A Combinatorial Approach for Frequency Hopping Schemes

Submitted by

Mwawi Mary Nyirenda

for the degree of Doctor of Philosophy

of the

Royal Holloway, University of London

2016

Declaration

I, Mwawi Mary Nyirenda, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed ..... (Mwawi Mary Nyirenda)

Date:

To my parents MacDonald and Margaret Nyirenda.

Abstract

In a frequency hopping (FH) scheme users communicate simultaneously using FH sequences defined on the same set of frequency channels. An FH sequence specifies the frequency channel to be used as communication progresses. An inherent problem for an FH scheme is interference, unintentional and intentional. Much of the existing research on the performance of FH schemes in the presence of interference is based on either pairwise mutual or adversarial interference (jamming), but not both. In this thesis, we develop a new model for evaluating the performance of an FH scheme with respect to both *group-wise mutual interference* and *jamming*, bearing in mind that more than two users may be transmitting simultaneously in the presence of a jammer.

We then analyse existing constructions of FH schemes in the new model proposed in this thesis. The FH schemes considered are optimal in the well-known Lempel-Greenberger or Peng-Fang bounds. We estimate the group-wise mutual interference using pairwise mutual interference to determine the performance of these FH schemes. Further, we note that these FH schemes do not withstand a jammer for a long period of time.

An FH scheme in which we can determine the minimum number of places an FH sequence can be successfully used in the presence of mutual interfering FH sequences can be designed from a cover-free code. We study and specify a jammer model for cover-free codes. We examine necessary and desirable additional properties of cover-free codes that can mitigate against jamming. We conclude that while MDS codes are ideal cover-free codes for mitigating against jamming, MDS codes also do not withstand a jammer for an extended period.

Finally, we propose an efficient and secure FH scheme. We consider the use of pseudorandomness in an FH scheme based on Latin squares and how it affects the resistance of an FH scheme against a jammer. We conclude that in order to have a guarantee of transmission, as well as withstand a jammer for a long time, FH schemes should minimize group-wise mutual interference and possess some form of pseudorandomness.

Acknowledgement

I wish to thank my supervisors Dr Siaw-Lynn Ng and Prof. Keith Martin for their suggestions, never ending patience and support throughout my research and when I was writing this thesis. Words are not enough to express my gratitude.

I am thankful to my friends and family for their moral support and understanding. To Chimwemwe, Tiwonge and Vinjeru for keeping me company. To my office mates, thank you for the talks we had on graph theory, coding theory and pseudorandomness, as well as the chit-chat during tea breaks in the common room.

I would like to thank Prof. John Ryan for the MSc in Coding and Cryptography which offered the basis for my PhD. Thanks to Prof. Ed. Shaefer for suggesting that I should apply to Royal Holloway for this PhD.

My studies and stay could not be possible had it not been for Schlumberger Faculty for the Future scholarship. Thank you for trusting me that I could manage to do research in cryptography and information security.

Last but not least, I would like to express my gratitude to my husband Steven and my little ones Wamaka and Walusungu. Without you around I would have been lost. You kept me going whenever I got stuck and your silly jokes kept me sane.

Contents

List of Figures

List of Tables

List of Notation

$\mathbb{Z}$	the set of integers
$\mathbb{Z}_n$	the group of integers modulo n
$\mathbb{F}_q$	a finite field with q elements
$\lfloor g \rfloor$	the largest integer less than or equal to g
$\lceil g \rceil$	the least integer greater than or equal to g
$\lvert S \rvert$	cardinality of the finite set S
$\mathcal{F}$	frequency library
$\mathcal{S}$	frequency hopping scheme
$(x_t)_{t=0}^{v-1}$	sequence of length v
(v, k, m)-FHS	frequency hopping scheme with k frequency hopping sequences of length v defined over a frequency library of size m
$Tr(\cdot)$	trace function
$Pr(x)$	the probability of an event x
$E(X)$	expected value of X

List of Abbreviations

AFH	Adaptive frequency hopping
BIBD	Balanced incomplete block design
CDMA	Code division multiple access
CRB	Cyclically resolvable balanced incomplete block design
DSSS	Direct sequence spread spectrum
FH	Frequency hopping
FH-CDMA	Frequency hopping-code division multiple access
FHMA	Frequency hopping multiple access
FHS	Frequency hopping scheme
FHSS	Frequency hopping spread spectrum
GHz	Gigahertz
IEEE	Insititute of electrical and electronics engineers
ISM	Industrial, scientific and medical
LAN	Local area network
MDS	Maximum distance separable (code)
MHz	Megahertz
OSI	Open systems interconnection (model)
PHY	Physical (layer of the OSI model)

Chapter 1

Introduction and motivation

Contents

1.1 Spread spectrum techniques

Spread spectrum is a signal transmission technique where the signal occupies a wider bandwidth than the information rate or original bandwidth. Bandwidth is the frequency width used for transmitting a signal. Figure 1.1 is an illustration of a spread spectrum communication system.

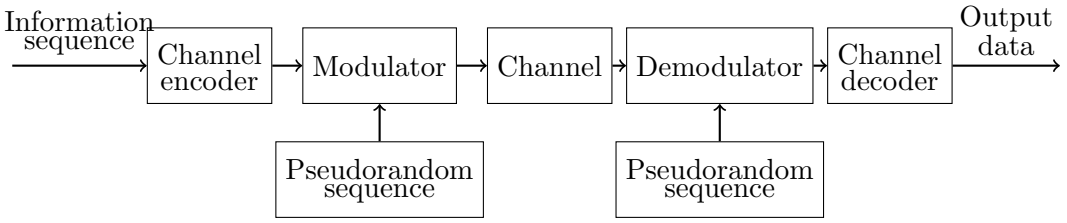

Figure 1.1: Spread spectrum communication model [3].

A transmitter sends data (information sequence) on a frequency channel. It is first encoded for the channel through the channel encoder. Spread spectrum signals are modulated twice. Modulation is the process of adding information signal on to a carrier signal (signal with constant amplitude and frequency). The first modulation is done using narrowband techniques such as *amplitude shift keying* (ASK), *frequency shift keying* (FSK) [96, 113], where the information is carried in a narrow band of frequencies. It is then modulated again using spread spectrum techniques. A spread spectrum technique uses pseudorandom sequence, called a *spreading code*, which is shared by the transmitter and receiver. The pseudorandom sequence increases the bandwidth over which the signal is to be transmitted. The modulated signal is then transmitted through the frequency channel. A receiver then does the opposite of what was done by the transmitter. To recover the information signal, the received signal is extracted using the shared pseudorandom sequence. The demodulated signal is then decoded using the channel decoder to obtain the transmitted data.

Spread spectrum communication techniques exploit the Shannon-Hartley theorem. The Shannon-Hartley theorem $C = B\log_2(1 + \text{SNR})$, provides the maximum rate

at which data can be transmitted through a noisy channel (a communication channel where information is distorted), where SNR is the *signal-to-noise ratio*, C is the *channel capacity* and B is the *bandwidth* that the signal occupies [104]. The SNR is the measure of signal strength against noise at the receiver. A large SNR means a better system, that is the signal level is much higher than the noise. However, note that even if the SNR is very low (the transmitted signal being below the noise level), communication performance can still be increased by allowing the signal to occupy a larger bandwidth than it would normally do, that is by increasing B. So, even though increasing the bandwidth B has the effect of increasing the noise and thereby reducing the SNR, the data can still be transmitted at the same channel capacity C as when B is not increased.

Despite the inherent redundancy of these techniques on the bandwidth, they have some advantages over conventional narrowband signal transmission. Some of the significant benefits are as follows [79, 81]:

- Low probability of intercept: the signal is transmitted at low power thus making it difficult to detect its presence.
- Message privacy: only intended receivers can retrieve transmitted signals because of their knowledge of the pseudorandom spreading code.
- Interference rejection: the signal is spread/transmitted over a range of frequency channels to avoid interference.

We are particularly interested in the interference rejection capabilities of spread spectrum techniques. Some of the sources of interference result from *cross talk* (other users sharing the medium), *multipath* fading (self-jamming) and jamming by adversaries. We will focus on mutual interference and jamming.

In Sections 1.1.1 and 1.1.2 a brief overview of the two fundamental spread spectrum techniques: *direct sequence* and *frequency hopping* spread spectrum are given respectively.

1.1.1 Direct sequence spread spectrum (DSSS)

Direct sequence spread spectrum (DSSS) is a technique where data is spread directly by combining it with a pseudorandom sequence called a *spreading code* [50]. The spreading code defines redundant bits that are transmitted for each information data bit. This improves the resistance of the transmitted data against interference, as well as the reliability of the received data in the event that it is corrupted during transmission. The combined signal is then used to modulate a radio frequency carrier. The size of the spreading code determines the *processing gain*, which is a measure of performance advantage of spread spectrum over ordinary narrowband signals. It is also defined as the ratio of the spread signal to that of the unspread signal.

The IEEE 802.11b standard [5] defines 14 overlapping 22MHz channels for DSSS on the 2.4GHz industrial, scientific and medical (ISM) band. Since the channels overlap, they can cause co-channel interference. However the 2.4GHz ISM band can have a maximum of three non-overlapping DSSS systems together, as shown in Figure 1.2.

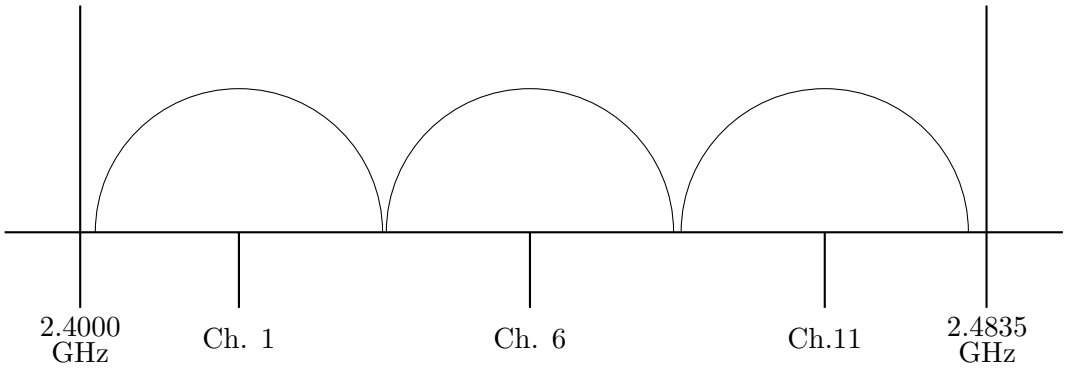

Figure 1.2: Direct sequence spread spectrum model [1].

A set of transmitters, each employing a particular spreading code and using the same communication channel simultaneously, form a *code division multiple access* (CDMA) channel access system. The CDMA technology is used, for example, in global positioning systems (GPS) and the Universal Mobile Telecommunications System (UMTS), for 3rd generation mobile communication.

1.1.2 Frequency hopping spread spectrum (FHSS)

The second spread spectrum method considered, *Frequency hopping spread spectrum* (FHSS), is where the spreading code is a *frequency hopping (FH) sequence*, that specifies the frequency channels on which data is transmitted. Data is transmitted on different radio frequency channels as transmission progresses.

A pseudorandom sequence can be used to generate an FH sequence. The main requirement for a transmitter and receiver to communicate is that they need to be on the same frequency channel at the same time. The receiver has to stay synchronised with the sender to generate the pseudorandom sequence and eventually the FH sequence. When both the sender and receiver derive the FH sequence, they can commence communication. The receiver knows which channel to tune to and the *dwelling time* on each channel, which is the amount of time spent on each radio frequency channel before hopping onto the next channel in the FH sequence. The pseudorandom sequence being used can be kept secret or not. In the latter case the choice of which FH sequence being used is kept secret. Otherwise an attacker can establish the FH sequence and jam subsequent transmissions.

Figure 1.3 shows FHSS signals of two communications A and B. The y-axis and x-axis represent frequency channels and time respectively. In the first time period, communications A and B are on channels seven and two respectively. In the fifth time period both communications A and B are on channel one and the signals interfere.

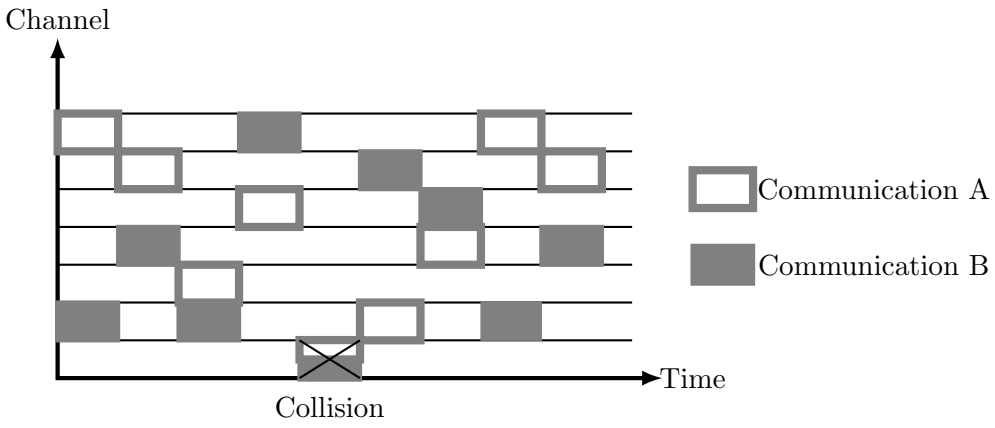

Figure 1.3: Frequency hopping spread spectrum example [2].

