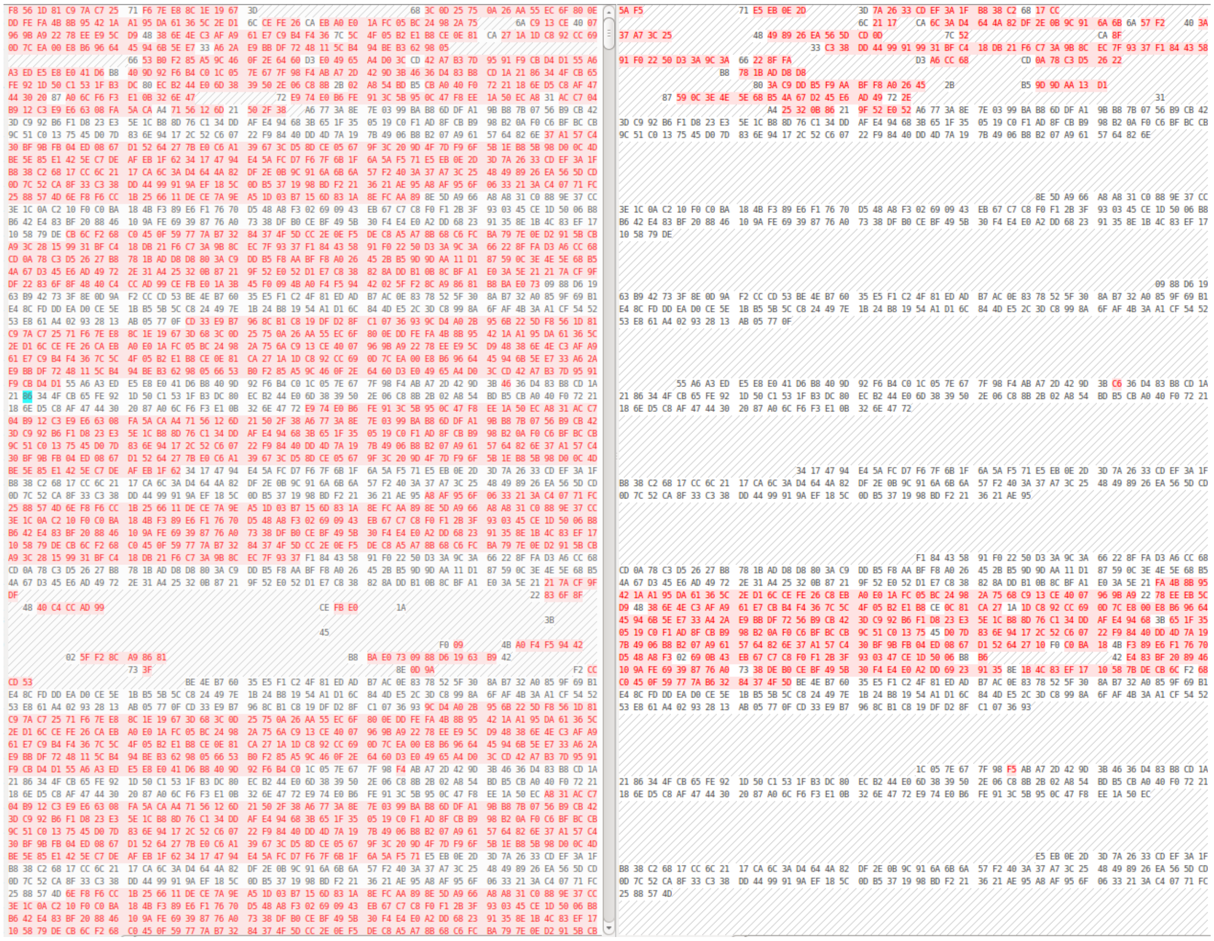


Figure D.4: Sent and Received Messages for the Case with $k1 = k2 = (1, -1, 1, 1, 1, -1)$ in the Laboratory

# Appendix E

# Proof of Theorem 1

*Proof.* Use the same notations as in Lemma 2, denote

$$\Omega = \{\mathbf{a} : \mathbf{a} = (1, [0]^l, 1, \cdots) \in G(h), n \leq l < 2n\}.$$

Since $\Omega \subset G(h)^*$ and $\Omega \cap (G(f) \cup G(g)) = \emptyset$, we have

$$\Omega \subset (G(f)^* \oplus G(g)^*). \tag{E.1}$$

Moreover, for $0 \leq i < N$, we have

$$G_i \cap \Omega \neq \emptyset \iff [0]^n \in G_i[n] \iff \forall \mathbf{a} \in G_i, [0]^n \in \mathbf{a}[n].$$

Denote

$$\mathcal{I} = \{i : 0 \leq i < N, G_i \cap \Omega \neq \emptyset\}.$$

Based on Lemma 2 and Equation (E.1), we have

$$|\mathcal{I}| \leq |\Omega|, \tag{E.2}$$

where the inequality holds iff $\exists i \in \mathcal{I}$ satisfying $|G_i \cap \Omega| > 1$.