The IEEE 802.11 standard [5] employs 79 non-overlapping 1MHz channels for FH sequences in the 2.4GHz ISM band. It is widely used in signal transmission such as Wi-Fi, Bluetooth and ultrawideband (UWB) communications [53, 33, 90]. Frequency hopping spread spectrum can also be used in a multiple access system (see Section 1.1.4).

1.1.3 Comparison of frequency hopping and direct sequence spread spectrum techniques

In this section we compare FHSS and DSSS techniques with respect to: narrowband interference rejection, collocating systems, data rates, multipath immunity and finally the near/far problem.

- *Narrowband interference rejection:* narrowband interference is unwanted signal that is narrower than the wanted, ordinarily modulated signal. Consider a DSSS system in the presence of narrowband interference. At the receiver, the interfering signal is spread with the spreading code applied by the receiver while the transmitter's signal is despread. When both the interfering signal and the transmitted data signal goes through a process of removing the interfering signal called filtering, a small part of the interfering signal remains in the bandwidth of the data signal [41]. The interfering signal now appears as noise. As long as the signal-

to-noise ratio is above a defined threshold, the receiver will successfully retrieve and demodulate the legitimate transmitted signal. The resistance of DSSS to a narrowband interference is dependent on the strength of the interfering signal. In FHSS when a channel hop is experiencing interference, then demodulation of a signal may not be successful (depending on the interference-signal-ratio). However if there is no interference on the next jump then data can be successfully retrieved. Further, FHSS was introduced to mitigate interference from unauthorised users of a communication system on the assumption that the unauthorised users have no knowledge of the FH sequences being used [83]. Therefore it is crucial that the interfering signal does not hop in synchronisation with the transmitter's signal. So, in DSSS there is narrowband interference suppression while in FHSS we have interference avoidance.

- *Collocating systems:* applications that use FHSS have the advantage of putting more systems in the same area than DSSS. By definition a DSSS signal occupies a larger bandwidth compared to FHSS channels. The distance between non-interfering wide band frequencies is also large in DSSS. As the total ISM unlicensed band is 83.5MHz wide (2.4GHz - 2.4835GHz), the number of DSSS systems that can be put together without causing interference with each other is thus small, 3 for DSSS and 26 for FHSS.

- *Data rates:* in practice DSSS is often favoured over FHSS for its speed. The data rate for FHSS, 2Mbps, is lower than that for DSSS, 7Mbps. So, users seek applications that offer high data rates.

- *Multipath immunity:* DSSS systems are sensitive to delays as the signals are transmitted at higher data rates than FHSS signals. Multiple copies of signals are received, which are shifted versions of the transmitted signals. Therefore receivers have more difficulty demodulating transmitted signals in DSSS systems. However, there are ways in which the delayed spread signals can be controlled

[93].

- *Near/far problem:* this is the ability of a receiver to be able to retrieve a signal from the intended transmitter in the presence of other foreign transmitters in the proximity of the receiver. The issue is how well can a receiver acquire signals from the intended transmitters in the presence of other more powerful signals from other transmitters. FHSS receivers operate well in such conditions where the foreign transmitters only hop to some of the radio frequency channels visited by legitimate transmitters. On the other hand DSSS systems fare less well.

In conclusion, the choice of which spread spectrum technology to use depends on the environment in which it is deployed.

1.1.4 Frequency hopping in applications requiring multiple access

A set of FH sequences form a *frequency hopping scheme* (FH scheme). An FH scheme is used in a *frequency hopping multiple access*[1] (FHMA) system, where a number of users employ FH sequences which are defined on the same set of frequency channels. Each transmitter-receiver pair that are to communicate in an FHMA system share an FH sequence and change the frequency channels in synchronisation. In this thesis we use the term FH scheme to mean an FHMA.

Mutual interference occurs when two or more transmitters use the same frequency channel simultaneously, which can result in signal loss. *Pairwise mutual interference* is when two users mutually interfere with each other. When interference comes from adversarial sources then it is called *jamming*. The adversary in this context is called a *jammer*. It is desirable that an FH scheme be constructed such that interference from both other users of the system, as well as adversaries, is minimised.

In Chapter 2 we describe the system model of an FH scheme, as well as the effect of the presence of adversarial interference.

[1] Frequency hopping code-division multiple access (FH-CDMA) is a variant of FHMA that employs both FHSS and DSSS. See [92, 105] for a description of FH-CDMA.

1.1.5 Example: frequency hopping in IEEE 802.11 wireless LAN

In this section we look at how FH sequences are employed in IEEE 802.11 wireless local area metworks (LAN) [5]. We consider the FH sequences in this standard for the following reasons:

1. An FH sequence transmits at maximum transmission rate in the presence of other FH sequences.

2. Although FH sequences in this standard of wireless LAN are labelled as obsolete, they are still being used in hybrid frequency hopping-direct sequence spread spectrum systems [105].

3. The FH sequences in this standard provides a motivation for a scheme we consider briefly in Section 1.2.3 and in more detail in Chapter 5, which also achieves the maximum transmission capacity in the presence of other FH sequences.

The IEEE 802.11 wireless LAN standard [5] describes FH sequences and how they are employed in wireless LANs in the unlicensed ISM bands. We mentioned in Section 1.1.2 that the standard defines 79 non-overlapping frequency channels, each 1 MHz wide. The IEEE standard defines the total number of frequency channels that can be used in different geographical locations: 23 for Japan, 27 for Spain, 35 for France and 79 for China, North America, as well as Europe. However, to avoid co-channel interference it defines a minimum hop distance of 6 channels. Further, to minimise mutual interference there are three sets of FH sequences, each comprised of 26 FH sequences. Therefore, in terms of multiple access, a maximum of up to 26 users can be placed in the same geographical area.

The standard describes four ways in which FH sequences can be determined. When users are in a regulatory domain (channels in the 2.4 GHz spectrum that are regulated by the country in which they are used) they can use a predefined FH scheme. Otherwise, they use some algorithms known as hyperbolic congruence code (HCC) and

the extended HCC (EHCC) [66, 75]. Lastly, randomly generated FH sequences shared between a transmitter-receiver pair can also be used. We consider these FH schemes in more detail in Chapter 3.

All but the randomly generated FH sequences have the following property. The channels used at each point in time by all the FH sequences in the FH scheme are distinct, that is a channel does not appear on more than one FH sequence at a time. We will describe a similar FH scheme in Section 1.2.3 and Chapter 5.

1.2 Overview of existing constructions of frequency hopping sequences

In this section we present a brief summary of some FH schemes that exist in the literature. The goal of most of the existing constructions is either to minimise pairwise mutual interference or improve the resistance of adversarial interference of FH sequences, but not both. This motivated us to identify the two interference aspects of FH schemes, which we then incorporated into a combinatorial framework in order to analyse the performance of FH schemes. Most of the FH schemes' constructions described in this section will be discussed in more detail in Chapter 3 by considering them in our proposed model.

1.2.1 Constructions minimizing pairwise mutual interference

Much research in the literature focuses on mitigating the problem of pairwise mutual interference. Optimality of FH sequences, and in general optimality of FH schemes, is often defined in terms of the well-known bounds on Hamming correlation developed by Lempel and Greenberger in [55], (Lemma 2.2.5) and by Peng and Fan in [77], (Theorem 2.2.11). In their seminal paper Lempel and Greenberger developed the well-known Lempel-Greenberger bound, a lower bound for maximum Hamming auto-correlation of FH sequences. Peng and Fan on the other hand gave a lower bound for the maximum

Hamming correlation of an FH scheme which takes into account both the Hamming auto- and cross-correlation of FH sequences. We describe these bounds in Chapter 2.

Most of the existing constructions of FH sequences use mathematical structures in algebra, combinatorial designs, codes, as well as recursive constructions from other sets of FH schemes. We now consider a sample of such constructions, differing in the mathematical structures they use, as well as giving different parameters with respect to the length of the FH sequences and the number of channels used in the FH scheme.

Algebraic contructions. Several researchers have used the algebraic linear transformation of other sequences, theory of cyclotomy, as well as trace functions to construct FH sequences.

Lempel and Greenberger [55] developed the well-known lower bound on Hamming correlation. They also constructed an FH scheme using algebraic transformation of m-sequences whose FH sequences achieve their bound.

Chu and Colbourn [19] provided some of the early work on construction of FH sequences using cyclotomy. The authors developed FH sequences over a prime field meeting the Lempel-Greenberger bound. Several researchers have since then generated FH sequences over prime power fields and with different FH scheme parameters.

Ge, Miao and Yao [37] used trace functions to construct FH sequences optimal in the Lempel-Greenberger bound.

Combinatorial constructions. Fuji-Hara, Miao and Mishima [35] provided several combinatorial constructions of FH sequences optimal in the Lempel-Greenberger bound using affine geometries, cyclic designs and difference families. The authors provided a correspondence between FH sequences and partition type difference packings.

Codes. Sarwate [91] provided a correspondence between FH sequences and cyclic codes. A cyclic code can be obtained from an FH scheme by taking all the FH sequences in the FH scheme together with all the cyclic shifts of each FH sequence. On the other

hand, an FH scheme can be obtained from a cyclic (linear) code by considering a single codeword from each of the equivalence classes of the code.

Note that this construction based on obtaining a representative codeword from each equivalence class of a code was also considered by Ding, Fuji-Hara, Fujiwara, Jimbo and Mishima [27]. Further the authors provided upper bounds on the number of FH sequences in an FH scheme from coding theory bounds: these are the Singleton, Plotkin, sphere-packing and Johnson bounds on FH sequences. Optimality in these bounds does not mean optimality in the Peng-Fan or Lempel-Greenberger bounds as the latter are on the Hamming correlation of FH sequences. For instance, a $[q^{m-1}/q-1, n-m, 3; q]$-linear code, q a prime power, m a positive integer with $\gcd(m, q) = 1$, is optimal in the sphere-packing bound for FH sequences but not optimal in the Lempel-Greenberger bound.

Recursive constructions. Apart from constructing FH schemes using algebraic, combinatorial structures and codes, some researchers have also explored using known FH schemes to obtain new ones.

Chung, Han and Yang [21] used interleaving techniques to obtain FH sequences optimal in the Peng-Fan bound.

Cyclic difference matrices have also been used by Ding et al. [27], as well as Fuji-Hara et al. [35] to obtain an FH scheme by a recursive construction.

Pseudorandom construction. The Bluetooth 2010 standard [4] describes the generation of pseudorandom FH sequences. Bluetooth devices uses *adaptive frequency hopping* (AFH) spread spectrum, where a controller can eliminate frequency channels from the given set of frequency channels that are experiencing interference in the course of communication. The goal of AFH spread spectrum is to improve the co-existence of Bluetooth devices with other users, not using AFH spread spectrum, but operating on the same ISM band. So, if there are no interfering devices, Bluetooth's AFH spread spectrum reverts back to an FH scheme with a full set of frequency channels.

1.2.2 Constructions improving resistance against adversarial interference

Interference originating from unauthorised entities where signals are deliberately transmitted to interfere with legitimate transmission is called *adversarial interference* or *jamming*. We discuss an adversarial interference model further in Chapter 2. Here we briefly describe the work of Emek and Wattenhofer [31]. These researchers considered FH sequences used in the presence of adversarial interference.

Emek and Wattenhofer [31] constructed FH sequences as random walks on an expander graph. The authors considered a single pairwise communication where subsequent channels for transmission are included in the data transmitted. An adversary can eavesdrop and jam a fraction of the available frequency channels.

Two adversarial models were considered: in the first model, an adversary can only acquire information about the channel that was used in previous time slots after a certain number of time slots have lapsed, but not the transmitted data. In the second model an adversary has knowledge of both. Knowledge of the transmitted messages is vital since information of the subsequent frequency channels to be used is transmitted in the messages. At any time slot, the transmitted data is guaranteed a successful transmission with probability at least $1 - \theta - \epsilon$ where θ is the fraction of the channels an adversary jams and ϵ is a security parameter that defines the resilience of the FH sequence. However, it is not clear what happens if more than one pair (transmitter/receiver) of communication occurs simultaneously. We consider this construction in more detail in Section 3.2.

1.2.3 Combined approach constructions

In Sections 1.2.1 and 1.2.2 we described constructions of FH schemes whose performance measure considers minimizing either the pairwise mutual interference or improving resistance against adversarial interference, but not both. In this section we consider schemes that suggest a combined approach to analyse the performance of FH schemes.

Combinatorial construction. Bag, Ruj and Roy [9] used Latin squares with pseudorandomness to obtain an FH scheme. We note that this scheme can be obtained from the IEEE 802.11 FH sequences described in Section 1.1.5, with the added feature of pseudorandomness. All legitimate FH sequences in this FH scheme share a single pair of secret pseudorandom numbers (keys) before the start of communication which are used for a specified number of time slots. The adversary can eavesdrop and jam at most a certain number of the frequency channels in the frequency library. So, the authors considered communication in the presence of both other mutual interfering devices, as well as adversarial interference.

We point out that this construction has the following good features:

- The FH sequences constructed achieve a maximum transmission capacity without adversarial interference. That is, in the presence of only mutual interference each transmitter can communicate successfully at all time slots.
- The channels in the FH sequences are randomized by secret pseudorandom numbers which are then used for the entire duration (specified length) of the FH sequences. Our study of cover-free codes in Chapter 4 shows that indeed we do need pseudorandomness as it improves the resistance of an FH scheme against adversarial interference. This scheme motivates our discussion in Chapter 5 where we explore FH schemes with maximum transmission and improved resistance against an adversary.

However, we note that the constructed FH scheme is unsatisfactory in several aspects:

- By using Latin squares to design the FH scheme, the number of FH sequences is restricted by the number of frequency channels in the frequency library, that is, the two must be the same. Therefore the maximum number of FH sequences to be used in an FH scheme is restricted.

- The authors assume that devices cannot leak information about the frequency channels they are using and thus the adversary has no knowledge of active frequency channels. However, in their adversarial model they state that the adversary is capable of eavesdropping, inserting messages and jamming. It is not clear what information the devices can leak and in turn what the adversary can obtain from eavesdropping. In practice however it is assumed that an adversary can acquire frequency channel information, and in some instances the messages being transmitted on those frequency channels.

- In their analysis of the performance of the FH scheme Bag et al. [9] conclude that FH sequences achieve maximum transmission capacity in the presence of an adversary. It was shown in [73] that an adversary only needs to eavesdrop at a single time slot to obtain the pair of secret shared pseudorandom keys. Acquiring the secret keys enables the adversary to derive legitimate FH sequences and thus interfere with any FH sequence of its choice. This is discussed in more detail in Section 5.3.

Pseudorandom construction. In the FH sequences discussed thus far, a transmitter and receiver need to share an FH sequence. Strasser, Pöpper, and Čapkun [102] suggests uncoordinated FHSS. They propose using a random FH sequence between a transmitter and a receiver, in the sense that the pair of communicating users do not share an FH sequence but both randomly select a frequency channel to transmit/receive independently. To improve successful communication, a transmitter hops among frequency channels at a higher rate than a receiver. Further, the sender and receiver do not use all the frequency channels in the frequency library to increase the receiver's chances of listening on a frequency channel being used by the transmitter. It was shown that with positive probability the transmitter and receiver communicate in the presence of both mutual interference, as well as an adversary that eavesdrops and interferes on a subset of frequency channels in the given set of frequency channels.

As mentioned in their research work, uncoordinated FHSS provides a way of establishing keys for the generation of FH sequences in situations where the transmitter and receiver are not known to each other before commencing communication. After establishing common FH sequences to be used, the transmitter and receiver then use coordinated FHSS, that is, they follow the shared FH sequence to communicate. In our work we make the assumption in Chapter 2 that a transmitter and receiver have the means to establish a common FH sequence and only focus on its construction.

In an uncoordinated FH scheme as the transmitter has to hop among several frequency channels within a specified time period, while the receiver dwells on a single frequency channel within the same time period, they only transmit and listen successfully for a small fraction of the time when compared to coordinated FH schemes.

1.3 Our contributions

The majority of the research on the performance of FH schemes in the presence of interference is based on pairwise mutual interference. We have considered briefly some such FH schemes in Section 1.2.1. However, keeping in mind that in an FH scheme more than two users can be transmitting simultaneously in the presence of an adversary, this renders the pairwise mutual interference criterion inadequate. The inadequacy of the pairwise criterion was discussed in Wang and Bhargava [110] in that possibly more than one user can be using a frequency channel at the same time however the authors did not consider adversarial interference. Further, Wang and Bhargava consider FH sequences used in conjunction with error correcting codes. It was concluded that FH schemes should be designed in such a way that the probability of more than one user being at a particular frequency channel is minimised. Note that none of the FH schemes considered in Section 1.2.1 consider adversarial interference. In this thesis, we evaluate the performance of an FH scheme with respect to both *group-wise mutual interference* and *adversarial interference*. This framework was introduced in [73].

An overview of our four major contributions is as follows:

1. We develop a combinatorial framework for an FH scheme in Chapter 2. In this model we consider the performance of an FH scheme in the presence of both group-wise mutual interference and adversarial interference.

2. In Chapter 3 we investigate existing constructions of FH sequences in our model. We study in detail the mathematics behind these FH schemes. We note that most of these FH schemes are optimal in the well-known bounds developed by either Lempel and Greenberger [55] or by Peng and Fan [77]. These bounds are based on pair-wise Hamming correlation. However we want to explore the performance of the existing FH schemes in the proposed model of Chapter 2 and determine connections amongst some of them. We consider FH schemes constructions based on the following: random walks, difference packing, m-sequences, cyclotomic classes, trace functions, Reed-Solomon codes, Latin squares and we also consider recursive constructions.

3. We discuss a correspondence between a cover-free code and an FH scheme in Chapter 4. We note that when a cover-free code is considered as an FH scheme, a user can successfully transmit in at least a specified fraction of time in the presence of a given number of interfering FH sequences. To the best of our knowledge, this is the first time this correspondence has been highlighted. A cover-free code however provides no additional information for use of the FH sequences in the presence of adversarial interference. Therefore, we seek to determine these additional properties of cover-free codes that mitigate adversarial interference activities. Finally, we discuss the limitations of cover-free codes against a jammer, and we propose the use of pseudorandomness to improve resistance against a jammer.

4. In Chapter 5 we discuss employing pseudorandomness in an FH scheme. From the discussions of Chapter 3 and 4 we know that given an FH scheme we can estimate the effect of mutual interference by using Hamming group-wise mutual

interference or as given directly when the FH scheme is a cover-free code. However in order to withstand an adversary for a longer time (period) FH sequences should possess some form of pseudorandomness. So, we propose an efficient and secure FH scheme that employs Latin squares with pseudorandomness.

1.4 Summary

In this chapter we introduced the theory of spread spectrum technologies. We looked at some of the types of spread spectrum techniques, in particular direct sequence and frequency hopping spread spectrum techniques. Further, we introduced a frequency hopping multiple access system and a frequency hopping scheme. Finally, we considered some existing constructions of frequency hopping schemes and their performance measures. We pointed out a deficiency of previous works: bearing in mind that more than two users can be transmitting simultaneously in the presence of an adversary, the pairwise mutual interference based analysis is inadequate. Therefore in our work we evaluate the performance of a frequency hopping scheme with respect to both *group-wise mutual interference* and *adversarial interference*.

Chapter 2

System and attacker model

Contents

2.1 Introduction

Communication is a process that involves at least two entities, a transmitter and receiver, together with the medium through which they communicate. As presented in Chapter 1, in the literature most researchers analyse the performance of FH sequences in terms of pairwise mutual interference only, or adversarial interference, and very few have considered both pairwise mutual and adversarial interference. We pointed out that there exists a gap in the analysis of FH sequences, as well as giving the shortcomings of some of the previous constructions. In this chapter we propose a new model of analysing the performance of FH sequences.

In Section 2.2 we present the definitions and notation that will be used in this thesis. We introduce a measure of pairwise mutual interference, the Hamming correlation, which is the basis for analysing the performance of most FH sequences that exist in the literature. Section 2.2 also presents a review of bounds that exist in the literature which are based on the Hamming correlation of FH sequences. We consider the bounds developed by Lempel and Greenberger [55], as well as those of Peng and Fan [77]. In analysing the Peng-Fan bounds in detail we make the observation that optimality should be defined in terms of only one of the bounds and not both.

In Sections 2.3 through 2.5 we present the main contribution of this chapter: we develop a combinatorial framework for analysing the performance of an FH scheme in a multiple access communication system in the presence of a jammer. In Sections 2.3 and 2.4 we describe the system model where we consider only group-wise mutual interference and its effect on an FH scheme. In Section 2.5 we introduce an adversary into the system model, that is we describe the attacker model in an FH scheme. In Section 2.5 we also provide the measures of the performance of an FH scheme in the presence of both group-wise mutual and adversarial interference.

Finally, we summarise the chapter in Section 2.6.

2.2 Hamming correlation

2.2.1 Definition

Let $\mathcal{F} = \{ f_0, f_1, \ldots, f_{m-1} \}$ be a set of m frequency channels; $\mathcal{F}$ is called a *frequency library*. For simplicity, we assume a one-to-one mapping between the frequency channels in $\mathcal{F}$ and a set of m elements, that is we write i for f_i, $0 \leq i \leq m-1$.

Definition 2.2.1. *A **frequency hopping** (**FH**) **sequence** over a frequency library $\mathcal{F}$ is a sequence $X = (x_t)_{t=0}^{v-1}$ (or $X = (x_t)$ if there is no ambiguity) of length v, $x_t \in \mathcal{F}$.*

A FH sequence $X = (x_0, x_1, \ldots, x_{v-1})$ specifies that at time slot t a user of the FH sequence transmits on frequency channel x_t.

Definition 2.2.2. *A (v, k, m)-**frequency hopping scheme**, denoted (v, k, m)-FHS, is a set $\mathcal{S} = \{ X_i : 0 \leq i \leq k-1 \}$ of size k, where X_i is an FH sequence of length v defined over a frequency library $\mathcal{F}$ of size m.*

Given a (v, k, m)-FHS, the use of the same frequency channel at the same time by two FH sequences (or more) causes *interference*. *Pairwise mutual interference* is where two FH sequences in a (v, k, m)-FHS interfere with each other. Formally, Definition 2.2.3 describes pairwise mutual interference as pairwise Hamming correlation or simply Hamming correlation.

Definition 2.2.3. *Let $\mathcal{S}$ be a (v, k, m)-FHS and $X, Y \in \mathcal{S}$, $X = (x_0, x_1, \ldots, x_{v-1})$ and $Y = (y_0, y_1, \ldots, y_{v-1})$. The **Hamming correlation** $H_{X,Y}$ at relative time delay τ between X and Y is:*

$$H_{X,Y}(\tau) = \sum_{i=0}^{v-1} h(x_i, y_{i+\tau}), \qquad 0 \leq \tau < v, \tag{2.1}$$

where

$$h(x_i, y_i) = \begin{cases} 1 & \text{if } x_i = y_i, \\ 0 & \text{if } x_i \neq y_i. \end{cases}$$

Consider two FH sequences X, Y. At relative time delay τ there is mutual interference between X and Y when $h(x_i, y_i) = 1$ at time slot i and no mutual interference otherwise. The Hamming correlation in Equation (2.1) gives the total number of positions at which the FH sequences X, Y interfere.

Note that in Definition 2.2.3 the operations on indices are performed modulo v. When $X = Y$ we write $H_X(\tau)$ for $H_{X,X}(\tau)$ and this is the *Hamming auto-correlation* of X.

Definition 2.2.4. *Let $\mathcal{S}$ be a (v, k, m)-FHS and $X, Y \in \mathcal{S}$.*

1. *The **maximum out-of-phase Hamming auto-correlation** on an FH sequence X is:*

$$H(X) = \max_{1 \leq \tau < v} \{H_X(\tau)\}. \tag{2.2}$$

2. *The **maximum Hamming cross-correlation** between any two distinct FH sequences X and Y is:*

$$H(X, Y) = \max_{0 \leq \tau < v} \{H_{XY}(\tau)\}. \tag{2.3}$$

3. *The **maximum Hamming correlation** on FH sequences X, Y is:*

$$M(X, Y) = \max\{H(X), H(Y), H(X, Y)\}. \tag{2.4}$$

2.2.2 Bounds

As discussed in Chapter 1, performance of FH sequences has mainly been analysed in terms of Hamming correlation. Some researchers developed bounds on the measure of Hamming correlation for FH schemes. We first look at one of the early notable work of such bounds investigated in Lempel and Greenberger's 1974 seminal paper [55]. Then we consider a generalisation of Lempel and Greenberger's bounds provided by Peng and Fan [77].

Lempel and Greenberger [55] defined optimality of FH sequences in the following way.

1. $X \in \mathcal{S}$ is *optimal* if $H(X) \leq H(X') \ \forall \ X' \in \mathcal{S}$.
2. $X, Y \in \mathcal{S}$ is an *optimal pair* if $M(X,Y) \leq M(X',Y') \ \forall \ X', Y' \in \mathcal{S}$.
3. A subset $\mathcal{C} \subset \mathcal{S}$ is an *optimal family* if every pair of distinct members of $\mathcal{C}$ is an optimal pair.

Further, Lempel and Greenberger [55] developed a lower bound on $H(X)$ for any FH sequence X. We state the lemma and its proof. First, we need to define the multiplicity of a frequency channel on an FH sequence. Let X be an FH sequence defined over $\mathcal{F}$. For any frequency channel $f_j \in \mathcal{F}$, we define the following. Define

$$\mu_X(f_j) = \sum_{i=0}^{v-1} h(x_i, f_j) \tag{2.5}$$

where

$$h(x_i, f_j) = \begin{cases} 1 & \text{if } x_i = f_j, \\ 0 & \text{if } x_i \neq f_j. \end{cases}$$

to be the number of times that frequency channel f_j appears on an FH sequence $X \in \mathcal{S}$.

Lemma 2.2.5 (Lempel-Greenberger bound I, [55], Lemma 4)**.** *For every sequence $X = (x_t)$ of length v over $\mathcal{F}$, $|\mathcal{F}| = m$,*

$$H(X) \geq \frac{(v-r)(v+r-m)}{m(v-1)}, \tag{2.6}$$

where $v \equiv r \mod m$.