$M$-sequence of degree $n$ has $n$ degrees of the freedom. The multiplication of any two $m$-sequences of the same degree $n$ has $2n$ degrees of freedom. The fixed bits at the beginning of those elements in $\Omega$ are $n+i, i = 2, 3, 4, \ldots, n+1$ respectively. The corresponding degree of freedom of those elements are $2n-(n+i), i = 2, 3, 4, \ldots, n$ and 1 respectively. In brief, we have

$$\begin{aligned} |\Omega| &= 1 + \sum_{i=2}^{n} 2^{2n-(n+i)} \\ &= 1 + 2^n \sum_{i=2}^{n} 2^{-i} \\ &= 1 + 2^n(1/2 - 2^{-n}) \\ &= 1 + 2^{n-1} - 1 \\ &= 2^{n-1} \end{aligned} \tag{E.3}$$

Consequently, from Equation (E.2) and Equation (E.3), we have

$$|\mathcal{I}| \le |\Omega| = 2^{n-1} \tag{E.4}$$

Finally, from Lemma 2 and Equation (E.4), we could have

$$\begin{aligned} |coll(f,g)| &= |\{\mathbf{z} : \mathbf{z} \in G(f)^* \oplus G(g)^*, [0]^n \in \mathbf{z}[n]\}| \\ &= |\{G_i : 0 \le i < N, [0]^n \in G_i[n]\}| \cdot N \\ &= |\mathcal{I}| \cdot N \\ &\le 2^{n-1}N, \end{aligned}$$

Thus, we have

$$P_{coll}(f,g) = |coll(f,g)|/N^2 \le 2^{n-1}/N.$$

This completes the proof. □

# Appendix F

# Proof of Lemma 3

*Proof.* For $l > 0$, denote

$$\Lambda(l) = \{\mathbf{a} : \mathbf{a} \in \{0,1\}^l, \mathbf{a} = \mathbf{a}^{-1}\},$$

where $\mathbf{a}^{-1}$ is given by reversing all the elements of $\mathbf{a}$. $\Lambda(l)$ indeed consists of all the length-$l$ binary symmetrical sequences. In addition, denote

$$\Lambda = \cup_{l>0}\Lambda(l).$$

With the same notations as in Theorem 1 (replace $g$ by $f^{-1}$), $\forall \mathbf{a} \in G(h)^*$, if $\Lambda \cap \mathbf{a}[2n] \neq \emptyset$, there exists an integer $j$ satisfying $0 \leq j < N$ and $(L^j\mathbf{a})[N-n, 2n] \in \Lambda$. In this case, we have $(L^j\mathbf{a})[N-n, 2n] = (L^j\mathbf{a})^{-1}[N-n, 2n]$. In addition, since $h(x) = f(x)f^{-1}(x) = h^{-1}(x)$, we have $(L^j\mathbf{a}), (L^j\mathbf{a})^{-1} \in G(h)^*$. As the result, $(L^j\mathbf{a})[n, N-n-1] = (L^j\mathbf{a})^{-1}[n, N-n-1]$, because there is no more degree of freedom after fixed $2n$ bits at $(L^j\mathbf{a})[N-n, 2n] = (L^j\mathbf{a})^{-1}[N-n, 2n]$. Therefore, we have

$$L^j\mathbf{a} = (L^j\mathbf{a})^{-1}. \tag{F.1}$$

If $j$ is not unique, there exists $k \neq N-n$ satisfying $0 \leq k < N$ and $(L^j\mathbf{a})[k, 2n] \in \Lambda$. Then, we have $(L^j\mathbf{a})[k, 2n] = (L^j\mathbf{a})[2N-k-2n, 2n]$ based on (F.1). In this case, a contradiction happens because $k \not\equiv 2N-k-2n \mod N$. Thus, $j$ is unique if given $\mathbf{a}$, implying that

$$|\Lambda \cap \mathbf{a}[2n]| \leq 1, \forall \mathbf{a} \in G(h)^*. \tag{F.2}$$

In the following, we complete the proof by proving that

$$|\Lambda \cap \mathbf{a}[2n]| = 1, \forall \mathbf{a} \in G(f)^* \oplus G(f^{-1})^*. \tag{F.3}$$