Proof. The sum of the Hamming auto-correlation of the FH sequence X can be written

in terms of its average out-of phase Hamming auto-correlation:

$$\sum_{\tau=0}^{v-1} H_{XX}(\tau) = v + \sum_{\tau=1}^{v-1} H_{XX}(\tau) \tag{2.7}$$

$$= v + (v-1)\bar{H}(Y) \tag{2.8}$$

with $\bar{H}(Y)$ the average out-of phase Hamming auto-correlation.

Next, consider the sum of the Hamming auto-correlation of an FH sequence X in terms of the multiplicity of frequency channel on X:

$$\sum_{\tau=0}^{v-1} H_{XX}(\tau) = \sum_{\tau=0}^{v-1}\sum_{j=0}^{v-1} h(x_j, x_{j+\tau})$$

$$= \sum_{f\in\mathcal{F}} [\mu_X(f)]^2. \tag{2.9}$$

From Equations (2.7) and (2.9) we have:

$$\bar{H} = \frac{1}{v-1}\left(\sum_{f\in\mathcal{F}} [\mu_X(f)]^2 - v\right).$$

Let

$$\beta = \min_{\mu_X}\left\{\sum_{f\in\mathcal{F}} [\mu_X(f)]^2\right\} \tag{2.10}$$

where the minimization is over all non-negative integer-valued distribution sequences $\mu_X = \{\mu_X(f_i) : f_i \in \mathcal{F}, 0 \le i \le m-1\}$ on $\mathcal{F}$ that satisfy the constraint:

$$\sum_{f\in\mathcal{F}} \mu_X(f) = v. \tag{2.11}$$

Without loss of generality, assume:

$$\mu_X(f_0) \le \mu_X(f_1) \le \ldots \le \mu_X(f_{m-1}).$$

Then μ_X is a distribution that minimises β if $\mu_X(f_{m-1}) - \mu_X(f_0) \leq 1$.

Further, with constraint (2.11), the minimisation β can be achieved when the distribution μ_X is nearly uniform:

$$v = am + r, \qquad 0 \leq r < m, \qquad a \in \mathbb{Z}_+.$$

Then the following distribution can be used to obtain β:

$$\begin{cases} \mu_X(f_0) = \mu_X(f_1) = \ldots = \mu_X(f_{m-r-1}) = a, \\ \mu_X(f_{m-r}) = \mu_X(f_{m-r+1}) = \ldots = \mu_X(f_{m-1}) = a+1. \end{cases} \tag{2.12}$$

We have:

$$\beta = \frac{1}{m}[(v-r)(v+r) + mr].$$

Therefore:

$$\begin{aligned} H(X) &\geq \bar{H}(X) \\ &\geq \frac{1}{v-1}(\beta - v) \\ &= \frac{(v-r)(v+r-m)}{m(v-1)}. \end{aligned}$$

□

Lempel and Greenberger [55] also developed a lower bound on $M(X,Y)$ for FH sequences with particular parameters.

Lemma 2.2.6 (Lempel-Greenberger bound II, [55], Lemma 5)**.** *For every pair of sequences X, Y of length $v = p^n - 1 \geq 2$ over $\mathcal{F}$, $|\mathcal{F}| = p^i$, $1 \leq i \leq n$,*

$$M(X,Y) \geq p^{n-i}. \tag{2.13}$$

There are also the Peng-Fan bounds which were developed in [77]. Before discussing

the Peng-Fan bounds, we make further correlation definitions of an FH scheme.

Definition 2.2.7. *Let $\mathcal{S}$ be a (v, k, m)-FHS and $X, Y \in \mathcal{S}$.*

1. *The **maximum Hamming auto-correlation** of an FH scheme $\mathcal{S}$ is:*

$$H_a(\mathcal{S}) = \max\{H(X) : X \in \mathcal{S}\}.$$

2. *The **maximum Hamming cross-correlation** of an FH scheme $\mathcal{S}$ is:*

$$H_c(\mathcal{S}) = \max\{H(X, Y) : X, Y \in \mathcal{S}, X \neq Y\}.$$

3. *The **maximum Hamming correlation** of an FH scheme $\mathcal{S}$ is:*

$$H_m(\mathcal{S}) = \max\{H_a(\mathcal{S}), H_c(\mathcal{S})\}. \tag{2.14}$$

Peng and Fan [77] developed some bounds for the maximum Hamming correlation of an FH scheme. We are going to give the proof of the bounds. We start with the Lemmas that lead to Theorem 2.2.11 on the bounds. Let $\mathcal{S}$ be a (v, k, m)-FHS over $\mathcal{F}$, $|\mathcal{F}| = m$. Consider the sum of the Hamming correlations of two FH sequences $X, Y \in \mathcal{S}$:

$$P(X, Y) = \sum_{\tau=0}^{v-1} H_{X,Y}(\tau) \tag{2.15}$$

Lemma 2.2.8 gives an upper bound on $\sum_{X,Y \in \mathcal{S}} P(X, Y)$.

Lemma 2.2.8 ([77], Lemma 1)**.** *We have*

$$\sum_{X,Y \in \mathcal{S}} P(X, Y) \leq vk + (v-1)kH_a + (k-1)vkH_c. \tag{2.16}$$

See [77] for the proof of Lemma 2.2.8.

Lemma 2.2.9 gives the value of $\sum_{X,Y \in \mathcal{S}} P(X, Y)$ in terms of occurrences of frequency channels on an FH sequence, Equation (2.5).

Lemma 2.2.9 ([77], Lemma 2)**.**

$$\sum_{X,Y\in\mathcal{S}} P(X,Y) = \sum_{f\in\mathcal{F}} \left(\sum_{X\in\mathcal{S}} \mu_X(f) \right)^2. \tag{2.17}$$

For all integers $0, 1, 2, \ldots, m-1$, let

$$g_i = \sum_{X\in\mathcal{S}} \mu_X(f_i) \tag{2.18}$$

be the number of times that frequency channel $f_i \in \mathcal{F}$ occurs in the FH scheme $\mathcal{S}$. By definition, an FH scheme $\mathcal{S}$ is non-empty. That is, there exists at least one FH sequence in the FH scheme. Further, we can assume that each FH sequence in the (v, k, m)-FHS has frequency channels from the frequency library. Therefore, $g_i \geq 0$ for all $0 \leq i \leq m-1$. That is $g_i \in \mathbb{Z}_{\geq 0}$, g_i is a non-negative integer.

Next, we consider the lower bound on $\sum_{X,Y\in\mathcal{S}} P(X,Y)$.

Lemma 2.2.10 (Lemma 3, [77])**.** *Let $I = \lfloor vk/m \rfloor$, we have:*

$$\sum_{X,Y\in\mathcal{S}} P(X,Y) \geq \frac{v^2k^2}{m} \tag{2.19}$$

and

$$\sum_{X,Y\in\mathcal{S}} P(X,Y) \geq (2I+1)vk - (I+1)Im. \tag{2.20}$$

Proof. From Equation (2.18) and Lemma 2.2.9 we have:

$$\sum_{X,Y\in\mathcal{S}} P(X,Y) = \sum_{i=0}^{m-1} g_i^2$$

and the following constraints:

$$\begin{cases} g_i \geq 0, \\ \sum_{i=0}^{m-1} g_i = vk. \end{cases} \tag{2.21}$$

First, suppose all $g_0, g_1, \ldots, g_{m-1}$ are real numbers. We use the Lagrange's method to find the minimum on $\sum_{X,Y \in \mathcal{S}} P(X,Y)$. Let $f(g_0, g_1, \ldots, g_{m-1}) = \sum_{i=0}^{m-1} g_i^2$ and $g(g_0, g_1, \ldots, g_{m-1}) = \sum_{i=0}^{m-1} g_i$. Let λ be the Lagrange multiplier and consider the Lagrange function:

$$\begin{aligned}\mathcal{L}(g_0, g_1, \ldots, g_{m-1}, \lambda) &= f(g_0, g_1, \ldots, g_{m-1}) - \lambda \left(g(g_0, g_1, \ldots, g_{m-1}) - vk\right) \\ &= \sum_{i=0}^{m-1} g_i^2 - \lambda \left(\sum_{i=0}^{m-1} g_i - vk\right).\end{aligned}$$

Now we calculate the gradient:

$$\begin{aligned}&\bigtriangledown_{g_0, g_1, \ldots, g_{m-1}, \lambda} \mathcal{L}(g_0, g_1, \ldots, g_{m-1}, \lambda) \\ &= \left(\frac{\partial \mathcal{L}}{\partial g_0}, \frac{\partial \mathcal{L}}{\partial g_1}, \cdots, \frac{\partial \mathcal{L}}{\partial g_{m-1}}, \frac{\partial \mathcal{L}}{\partial \lambda}\right) \\ &= \left(2g_0 - \lambda, 2g_1 - \lambda, \ldots, 2g_{m-1} - \lambda, \sum_{i=0}^{m-1} g_i - vk\right).\end{aligned}$$

Then:

$$\bigtriangledown_{g_0, g_1, \ldots, g_{m-1}, \lambda} \mathcal{L}(g_0, g_1, \ldots, g_{m-1}, \lambda) = 0 \Leftrightarrow \begin{cases} 2g_0 - \lambda = 0 \\ 2g_1 - \lambda = 0 \\ \vdots \\ 2g_{m-1} - \lambda = 0 \\ \sum_{i=0}^{m-1} g_i = vk. \end{cases}$$

We have:

$$g_0 = g_1 = \ldots = g_{m-1} = \frac{\lambda}{2}.$$

Substituting into $\sum_{i=0}^{m-1} g_i = vk$, we have:

$$\begin{aligned}\sum_{i=0}^{m-1} \frac{\lambda}{2} &= vk \\ \frac{m\lambda}{2} &= vk \\ \lambda &= \frac{2vk}{m}.\end{aligned}$$

So:

$$g_0 = g_1 = \ldots = g_{m-1} = \frac{vk}{m}.$$

Therefore:

$$\begin{aligned}\sum_{X,Y \in \mathcal{S}} P(X,Y) &= \sum_{i=0}^{m-1} g_i^2 \\ &\geq \frac{v^2k^2}{m}.\end{aligned}$$

Next, suppose all $g_0, g_1, \ldots, g_{m-1}$ are non-negative. Recall we want to find the minimum of $\sum_{X,Y \in \mathcal{S}} P(X,Y)$. Let

$$\beta = \min_{g_0, g_1, \cdots, g_{m-1}} \left\{ \sum_{i=0}^{m-1} g_i^2 \right\}. \tag{2.22}$$

There exist a sequence of integers $g_0, g_1, \ldots, g_{m-1}$ such that the summand is minimum.

Without loss of generality, assume

$$g_0 \leq g_1 \leq \cdots \leq g_{m-1}.$$

It can be seen that the sequence $g_0, g_1, \ldots, g_{m-1}$ minimizes $\sum_{i=0}^{m-1} g_i^2$ when $g_{m-1} - g_0 \leq 1$. Let

$$g_i = I_i m + r_i, \qquad 0 \leq r_i < m.$$

Then:

$$\begin{aligned} vk &= \sum_{i=0}^{m-1} I_i m + r_i \\ &= m \sum_{i=0}^{m-1} I_i + \sum_{i=0}^{m-1} r_i. \end{aligned}$$

Let $\sum_{i=0}^{m-1} r_i = I_{\mathcal{S}} m + r$. Then:

$$vk = (I_{\mathcal{S}} + \sum_{i=0}^{m-1} I_i)m + r = Im + r. \tag{2.23}$$

From condition (2.21) and Equation (2.23) we have $\sum_{i=0}^{m-1} g_i = vk = Im + r$. Then the following sequence minimizes $\sum_{i=0}^{m-1} g_i^2$:

$$\begin{cases} g_0 = g_1 = \ldots = g_{r-1} = I + 1, \\ g_r = g_{r+1} = \ldots = g_{m-1} = I. \end{cases} \tag{2.24}$$

Given the sequence of non-negative integers in (2.24), the value of β is:

$$\begin{aligned} r(I+1)^2 + (m-r)I^2 &= mI^2 + 2Ir + r \\ &= (2I+1)vk - (I+1)Im. \end{aligned}$$

Therefore,

$$\sum_{X,Y \in \mathcal{S}} P(X,Y) \geq (2I+1)vk - (I+1)Im.$$

□

Theorem 2.2.11 follows from Lemma 2.2.8 and 2.2.10 with $H_m(\mathcal{S}) = \max\{H_c(\mathcal{S}), H_a(\mathcal{S})\}$.

Theorem 2.2.11 (The Peng-Fan Bounds, [77], Corollary 1)**.** *Let $\mathcal{S}$ be a (v,k,m)-FHS. Let $I = \lfloor \frac{vk}{m} \rfloor$. Then:*

$$H_m(\mathcal{S}) \geq \left\lceil \frac{(vk-m)v}{(vk-1)m} \right\rceil \tag{2.25}$$

and

$$H_m(\mathcal{S}) \geq \left\lceil \frac{2Ivk - (I+1)Im}{(vk-1)k} \right\rceil. \tag{2.26}$$

Now, we discuss the two bounds given in Lemma 2.2.11. In particular, we note that optimality should be defined only if the bound (2.26) is met. Normalising the denominators in both bounds we have,

$$\frac{(vk-m)vk}{(vk-1)km} \tag{2.27}$$

and

$$\frac{(2Ivk - (I+1)Im)m}{(vk-1)km}. \tag{2.28}$$

Substituting $I = \lfloor \frac{vk}{m} \rfloor$ in the numerator of (2.28) we have,

$$2\left\lfloor \frac{vk}{m} \right\rfloor vkm - \left\{ \left(\left\lfloor \frac{vk}{m} \right\rfloor + 1 \right) \left\lfloor \frac{vk}{m} \right\rfloor m^2 \right\}. \tag{2.29}$$

Let ε denote the fractional part of $\frac{vk}{m}$. Then (2.29) becomes:

$$2vkm\left(\frac{vk}{m} - \varepsilon\right) - \left(\frac{vk}{m} - \varepsilon + 1\right)\left(\frac{vk}{m}\varepsilon\right)m^2,$$

which reduces to:

$$\begin{aligned} &(vk)^2 - vkm - m^2(\varepsilon^2 - \varepsilon) \\ &= (vk-m)vk - m^2(\varepsilon^2 - \varepsilon). \end{aligned} \tag{2.30}$$

Note that when m divides vk then $\varepsilon = 0$ in (2.30). Therefore (2.30) and the numerator of (2.27) are the same. That is the two bounds (2.25) and (2.26) are the same when m divides vk.

On the other hand, when m does not divide vk and thus $\varepsilon \neq 0$, then we have the following. Note that $\varepsilon^2 - \varepsilon < 0$ since $0 < \varepsilon < 1$. Comparing the numerators of (2.27)

and (2.28) (which has been reduced to (2.30)) we have:

$$(vk-m)vk < (vk-m)vk - m^2(\varepsilon^2-\varepsilon).$$

We conclude that:

$$\frac{(vk-m)vk}{(vk-1)mk} \leq \frac{(vk-m)vk - m^2(\varepsilon^2-\varepsilon)}{(vk-1)mk}.$$

So,

$$\left\lceil \frac{(vk-m)vk}{(vk-1)mk} \right\rceil \leq \left\lceil \frac{(vk-m)vk - m^2(\varepsilon^2-\varepsilon)}{(vk-1)mk} \right\rceil.$$

Therefore the bound in (2.26) is better than that of (2.25).

Most researchers define optimality of FH sequences as follows.

Definition 2.2.12. *An FH sequence $X \in \mathcal{S}$ is **optimal** in the Lempel-Greenberger bound if the bound (2.6) is met.*

Definition 2.2.13. *A pair of FH sequences $X, Y \in \mathcal{S}$ is an **optimal pair** in the Lempel-Greenberger bound if the bound (2.13) is met.*

Definition 2.2.14. *A (v, k, m)-FHS, is an **optimal FH scheme** in the Peng-Fan bound if either of the bounds in Lemma 2.2.11 is met.*

Peng and Fan [77] showed that the Lempel-Greenberger bounds are special cases of the Peng-Fan bounds. Therefore optimality in the Peng-Fan bounds implies optimality in the Lempel-Greenberger bounds.

Thus far we have looked at how other researchers analyse the performance of FH sequences in terms of Hamming correlation, as well as how they define optimality of FH schemes using the Lempel-Greenberger and Peng-Fan bounds. These well-known bounds are indeed useful and simplify the question of what it means to have good FH sequences in the presence of Hamming correlation: we only need to have FH sequences such that the Hamming correlation is minimised with respect to those bounds. In our

research, however, we consider group-wise mutual interference, which will be defined in Section 2.3, and adversarial interference to be considered in Section 2.5. Our notion of optimality considers transmission capacity of a user in the presence of both group-wise mutual and adversarial interference.

2.3 System model

Consider an FHMA system. As has been previously described, in an FHMA system a set of users communicate simultaneously using FH sequences defined on the same set of frequency channels. In this thesis we consider a finite set of n users $\mathcal{N} = \{ N_i : 0 \leq i \leq n-1 \}$ communicating pairwise using a given (v, k, m)-FHS, $\mathcal{S}$.

Consider $\mathcal{S}$ a (v, k, m)-FHS over $\mathcal{F}$. The FH sequences in a (v, k, m)-FHS are used periodically. By *periodic* we mean that given an FH sequence $X = (x_0, x_1, \ldots, x_{v-1})$, then it can be used as $X' = (x_0, x_1, \ldots, x_{v-1}, x_0, x_1, \ldots)$. A user can be both a transmitter and a receiver when sending and receiving data from another user respectively.

It is outside the scope of this thesis to address how users agree on the sending and receiving FH sequences in $\mathcal{S}$. In practice an FH sequence could simply be assigned by some central controlling user, or the transmitters/receivers could have predistributed keys allowing them to choose an FH sequence in $\mathcal{S}$. So, we make the assumption that a transmitter-receiver pair can pre-agree on an FH sequence to be used in a session. A *session* is a number of pre-defined time slots. In this thesis we define a session as being made up of v time slots, that is one full length of an FH sequence. We take a *time slot* as a unit of time.

Let w, $0 \leq w < k$, be a positive integer. In any session there are $w+1$ FH sequences that are in use by legitimate users. We call these *active FH sequences*. Let $\mathcal{V} \subseteq \mathcal{S}$ be the set of $w+1$ active FH sequences. At any time slot t, $0 \leq t \leq v-1$, in a session, there are at most $w+1$ frequency channels in use, which we call *active frequency channels*. At any time slot t, let the multiset $\mathcal{F}_t = \{x_t^0, ..., x_t^{k-1}\}$ denote all

the frequency channels that appear in all the FH sequences at that time. The vector $M_t = \{a_0, ..., a_{m-1}\}$ denotes the multiplicity of each frequency channel at time slot t, where $a_i = |\{j : x_t^j = i\}|$. Let $\mathcal{F}_t^{active} = \{x_t^{i_0}, ..., x_t^{i_w}\}$ and $M_t^{active} = \{a'_0, ..., a'_{m-1}\}$ denote the multisets of active frequency channels and multiplicity of active frequency channels respectively. Note that $a'_i \leq a_i$ for all i, $0 \leq i \leq m-1$.

There is the issue of synchronisation, which is one of the challenges in an FH scheme. We make the assumption that all users start at $t = 0$ at the same time. Shifts of an FH sequence are treated as distinct FH sequences if needed.

In the literature a (v, k, m)-FHS is formed of FH sequences as follows. Some researchers construct a single FH sequence of length v over a frequency library of size m. Then, each transmitter-receiver pair starts at a particular time slot of the FH sequence. That is, a (v, k, m)-FHS contains all cyclic shifts of the single FH sequence and a particular transmitter and receiver that wish to communicate use one of these sequences [17, 23, 35, 36, 51, 55, 106]. Another way is to consider cyclic shifts of more than one FH sequence [27, 91]. Finally, another approach is to obtain k distinct FH sequences [39, 62, 72, 108]. Our analysis in this thesis covers all these ways of looking at FH sequences. We treat a FH scheme simply as a collection of FH sequences.

2.4 Effect of mutual interference on an FH scheme

In this section we discuss the performance of an FH scheme in the presence of mutual interference where an adversary is not present. As mentioned earlier, in an FH scheme where more than two users can be transmitting at the same time, the Hamming pairwise criterion which is widely used in the literature is inadequate [73, 110]. We thus introduce the *Hamming group correlation*, a parameter that measure the performance of an FH sequence in the presence of subsets of FH sequences.

Definition 2.4.1. *Let $\mathcal{S}$ be a (v, k, m)-FHS, $\mathcal{U} \subset \mathcal{S}$, $|\mathcal{U}| = w$, $0 \leq w < k$ and $X \in \mathcal{S} \backslash \mathcal{U}$. The **Hamming group correlation** $G(X, \mathcal{U})$ between the FH sequence X and the FH*

sequences in $\mathcal{U}$, is defined as the number of coordinates in X that contain the same symbols as the corresponding coordinates of some FH sequences in $\mathcal{U}$:

$$G(X,\mathcal{U}) = |\{\, x_t : \exists Y \in \mathcal{U} \text{ such that } x_t = y_t, 0 \leq t \leq v-1 \,\}|. \tag{2.31}$$

Considering a (v,k,m)-FHS as a set of k codewords of length v over $\mathcal{F}$, $|\mathcal{F}| = m$, then the Hamming group correlation, $G(X,\mathcal{U})$, coincides with the notion of group distance as defined by Jin and Blaum [46] in the context of traceability codes.

We now define the main performance measure of an FH scheme which is used throughout the remainder of the thesis, the *throughput* of an FH sequence. We use the basic throughput defined here to develop further throughput measures of an FH scheme. In the remainder of this chapter we will use the following. Let $\mathcal{S}$ be a (v,k,m)-FHS, $\mathcal{U} \subset \mathcal{S}$, $|\mathcal{U}| = w$, $\mathcal{V} \subseteq \mathcal{S}$, $|\mathcal{V}| = w+1$, $0 \leq w < k$ and $X \in \mathcal{S} \setminus \mathcal{U}$.

Definition 2.4.2. *The w-**throughput of an FH sequence** X is the rate of successful transmission in a session in the presence of FH sequences in $\mathcal{U}$,*

$$\rho_w(X,\mathcal{U}) = 1 - \frac{G(X,\mathcal{U})}{v}. \tag{2.32}$$

Note that when $w = 0$ then there is only one FH sequence being used in the communication system and the w-throughput is one. It is desirable that $\rho_w(X,\mathcal{U})$ be large, which means an FH sequence transmits at many time slots.

Ideally, we aim to construct a (v,k,m)-FHS that maximises throughput in both the average case and worst-case.

2.4.1 Average throughput

Let $\mathcal{S}$ be a (v,k,m)-FHS. We define the average w-throughput of an FH sequence, of a subset of an FH scheme and of an FH scheme.

Definition 2.4.3. *The **average** w-**throughput of an FH sequence** $X \in \mathcal{S}$ is:*

$$\bar{\rho}_w(X, \mathcal{S}) = \frac{1}{\binom{k-1}{w}} \left(\sum_{\mathcal{U} \subseteq \mathcal{S} \setminus \{X\}} \rho_w(X, \mathcal{U}) \right), \tag{2.33}$$

$|\mathcal{U}| = w$.

The average w-throughput of an FH sequence provides the average number of time slots in which an FH sequence can successfully send information if w other FH sequences in an FH scheme are being used.

Definition 2.4.4. *The **average** w-**throughput of a subset** $\mathcal{V}$ is:*

$$\bar{\rho}_w(\mathcal{V}) = \frac{1}{w+1} \left(\sum_{X \in \mathcal{V}} \rho_w(X, \mathcal{V} \setminus \{X\}) \right), \tag{2.34}$$

$|\mathcal{V}| = w + 1$.

Thus, given a $(w+1)$-subset $\mathcal{V}$ of a (v, k, m)-FHS, $\mathcal{S}$, (2.34) provides the average number of time slots in which an FH sequence $X \in \mathcal{V}$ can successfully transmit information if the other w FH sequences in $\mathcal{V}$ are also transmitting.

Definition 2.4.5. *The **average** w-**throughput of an FH scheme** $\mathcal{S}$ is the average of $\bar{\rho}_w(\mathcal{V})$, over all $(w+1)$-subset $\mathcal{V}$:*

$$\bar{\rho}_w(\mathcal{S}) = \frac{1}{\binom{k}{w+1}} \sum_{\mathcal{V} \subseteq \mathcal{S}} \bar{\rho}_w(\mathcal{V}). \tag{2.35}$$

So, (2.35) provides the average number of time slots that an FH sequence can transmit information successfully in the presence of any $(w+1)$-subset of $\mathcal{S}$.

2.4.2 Worst-case throughput

Consider $\mathcal{S}$ a (v, k, m)-FHS. We define the worst-case w-throughput of an FH sequence, of a subset of an FH scheme and of an FH scheme. We first look at the case without an

adversary. The worst-case w-throughput in the presence of an adversary will be dealt with in Section 2.5.

Definition 2.4.6. *The **worst-case w-throughput of an FH sequence** X is:*

$$\hat{\rho}_w(X, \mathcal{S}) = \min_{\mathcal{U} \subseteq \mathcal{S} \setminus \{X\}} \Big\{ \rho_w(X, \mathcal{U}) \Big\}, \tag{2.36}$$

$|\mathcal{U}| = w$.

So, given an FH sequence $X \in \mathcal{S}$, (2.36) provides the minimum number of time slots in which the FH sequence can transmit data if some w FH sequences in $\mathcal{S}$ are also in use.

Definition 2.4.7. *The **worst-case w-throughput of a subset of an FH scheme**, $\mathcal{V}$ is:*

$$\hat{\rho}_w(\mathcal{V}) = \min_{X \in \mathcal{V}} \Big\{ \rho_w(X, \mathcal{V} \setminus \{X\}) \Big\}, \tag{2.37}$$

$|\mathcal{V}| = w + 1$.

Equation (2.37) provides the minimum number of time slots in which an FH sequence $X \in \mathcal{V}$ can transmit information if w FH sequences in $\mathcal{V} \setminus \{X\}$ are in use.

Definition 2.4.8. *The **worst-case w-throughput of an FH scheme**, $\mathcal{S}$ is:*

$$\hat{\rho}_w(\mathcal{S}) = \min_{\mathcal{V} \subseteq \mathcal{S}} \Big\{ \hat{\rho}_w(\mathcal{V}) \Big\}, \tag{2.38}$$

$|\mathcal{V}| = w + 1$.