Since $f(x) \neq f^{-1}(x)$, we have

$$\mathbf{a} \nsim \mathbf{a}^{-1}, \forall \mathbf{a} \in G(f)^* \cup G(f^{-1})^*. \tag{F.4}$$

Then, based on (F.1) and (F.4), we have $\Lambda \cap (G(f)^* \cup G(f^{-1})^*)[2n] = \emptyset$. Note that $\Lambda(2n) \subset G(h)[2n]$. Therefore, we have

$$|\Lambda \cap (G(f)^* \oplus G(f^{-1})^*)[2n]| = |\Lambda(2n)| - 1 = N. \tag{F.5}$$

Based on (F.2) and (F.5), we have

$$|\Lambda \cap G_i[2n]| = 1, 0 \leq i < N.$$

Thus, (F.3) holds. This completes the proof. □

# Appendix G

# Proof of Theorem 2

*Proof.* With the same notations as in Theorem 1, we have

$$\Omega = \{\mathbf{a} : \mathbf{a} = (1, [0]^l, 1, \cdots) \in G(h), n \leq l < 2n\},$$

where

$$\begin{gathered} G(h) = G(f) \oplus G(f^{-1}) = \{\mathbf{a} + \mathbf{b} : \mathbf{a} \in G(f), \mathbf{b} \in G(f^{-1})\} \\ f(x) \neq f^{-1}(x) \in \mathcal{P}_n(x), \text{ and } h(x) = f(x)f^{-1}(x) \\ \Omega \subset (G(f)^* \oplus G(j^{-1})^*), \end{gathered}$$

and

$$\mathcal{I} = \{i : 0 \leq i < N, G_i \cap \Omega \neq \emptyset\}.$$

$\forall \mathbf{a} \in \Omega$, let $l(\mathbf{a})$ be the number of the consecutive zeros starting from $a_1$, i.e., $\mathbf{a}[0, 2 + l(\mathbf{a})] = (1, [0]^{l(\mathbf{a})}, 1)$. In addition, based on Lemma 3, there exists an unique integer $j(\mathbf{a})$ satisfying $0 \leq j(\mathbf{a}) < N$ and $L^{j(\mathbf{a})}\mathbf{a} = (L^{j(\mathbf{a})}\mathbf{a})^{-1}$. In this case, we have $(L^{j(\mathbf{a})}\mathbf{a})[N - j(\mathbf{a}), 2 + l(\mathbf{a})] = (L^{j(\mathbf{a})}\mathbf{a})[j(\mathbf{a}) - l(\mathbf{a}) + N - 2, 2 + l(\mathbf{a})] = (1, [0]^{l(\mathbf{a})}, 1)$. Thus, we have

$$L^{2j(\mathbf{a}) - l(\mathbf{a}) + N - 2}\mathbf{a} \in \Omega.$$

Let

$$A = \{\mathbf{a} : \mathbf{a} \in \Omega, \mathbf{a} = L^{2j(\mathbf{a}) - l(\mathbf{a}) + N - 2}\mathbf{a}\}.$$

$\forall i \in \mathcal{I}$, if $G_i \cap (\Omega \setminus A) \neq \emptyset$, then $\forall \mathbf{a} \in G_i \cap (\Omega \setminus A)$. Let $\mathbf{b} = L^{2j(\mathbf{a})-l(\mathbf{a})+N-2}\mathbf{a}$, then we have $l(\mathbf{b}) = l(\mathbf{a})$ and $j(\mathbf{b}) \equiv j(\mathbf{a}) - (2j(\mathbf{a}) - l(\mathbf{a}) + N - 2) \mod N$. Thus, we have $L^{2j(\mathbf{b})-l(\mathbf{b})+N-2}\mathbf{b} = \mathbf{a} \neq \mathbf{b}$, implying $\mathbf{b} \in G_i \cap (\Omega \setminus A)$ and $|G_i \cap (\Omega \setminus A)| \geq 2$. Furthermore, we have

$$|\mathcal{I}| \leq \frac{|\Omega \setminus A|}{2} + |A| = 2^{n-2} + \frac{|A|}{2}. \tag{G.1}$$

Now, we focus on $|A|$. Let

$$\begin{aligned} B &= \{\mathbf{a} : \mathbf{a} \in G(h)^*, \mathbf{a} = \mathbf{a}^{-1}, \mathbf{a}[N - \lceil n/2 \rceil, 2\lceil n/2 \rceil] = [0]^{2\lceil n/2 \rceil}\}, \\ C &= \{\mathbf{a} : \mathbf{a} \in G(h)^*, \mathbf{a} = \mathbf{a}^{-1}, \mathbf{a}[2^{n-1} - 1 - \lfloor n/2 \rfloor, 2\lfloor n/2 \rfloor + 1] = [0]^{2\lfloor n/2 \rfloor + 1}\}. \end{aligned}$$