Equation (2.38) provides the minimum of the values $\rho_w(X, \mathcal{V} \setminus \{X\})$ for each possible FH sequence X and the set of w FH sequences $\mathcal{V} \setminus \{X\}$ in $\mathcal{S}$ not containing X.

A (v, k, m)-FHS, $\mathcal{S}$ with worst-case w-throughput $\hat{\rho}_w(\mathcal{S})$ will be denoted $(v, k, m; \hat{\rho}_w(\mathcal{S}))$-FHS.

Clearly ρ_w and all its associated variations takes on values in the interval $[0, 1]$. In Chapter 5 we examine FH schemes with $\hat{\rho}_w(\mathcal{S}) = 1$ for any w.

2.5 Attacker model

In both wired and wireless networks, most security issues and data recovery can be addressed by architectures in advanced higher layers of the Open Systems Interconnection (OSI) model, such as coding or cryptographic methods [13, 88, 98]. However, there are problems that exist on the lower physical (PHY) layer that may not be addressed by these higher layer solutions. In particular jamming is an example of such a threat on the PHY layer.

2.5.1 Jamming definition

In the literature [47, 58, 82, 101, 103, 107], jamming has been defined as the action of inserting, modifying or blocking messages. Interference occurs if the jamming signal is transmitted on a frequency channel that is occupied by legitimate users. A malicious user can replay or insert its own messages on the frequency channel. Further, a malicious user can modify messages by flipping bits in the transmitted messages. The receiver will get a different signal which is that of the modified message (a malicious user's signal) and not the original transmitted signal that was sent by the legitimate transmitter. In either case, if the jamming signal has a higher power then the legitimate transmitter's signal is overshadowed and this results in a modified message at the receiver's end. The actions of message inserting and modifications are executed in the higher layers of the OSI reference model and we therefore assume that they can be taken care of by higher-layer security mechanisms such as coding and cryptographic methods. In this thesis we only consider signal jamming:

Definition 2.5.1. ***Jamming*** *is defined as intentionally sending noisy signals on frequency channels to block the signal transmissions of legitimate users. It is considered as a denial-of-service attack on the physical layer. We call a malicious user that sends jamming messages a* ***jammer****.*

A jammer can further be classified according to its capabilities [78, 81, 84]:

- A *narrowband jammer* concentrates its jamming signal on a narrowband stretch of the communication spectrum.
- A *broadband jammer* generates a jamming signal that occupies a continuous set of adjacent frequency channels simultaneously, stretching over frequency ranges longer than those occupied by narrowband transmissions.

A jammer can also be classified according to its behaviour [69, 76, 112]:

- A *constant jammer* continuously sends jamming signals on the frequency channels.
- A *random jammer* switches between jamming and sleeping mode without a defined strategy. This jammer saves energy when in sleeping mode.
- A *reactive jammer* is only active when a frequency channel is active with legitimate transmissions. This jammer has to be actively eavesdropping to sense ongoing transmissions on frequency channels. Therefore, it spends more energy during eavesdropping.

2.5.2 Jamming strategy

We now describe the jamming model that is used in this thesis. Further, we develop the measures of the performance of an FH scheme in the presence of a jammer and also incorporate the presence of mutual interference.

The strategy of a jammer in this thesis is to eavesdrop and jam. It knows the frequency library $\mathcal{F}$, the (v, k, m)-FHS, $\mathcal{S}$, the current time slot t, and thus it knows $\mathcal{F}_t$ and M_t the multiset of all channels that appear in all the FH sequences and the multiplicity of each channel at time slot t respectively. It also knows $w' = w + 1$ ($0 \leq w < k$), the number of FH sequences being used in a session. However, it has no knowledge of the actual FH sequences being used if the number of active FH sequences is less than k. In this case, at each time slot it has no knowledge of $\mathcal{F}_t^{active}$ or M_t^{active}.

At each time slot a jammer has enough resources to eavesdrop on $\theta_1 m$ channels, $0 \leq \theta_1 \leq 1$. In our model we assume that by eavesdropping a jammer only finds out whether a channel is active or not, but does not acquire the information being transmitted on an active channel. We will call a jammer that eavesdrops on an active and inactive channel at a time slot, t, $0 \leq t \leq v-1$, a *lucky* and *unlucky* jammer respectively. We assume that a jammer cannot jam all the frequency channels at each time slot, but rather say it can jam $\theta_2 m$ channels, $0 \leq \theta_2 < 1$. A jammer can use the information it acquires while eavesdropping to jam on frequency channels. This adversary is denoted as a (θ_1, θ_2)-*adaptive jammer*.

Note that a (θ_1, θ_2)-adaptive jammer includes all the jammers that apply to an FH scheme. For example, a narrowband jammer can be considered as a $(\theta_1, \frac{1}{m})$-adaptive jammer, where it can eavesdrop on any number of frequency channels, $0 \leq \theta_1 \leq 1$, but can only jam on a single narrowband frequency channel. A broadband jammer can be modelled as a (θ_1, θ_2)-adaptive jammer, where $\theta_2 \geq \frac{1}{m}$, with an additional condition that it jams on $f_i, f_{i+1}, \ldots, f_{i+\theta_2 m-1}$ and $0 \leq \theta_1 \leq 1$.

At each time slot, a jammer will either send interfering signals on any random channel(s) or will choose a particular channel such that its chances of jamming an active FH sequence is improved.

A jammer can improve its chances of jamming an active frequency channel as follows. At each time slot, there are k FH sequences assumed to be equally likely over m frequency channels, and for each frequency channel i there are a_i FH sequences of that frequency channel. The probability that frequency channel i is active is

$$Prob(i \text{ is active}) = 1 - \binom{k-a_i}{w+1} \Big/ \binom{k}{w+1}. \tag{2.39}$$

The probability in (2.39) is maximum when the jammer selects a frequency channel i such that $a_i \geq a_j$ for all $i \neq j$. Therefore, if there exists some i such that $a_i \geq a_j$ for all $i \neq j$, then a jammer will choose frequency channel i to jam. A jammer can follow

this strategy at any time slot t, $0 \leq t \leq v-1$.

A jammer can also try to determine an active FH sequence. It aims to identify an active FH sequence as quickly as possible. It can then reduce the worst-case w-throughput to 0, or close to 0. We call the *jammer's search space* the set of FH sequences denoted $\mathcal{S}_t^*$, a subset of the $(v, k, m; \hat{\rho}_w(\mathcal{S}))$-FHS, which the jammer needs to look at to identify an active FH sequence at time slot t. Note that at the beginning of a session, $t = 0$, the search space is the whole FH scheme, $\mathcal{S}_0^* = \mathcal{S}$. We will denote the number of time slots it takes a jammer to determine an active FH sequence as γv, $0 \leq \gamma \leq 1$. It is desirable that γ be large. The aim of a $(v, k, m; \hat{\rho}_w(\mathcal{S}))$-FHS, $\mathcal{S}$, is to make the jammer's advantage not much better than a random guess.

Note that knowledge of $\mathcal{F}$ and $\mathcal{S}$ is a standard security assumption. For example in the IEEE 802.11 standard the frequency library and the FH scheme are publicly known [6]. It is also possible for a jammer to eavesdrop on ongoing transmissions by a communication system and learn $\mathcal{F}$ and $\mathcal{S}$.

When a signal is jammed, legitimate users hear noise and acknowledge failure of transmission. So we treat a jamming signal as an erasure.

We model a jammer's channel selection strategy for jamming as a set of FH sequences $\mathcal{J} = \{Y_i | i = 0, \ldots, \theta_2 m - 1\}$, where Y_i is an FH sequence of length v over $\mathcal{F}$.

Definition 2.5.2. *Let $\mathcal{S}$ be a (v, k, m)-FHS. Let $\mathcal{U} \subseteq \mathcal{S}$, $|\mathcal{U}| = w, 0 \leq w < k$ and $X \in \mathcal{S} \setminus \mathcal{U}$. Consider the existence of a (θ_1, θ_2)-adaptive jammer. We now define the throughput of an FH sequence in the presence of w mutual interfering FH sequences from $\mathcal{U}$, as well as jamming FH sequences from $\mathcal{J}$ similarly to Section 2.4:*

1. *The $(w, \mathcal{J})$-**throughput of an FH sequence** $X \in \mathcal{S} \setminus \mathcal{U}$:*

$$\rho_{w,\mathcal{J}}(X, \{\mathcal{U} \cup \mathcal{J}\}) = 1 - \frac{G(X, \{\mathcal{U} \cup \mathcal{J}\})}{v}, \tag{2.40}$$

is the number of time slots an FH sequence X can successfully transmit in the

presence of other w mutual interfering FH sequences from $\mathcal{U}$ and jamming FH sequences from $\mathcal{J}$.

2. *The* ***average*** $(w, \mathcal{J})$***-throughput of an FH sequence*** $X \in \mathcal{S} \setminus \mathcal{U}$*:*

$$\bar{\rho}_{w,\mathcal{J}}(X, \mathcal{S} \cup \mathcal{J}) = \frac{1}{\binom{k-1}{w}} \sum_{\mathcal{U} \subseteq \mathcal{S} \setminus \{X\}} \rho_{w,\mathcal{J}}(X, \mathcal{U} \cup \mathcal{J}), \tag{2.41}$$

is the average number of time slots in which X can successfully send information in the presence of other w FH sequences from $\mathcal{S}$, as well as jamming FH sequences from $\mathcal{J}$.

3. *The* ***average*** $(w, \mathcal{J})$***-throughput of a subset*** $\mathcal{V}$*:*

$$\bar{\rho}_{w,\mathcal{J}}(\mathcal{V}) = \frac{1}{w+1} \sum_{X \in \mathcal{V}} \rho_{w,\mathcal{J}}(X, \mathcal{V} \setminus \{X\} \cup \mathcal{J}), \tag{2.42}$$

is the mean number of time slots in which an FH sequence X from $\mathcal{V}$ can communicate successfully if other w FH sequences from $\mathcal{V} \setminus \{X\}$, as well as jamming FH sequences from $\mathcal{J}$ are present.

4. *The* ***average*** $(w, \mathcal{J})$***-throughput of an FH scheme*** $\mathcal{S}$*:*

$$\bar{\rho}_{w,\mathcal{J}}(\mathcal{S}) = \frac{1}{\binom{k}{w+1}} \sum_{\substack{\mathcal{V} \subseteq \mathcal{S} \\ |\mathcal{V}| = w+1}} \bar{\rho}_{w,\mathcal{J}}(\mathcal{V}), \tag{2.43}$$

is the overall average of time slots with respect to all $(w+1)$-subsets, in which an FH sequence can successfully transmit in the presence of other w mutual interfering FH sequences from $\mathcal{S}$ and jamming FH sequences from $\mathcal{J}$.

5. *The* ***worst-case*** $(w, \mathcal{J})$***-throughput of an FH sequence*** X*:*

$$\hat{\rho}_{w,\mathcal{J}}(X, \mathcal{S} \cup \mathcal{J}) = \min_{\mathcal{U} \subseteq \mathcal{S} \setminus \{X\}} \left\{ \rho_{w,\mathcal{J}}(X, \mathcal{U} \cup \mathcal{J}) \right\}, \tag{2.44}$$

is the lowest possible number of time slots in which an FH sequence $X \in \mathcal{S}$ can communicate in the presence of w mutual interfering FH sequences from $\mathcal{U} \subseteq \mathcal{S} \setminus \{X\}$ and other jamming FH sequences from $\mathcal{J}$.

6. *The* ***worst-case*** $(w, \mathcal{J})$***-throughput of a subset*** $\mathcal{V}$*:*

$$\hat{\rho}_{w,\mathcal{J}}(\mathcal{V}) = \min_{X \in \mathcal{V}} \{\rho_{w,\mathcal{J}}(X, \mathcal{V} \setminus \{X\} \cup \mathcal{J})\}, \tag{2.45}$$

is the least achievable number of time slots for an FH sequences $X \in \mathcal{S}$, with respect to all $(w+1)$-subsets of $\mathcal{S}$, to successfully transmit in the presence of both mutual interfering FH sequences from $\mathcal{V} \setminus \{X\}$ and jamming FH sequences from $\mathcal{J}$.

7. *The* ***worst-case*** $(w, \mathcal{J})$***-throughput of an FH scheme*** $\mathcal{S}$*:*

$$\hat{\rho}_{w,\mathcal{J}}(\mathcal{S}) = \min_{\substack{\mathcal{V} \subseteq \mathcal{S} \\ |\mathcal{V}|=w+1}} \{\hat{\rho}_{w,\mathcal{J}}(\mathcal{V})\} \tag{2.46}$$

is the minimum number of time slots every FH sequence from $\mathcal{S}$ can transmit in the presence of w FH sequences from $\mathcal{S}$ and jamming FH sequences of $\mathcal{J}$,

In this thesis, the goal of a jammer is to reduce the worst-case $(w, \mathcal{J})$-throughput of a (v, m, k)-FHS, $\mathcal{S}$.

2.5.3 Existing jamming countermeasures

In Sections 2.5.1 and 2.5.2 we have defined a jammer and its strategies. Before summarising this chapter we review jamming countermeasures that exist in the literature.

There are three countermeasures to communication jamming [81, 85, 101]:

1. *Jamming avoidance* methods involve moving out of the jamming signal's range or changing the communication medium (switching from wireless to wired communication).

2. *Jamming detection* is the action of detecting the presence of jamming activity in a communication system.

3. *Jamming mitigation* techniques minimises the effect of jamming in a communication system. Directional antennas and spread spectrum techniques are considered as jamming mitigation techniques.

Bluetooth's adaptive FHSS can be considered as a jamming detection and avoidance mechanism. As described in Chapter 1, a master user in a Bluetooth network adaptively changes the frequency library over which the FH sequences are defined by removing channels on which it experiences interference.

Note that jamming detection and jamming avoidance may not be feasible in other applications such as wired systems or wireless sensor networks. For example, moving out of jamming range may not be practical for wired systems. Further, as wireless sensors are energy constrained devices, detecting jamming will further need the use of the already limited energy resource. Further, the geographical positions of some wireless sensors cannot be changed once they have been deployed and thus not making jamming avoidance viable. In this thesis, we consider FH sequences as a jamming mitigation method.

2.6 Summary

In this chapter, we started with a review of the literature on Hamming correlation and its related bounds. Next, we have presented a new framework for analysing the performance of an FH scheme considering the presence of both mutual interference and a jammer. We have taken into account more than two users transmitting simultaneously and have considered the throughput in that setting. A jammer model was introduced in an FH scheme. The metrics for the performance of an FH scheme given the presence of both group-wise mutual interference and jamming signal were presented. We will now use the new proposed model to analyse the performance of existing FH schemes in

Chapter 3, as well as new FH schemes to be considered/proposed in Chapters 4 and 5.

Chapter 3

Investigating existing FH schemes in the new proposed model

Contents

3.1 Introduction

In Chapter 1 we introduced some constructions of FH schemes that exist in the literature whose performance is measured with respect to the well-known Lempel-Greenberger or Peng-Fan bounds. The bounds are based on Hamming correlation. In Chapter 2 we developed a new model for analysing the performance of FH schemes: provided an FH scheme, we consider the successful transmission of an FH sequence in the presence of group-wise mutual interference, as well as in the presence of an adaptive jammer. In this chapter we investigate the performance of some of the existing FH schemes constructions within the new model proposed in Chapter 2. For each FH scheme we:

1. Describe the FH scheme construction in detail;
2. Determine the Hamming group correlation and w-throughput of an FH sequence, as well as the worst-case w-throughput of the FH scheme;
3. Examine the resistance of the FH scheme against a (θ_1, θ_2)-adaptive jammer.

We also explore possible relations between various FH schemes. Some of these can be shown to be the same even though they have been constructed using different mathematical structures.

The remainder of this chapter is structured as follows. We consider existing constructions of FH schemes which use the following structures: random walks on a graph

in Section 3.2, difference packing in Section 3.3, m-sequences in Section 3.4, cyclotomy in Section 3.5, trace functions in Section 3.6, Reed-Solomon codes in Section 3.7, recursive constructions in Section 3.9. In Section 3.10 we compare the different constructions considered in this chapter with respect to their performance in the presence of both group-wise mutual interference and jamming. We summarise the chapter in Section 3.12.

3.2 Random walks on a Ramanujan graph

In [31] Emek and Wattenhofer constructed FH sequences as random walks on expander graphs, in particular on Ramanujan graphs. The authors consider a single pairwise communication where subsequent channels in an FH sequence for transmission are included in the data transmitted. The FH scheme is analysed in the presence of an adversary that can eavesdrop and jam a certain fraction of the available frequency channels. However, it is not clear what happens if more than one pair of communication occurs simultaneously. So, we consider their FH scheme in our model where we consider *both* mutual (group-wise) and adversarial interference, where the adversary can also eavesdrop and jam.

3.2.1 Random walks on a graph

Random walks are a combinatorial tool with many applications, such as models in mathematics and physics (brownian motion of particles) [111], as well as in computer science, where they are used in the generation of random samples [59]. In these applications they are attractive for their randomness. In [31] they are used to construct pseudorandom FH sequences.

We start with the basic definitions of graphs and introduce random walks on graphs, which are relevant for this construction. We refer the reader to [16, 42] for a detailed introduction to this topic.

Definition 3.2.1. *A **graph** $G = (V, E)$ is a set of **vertices** $V = \{u_0, \ldots, u_{m-1}\}$ and a set of **edges** $E = \{e_0, \ldots, e_{n-1}\}$, where $e_\kappa = (u_i, u_j) \in E$, $0 \leq \kappa \leq n-1$, is an edge between the vertices u_i and u_j, and we say that the edge (u_i, u_j) is **incident** to its endpoints u_i and u_j. Wherever an edge (u_i, u_j) exists, u_i and u_j are said to be **adjacent**.*

The graphs considered in the construction of this section will be simple graphs.

Definition 3.2.2. *A **simple graph** is an undirected graph where both multiple edges and loops are not allowed.*

Given a graph $G = (V, E)$, a *walk* in G is a finite sequence alternating vertices $u_{i_j} \in V$ and edges $e_{i_j} \in E$ in the form $(u_{i_0}, e_{i_1}, u_{i_1}, e_{i_2}, u_{i_2}, \ldots, e_{i_v}, u_{i_v})$, where for $1 \leq j \leq v$, the edge e_{i_j} is incident with the vertices $u_{i_{j-1}}$ and u_{i_j}. Less formally, a walk describes a sequence of vertices $(u_{i_0}, u_{i_1}, u_{i_2}, \ldots, u_{i_v})$, where u_{i_0} is called the *initial vertex* and u_{i_v} the *final vertex* and $u_{i_j}u_{i_{j+1}} \in E$, $0 \leq j \leq v-1$. The *length* of a walk is the number of edges in a walk. So $(u_{i_0}, e_{i_1}, u_{i_1}, e_{i_2}, u_{i_2}, \ldots, e_{i_v}, u_{i_v})$ is a walk of length v starting from vertex u_{i_0} then goes through the edge e_{i_1} to get to vertex u_{i_1} etc. until the final vertex u_{i_v}. A walk with distinct vertices is called a *path*.

A graph $G = (V, E)$ is *undirected* if for all $u_i, u_j \in V$:

$$(u_i, u_j) \in E \Leftrightarrow (u_j, u_i) \in E,$$

implying that pairs of vertices in the set of edges are not ordered. Otherwise it is called a *directed graph*. A graph is *connected* if for every pair of vertices there exist a path on the graph joining them. The construction of Emek and Wattenhofer [31] uses a connected, undirected graph.

Le $G = (V, E)$ be a connected, undirected graph with m vertices. The *degree* $d(u_i)$ of a vertex u_i is the number of edges incident with that vertex. A graph is said to be *r-regular* if each vertex has the same degree r. The *neighbourhood* of a vertex $u_i \in V$,

denoted $\mathcal{N}(u_i)$, is the set of adjacent vertices to u_i, that is $\mathcal{N}(u_i) = \{u_j \in V : (u_i, u_j) \in E\}$. We are now in a position to define a random walk on a graph.

Definition 3.2.3. *Let $G = (V, E)$ be a graph. A **random walk** is a sequence $(u_{i_0}, u_{i_1}, u_{i_2}, \ldots)$ at discrete time steps, where each $u_{i_j} \in V$, the initial vertex u_{i_0} is chosen randomly, and suppose at time t the walk is on vertex $u_{i_{t-1}}$, then a single succeeding vertex $u_{i_t} \in \mathcal{N}(u_{i_{t-1}})$ is chosen uniformly,*

$$Pr(u_{i_{t-1}}, u_{i_t}) = \begin{cases} \dfrac{1}{deg(u_{i_{t-1}})} & \text{if } u_{i_t} \in \mathcal{N}(u_{i_{t-1}}), \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

The *adjacency matrix*, $A \in \{0,1\}^{m \times m}$ of a graph is used to analyse random walks on a graph, where:

$$A(i,j) = \begin{cases} 1 & \text{if } (u_j, u_i) \in E, \\ 0 & \text{otherwise.} \end{cases}$$

Further, a *walk matrix* W of a graph is an $m \times m$ matrix provided by:

$$W(i,j) = \begin{cases} \dfrac{1}{deg(u_j)} & \text{if } (u_j, u_i) \in E, \\ 0 & \text{otherwise} \end{cases}$$

If the graph is r-regular then $W = \frac{1}{r}A$.

Example 3.2.4. *Consider $G = (V, E)$, $|V| = 6$, the 4-regular connected, undirected graph provided in Figure 3.1*

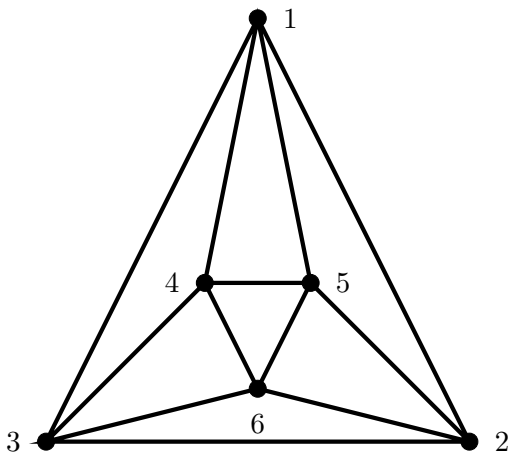

Figure 3.1: A 4-regular, connected, undirected graph on 6 vertices.

The adjacency matrix A for the graph in Figure 3.1 is,

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

and the walk matrix is,

$$W = \begin{pmatrix} 0 & 1/4 & 1/4 & 1/4 & 1/4 & 0 \\ 1/4 & 0 & 1/4 & 0 & 1/4 & 1/4 \\ 1/4 & 1/4 & 0 & 1/4 & 0 & 1/4 \\ 1/4 & 0 & 1/4 & 0 & 1/4 & 1/4 \\ 1/4 & 1/4 & 0 & 1/4 & 0 & 1/4 \\ 0 & 1/4 & 1/4 & 1/4 & 1/4 & 0 \end{pmatrix}.$$

At time t the matrix $W^t(G)$ is described as follows. The (i, j)-entry of $W^t(G)$ is the

probability that a random walk of length t starting at vertex u_j ends at vertex u_i. We will denote this probability as $W^t(G)(i,j) = Pr^t_{u_j}(u_i)$. At $t = 0$, $Pr^t_{u_j}(u_i) = 1/\deg(u_j)$. From the example graph in Figure 3.1, the matrix $W^5(G)$ corresponding to random walks of length 5 is,

$$W^5(G) = \begin{pmatrix} 0.157 & 0.173 & 0.173 & 0.173 & 0.173 & 0.157 \\ 0.173 & 0.157 & 0.173 & 0.157 & 0.173 & 0.173 \\ 0.173 & 0.173 & 0.157 & 0.173 & 0.157 & 0.173 \\ 0.173 & 0.157 & 0.173 & 0.157 & 0.173 & 0.173 \\ 0.173 & 0.173 & 0.157 & 0.173 & 0.157 & 0.173 \\ 0.157 & 0.173 & 0.173 & 0.173 & 0.173 & 0.157 \end{pmatrix}.$$

So, a random walk of length 5 starting at vertex v_6 will be at vertex v_3 with probability 0.173.

We end this section by defining Ramanujan graphs, the graphs used by Emek et al. [31] to construct random walks.

Definition 3.2.5. *Let $G(V, E)$ be an r-regular connected, undirected graph on m vertices. Let*

$$\omega(G) = max\{\lambda_1, |\lambda_{m-1}|\},$$

*where $\lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_{m-1}$ are the eigenvalues of the adjacency matrix of G. If $\omega(G) \leq 2\sqrt{r-1}$ then G is a **Ramanujan graph**.*

Ramanujan graphs belong to a class of important graphs called *expander graphs*. Expander graphs are r- regular graphs that are highly connected while, at the same time, sparse (having very few edges). A graph with m vertices is said to be highly connected if the minimum number of edges whose deletion results in a disconnected graph is greater than $m/2$. We will not provide a formal definition of expander graphs because the details are outside our scope. For more information on expander graphs and Ramanujan graphs we refer the reader to [24, 26, 45, 60].

Several researchers have established the existence of Ramanujan graphs. Existence of an infinite family of $(p+1)$-regular Ramanujan graphs, whenever p is a prime number and $p \equiv 1(\mod 4)$ is shown by Lubotzky, Phillips and Sarnak [60]. It is also known that d-regular complete graphs and and complete bipartite graphs are Ramanujan graphs [64]. Marcus, Spielman and Srivastava [64] proved the existence of bipartite Ramanujan graphs of every degree and every number of vertices. Further constructions of Ramanujan graphs can be found in [18, 48, 63, 65, 68, 80].

3.2.2 Random walks as an FH scheme

We now describe the random walk in detail as an FH scheme.