Then, we have

$$\begin{aligned} \forall \mathbf{a} \in A \Rightarrow \mathbf{a} &= L^{2j(\mathbf{a})-l(\mathbf{a})+N-2}\mathbf{a} \\ &\Rightarrow 2j(\mathbf{a}) - l(\mathbf{a}) + N - 2 \equiv 0 \mod N \\ &\Rightarrow j(\mathbf{a}) \equiv \begin{cases} (l(\mathbf{a}) + 2)/2 \mod N & l(\mathbf{a}) \text{ is even,} \\ (l(\mathbf{a}) + N + 2)/2 \mod N & l(\mathbf{a}) \text{ is odd.} \end{cases} \\ &\Rightarrow \begin{cases} [0]^{l(\mathbf{a})} = (L^{j(\mathbf{a})}\mathbf{a})[N - \frac{l(\mathbf{a})}{2}, l(\mathbf{a})] & l(\mathbf{a}) \text{ is even,} \\ [0]^{l(\mathbf{a})} = (L^{j(\mathbf{a})}\mathbf{a})[2^{n-1} - \frac{1+l(\mathbf{a})}{2}, l(\mathbf{a})] & l(\mathbf{a}) \text{ is odd.} \end{cases} \\ &\Rightarrow \begin{cases} L^{j(\mathbf{a})}\mathbf{a} \in B & l(\mathbf{a}) \text{ is even,} \\ L^{j(\mathbf{a})}\mathbf{a} \in C & l(\mathbf{a}) \text{ is odd.} \end{cases} \end{aligned} \tag{G.2}$$

$\forall \mathbf{a} \neq \mathbf{b} \in A$ with $l(\mathbf{a}) \equiv l(\mathbf{b}) \mod 2$, we have

$$\operatorname{mod}(j(\mathbf{a}) - j(\mathbf{b}), N) = \operatorname{mod}(\frac{l(\mathbf{a}) - l(\mathbf{b})}{2}, N) \in [0, n) \cup (N - n, N). \tag{G.3}$$

From Equation (G.3), if

$$\operatorname{mod}(j(\mathbf{a}) - j(\mathbf{b}), N) = 0,$$

we have

$$L^{\bmod (j(\mathbf{a})-j(\mathbf{b}),N)}\mathbf{a} = \mathbf{a} \neq \mathbf{b}.$$

Additionally, if

$$\operatorname{mod}(j(\mathbf{a}) - j(\mathbf{b}), N) \in (0, n),$$

the $L^{\text{mod }(j(\mathbf{a})-j(\mathbf{b}),N)}\mathbf{a}[0,1]$ bit is always equal to 0, but the $\mathbf{b}[0,1]$ bit is defined as 1, so $L^{\text{mod }(j(\mathbf{a})-j(\mathbf{b}),N)}\mathbf{a}$ and $\mathbf{b}$ are not equal. Besides, if

$$\operatorname{mod}(j(\mathbf{a}) - j(\mathbf{b}), N) \in (N - n, N),$$

the $L^{\text{mod }(j(\mathbf{a})-j(\mathbf{b}),N)}\mathbf{a}[l(b)+1,1]$ bit is always 0, but the $\mathbf{b}[l(b)+1,1]$ bit is defined as 1, so they are not equal. Finally, we have

$$L^{\text{mod }(j(\mathbf{a})-j(\mathbf{b}),N)}\mathbf{a} \neq \mathbf{b} \Rightarrow L^{j(\mathbf{a})}\mathbf{a} \neq L^{j(\mathbf{b})}\mathbf{b}. \tag{G.4}$$

Denote $A_e = \{\mathbf{a} : \mathbf{a} \in A, l(\mathbf{a}) \text{ is even}\}$ and $A_o = \{\mathbf{a} : \mathbf{a} \in A, l(\mathbf{a}) \text{ is odd}\}$. Based on (G.2) and (G.4), we have $|A_e| \leq |B| = 2^{\lfloor n/2 \rfloor} - 1$ and $|A_o| \leq |C| = 2^{\lceil n/2 \rceil} - 1$. Then, we have

$$|A| = |A_e| + |A_o| \leq |B| + |C| = 2^{\lfloor n/2 \rfloor} + 2^{\lceil n/2 \rceil} - 2. \tag{G.5}$$

Consequently, based on (G.1) and (G.5), we have

$$P_{coll}(f, f^{-1}) = |\mathcal{I}|/N \leq (2^{n-2} - 1 + 2^{\lfloor n/2 \rfloor - 1} + 2^{\lceil n/2 \rceil - 1})/N.$$

This completes the proof. □