Construction 3.2.6. *Consider $G = (V, E)$ an r-regular, connected, undirected graph (not necessarily a Ramanujan graph) on m vertices. We consider vertices of the graph as frequency channels. A transmitter and receiver start at some channel $u_{i_0} \in V$ chosen deterministically and take a random walk of length v. As the graph is r-regular, at each point in the walk there are r choices, u_{i_j} such that $u_{i_j} \in \mathcal{N}(u_{i_{j-1}})$, for a channel in the succeeding point of the walk. However, note that $u_{i_j} \neq u_{i_{j-1}}$ since the graph has no loops. Therefore, there are r^{v-1} sequences with u_{i_0} as a first vertex to visit. Thus there are $m \times r^{v-1}$ possible walks on G when considering all vertices $u_i \in V$, $0 \leq i \leq m-1$ as the starting vertex of a random walk. Consider a random walk as an FH sequence, then the set of all possible walks on G is a $(v, m \times r^{v-1}, m)$-FHS, $\mathcal{S}$, where $|\mathcal{S}| = m \times r^{v-1}$, $|\mathcal{F}| = m$.*

The properties of the $(v, m \times r^{v-1}, m)$-FHS obtained using random walks on a graph are as follows. Consider any $v-1$ consecutive time slots, for simplicity, $0, \ldots, v-2$. Any frequency channel in $\mathcal{F}$ appear r^{v-1} number of times at time slot 0. Next consider any r^{v-1} FH sequences with a particular frequency channel in $\mathcal{F}$ that appear at time slot 0. Then at time slot 1, some r frequency channels in $\mathcal{F}$ each appears r^{v-2} number of times on the r^{v-1} FH sequences of interest. If we continue in this manner, we have that on the last time slot $v-1$ we remain with r distinct frequency channels.

Example 3.2.7. *Consider the 4-vertex, 2-regular, connected, undirected graph in Figure 3.2:*

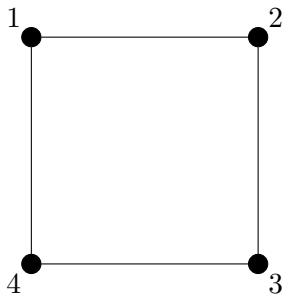

Figure 3.2: A 2-regular, connected, undirected graph on 4 vertices.

We have $\mathcal{F} = \{1, 2, 3, 4\}$. *A* $(4, 32, 4)$*-FHS can be constructed using this graph. Let* $v_{i0} = 1$ *be the initial vertex of walks,* $0 \leq i \leq 7$*, then all the FH sequences of length* 4 *starting with frequency channel* 1 *are:* $X_0 = (1, 2, 3, 2)$, $X_1 = (1, 4, 3, 2)$, $X_2 = (1, 2, 1, 2)$, $X_3 = (1, 4, 1, 2)$, $X_4 = (1, 2, 3, 4)$, $X_5 = (1, 2, 1, 4)$, $X_6 = (1, 4, 1, 4)$, $X_7 = (1, 4, 3, 4)$.

Note that there are three other sets, each with 8 sequences, each set with frequency channels $2, 3, 4$ *at the first time slot.*

3.2.3 Correlation

Hamming correlation

In this section we consider the Hamming correlation of FH sequences on the graph introduced in Section 3.2.2. We point out that Emek et al. [31] considered only adversarial interference and not mutual interference.

Let $G = (V, E)$ be an r-regular, connected, undirected graph on m vertices. Let $X = (x_0, x_1, \ldots, x_{v-1})$ and $Y = (y_0, y_1, \ldots, y_{v-1})$ be two random walks on G. The probability that these two random walks, X, Y, will start at the same vertex is:

$$Pr(x_0 = y_0) = \frac{1}{m}. \tag{3.2}$$

The probability that a pair of random walks X, Y will visit the same vertex at time slot i, $1 \leq i \leq v-1$ satisfies,

$$Pr(x_i = y_i) =$$
$$Pr(x_{i-1} \neq y_{i-1})Pr(x_i = y_i | x_{i-1} \neq y_{i-1}) + Pr(x_{i-1} = y_{i-1})Pr(x_i = y_i | x_{i-1} = y_{i-1}). \tag{3.3}$$

Now, we impose further restrictions on G to determine $Pr(x_i = y_i)$. We will consider G a strongly regular graph.

Definition 3.2.8. *([15]) An m-vertex, r-regular graph $G = (V, E)$ is called an $(m, r; \lambda, \mu)$-**strongly-regular graph** if:*

- *any two adjacent vertices have λ common neighbours;*
- *any two non-adjacent vertices have μ common neighbours.*

In the handbook of combinatorial designs [25] the authors provide strongly-regular graphs with different flexible parameters for m, r, λ and μ.

Notice that we lose some properties of expander graphs when we consider strongly regular graphs. A random walk on an expander graph has the property that after a finite number of steps the probability that it hits every vertex is uniform. So, we lose this uniformity of elements on the random walk. However, both strongly regular graphs and expander graphs are regular graphs. So, the probability of choosing the succeeding vertex for a random walk is the same in either of the graphs.

Consider G an $(m, r; \lambda, \mu)$-strongly-regular graph. Let $X = (x_i), Y = (y_i)$ be a pair of random walks on G. For any i, $1 \leq i \leq v-1$ consider the three states for the random walks X, Y:

- S_1: $x_i = y_i$,
- S_2: x_i and y_i are distinct and adjacent and

- S_3: x_i and y_i are distinct and non-adjacent.

Denote the probability of transitioning from state S_h to state S_k in one step by:

$$P_{h,k} = Pr(x_i, y_i \text{ are in state } S_k | x_{i-1}, y_{i-1} \text{ are in state } S_h).$$

Given the three states for a pair of random walks, a transition matrix M is:

$$M = \begin{pmatrix} P_{1,1} & P_{1,2} & P_{1,3} \\ P_{2,1} & P_{2,2} & P_{2,3} \\ P_{3,1} & P_{3,2} & P_{3,3} \end{pmatrix}. \tag{3.4}$$

To derive $P_{h,k}$, $h, k = \{1, 2, 3\}$ we do the following. We consider x_{i-1}, y_{i-1} in state S_h. Then we count the number of pairs x_i, y_i which satisfy the conditions of the state S_k. The total number of possibilities x_i, y_i is r^2. We consider the transition from each state S_h separately.

We start by deriving the equations for the transition from state S_1: $P_{1,k}$, $k = \{1, 2, 3\}$. In the state S_1 we have the following. We have a pair of vertices x_{i-1}, y_{i-1} such that $x_{i-1} = y_{i-1}$. For each $y_i \in N(y_{i-1})$ we have $N(y_i) \cap N(y_{i-1}) = \lambda$.

1. From state S_1 to state S_1, $P_{1,1}$.

   Out of r^2 possibilities x_i, y_i, we have r of them such that $x_i = y_i$. Therefore, given the state S_1, the total number of occurrences such that $x_i = y_i$ is r. So:

   $$P_{1,1} = \frac{r}{r^2}. \tag{3.5}$$

2. From state S_1 to state S_2, $P_{1,2}$.

   Out of r^2 possibilities x_i, y_i, we have the total number of occurrences such that given $x_{i-1} = y_{i-1}$ then $y_i \neq x_i$ and y_i, x_i are adjacent is $\lambda \cdot r$. So:

   $$P_{1,2} = \frac{\lambda \cdot r}{r^2}. \tag{3.6}$$

3. From state S_1 to state S_3, $P_{1,3}$.

   Each vertex y_i has λ common neighbours with y_{i-1} and so has $r-\lambda-1$ that are not neighbours of y_{i-1}. So each of the r neighbours y_i of y_{i-1} contribute $r-\lambda-1$ pairs x_i, y_i such that $x_i \neq y_i$ and x_i, y_i are non-adjacent. Therefore the total number of occurrences such that given state S_1 then $x_i \neq y_i$ and x_i, y_i are non-adjacent is $r(r-\lambda-1)$. So:

$$P_{1,3} = \frac{r(r-\lambda-1)}{r^2}. \tag{3.7}$$

We now derive the equations for the transition from state S_2: $P_{2,k}$, $k = \{1,2,3\}$. In the state S_2 we have the following. Given x_{i-1}, y_{i-1} such that $x_{i-1} \neq y_{i-1}$ and x_{i-1}, y_{i-1} are adjacent. Then x_{i-1} has λ vertices common with y_{i-1}.

1. From state S_2 to state S_1.

   Let x_{i-1}, y_{i-1} be in state S_2: $x_{i-1} \neq y_{i-1}$ and x_{i-1}, y_{i-1} are adjacent. Then x_{i-1} has λ vertices common with y_{i-1}. Then the total number of occurrences x_i, y_i such that $x_i = y_i$ is λ. Therefore the probability of transitioning from state S_2 to state S_1 is:

$$P_{2,1} = \frac{\lambda}{r^2}. \tag{3.8}$$

2. From state S_2 to state S_2.

   Suppose we are given x_{i-1}, y_{i-1} in state S_2. Here we consider three cases after choosing $y_i \in N(y_{i-1})$ and count the pairs x_i, y_i, with $x_i \in N(x_{i-1})$ that satisfy the condition of transitioning to state S_2: $y_i \in N(y_{i-1})$ and $y_i = x_{i-1}$; $y_i \in N(y_{i-1}), y_i \in N(x_{i-1})$ and $y_i \neq x_{i-1}$; $y_i \in N(y_{i-1}), y_i \notin N(x_{i-1})$ and $y_i \neq x_{i-1}$.

   There is a vertex $y_i \in N(y_{i-1})$ such that $y_i = x_{i-1}$ and thus we have r pairs x_i, y_i that are distinct and adjacent.

   Next consider vertex $y_i \in N(x_{i-1})$ with $y_i \neq x_{i-1}$. Then y_i, x_{i-1} have λ vertices in common. So, there are λ vertices $x_i \in N(x_{i-1})$ such that $y_i \neq x_i$ and y_i, x_i

are adjacent. Now, since x_{i-1}, y_{i-1} have λ vertices in common for being adjacent vertices, then there are λ vertices $y_i \in N(y_{i-1})$ such that $y_i \in N(x_{i-1})$. Then there are λ^2 pairs x_i, y_i that are distinct and adjacent.

Now consider $y_i \notin N(x_{i-1})$ and $y_i \neq x_{i-1}$. Then y_i and x_{i-1} have μ vertices in common in their neighbourhood. That is, there are μ vertices x_i such that $y_i \neq x_i$ and y_i, x_i are adjacent. Then we have in total $(r - \lambda - 1) \cdot \mu$ pairs x_i, y_i that are distinct and adjacent.

Given x_{i-1}, y_{i-1} in state S_2, the total number of occurrences of x_i, y_i such that $y_i \neq x_i$ and y_i, x_i are adjacent is:

$$r + \lambda^2 + (r - \lambda - 1) \cdot \mu.$$

The probability of transitioning from state S_2 to state S_2 is:

$$P_{2,2} = \frac{r + \lambda^2 + (r - \lambda - 1) \cdot \mu}{r^2}. \tag{3.9}$$

3. From state S_2 to state S_3.

   Suppose we are given x_{i-1}, y_{i-1} in state S_2. Here we consider two cases after choosing $y_i \in N(y_{i-1})$ and count the pairs x_i, y_i, with $x_i \in N(x_{i-1})$ that satisfy the condition of transitioning to state S_3: $y_i \in N(y_{i-1})$ and $y_i \in N(x_{i-1})$; $y_i \in N(y_{i-1})$ and $y_i \notin N(x_{i-1})$.

   Consider $y_i \in N(x_{i-1})$. We have a pair x_i, y_i such $y_i = x_i$. Next, we know the pair y_i, x_{i-1} have λ vertices in common in their neighbourhood. Then we have λ pairs x_i, y_i that are distinct and adjacent. So, $r - \lambda - 1$ pairs x_i, y_i are distinct and non-adjacent. However, there are λ vertices y_i such that $y_i \in N(x_{i-1})$. Then the total number of occurrences of x_i, y_i such that $y_i \in N(x_{i-1})$, $y_i \neq x_i$ and x_i, y_i are non-adjacent is $(r - \lambda - 1) \cdot \lambda$.

   Next consider $y_i \notin N(x_{i-1})$. The pair y_i, x_{i-1} have μ vertices in common and

$(r-\mu)$ not in common in their neighbourhood. There are $r-\lambda-1$ vertices y_i such that $y_i \notin N(x_{i-1})$. Then the total number of occurrences x_i, y_i such that $y_i \notin N(x_{i-1})$, $y_i \neq x_i$ and y_i, x_i are non-adjacent is $(r-\lambda-1)\cdot(r-\mu)$.

Given the state S_2, the total number of pairs x_i, y_i such that $y_i \neq x_i$ and y_i, x_i are non-adjacent is:

$$(r-\lambda-1)\cdot\lambda + (r-\lambda-1)\cdot(r-\mu) = (r-\lambda-1)\cdot(\lambda+(r-\mu)).$$

The probability of transitioning from state S_2 to state S_3 is:

$$P_{2,3} = \frac{(r-\lambda-1)\cdot(\lambda+(r-\mu))}{r^2}. \tag{3.10}$$

We now derive the equations for the transition from state S_3: $P_{3,k}$, $k = \{1,2,3\}$.

1. From state S_3 to state S_1.

   Consider $y_i \in N(x_{i-1})$, there is a pair x_i, y_i such that $y_i = x_i$. Now, the vertices y_{i-1} and x_{i-1} have μ vertices in common in their neighbourhood. So, there are μ vertices y_i such that $y_i \in N(x_{i-1})$. Therefore, given x_{i-1}, y_{i-1} in state S_3, the total number of occurrences x_i, y_i such that $x_i = y_i$ is μ.

   So, the probability of transitioning from state S_3 to state S_1 is:

   $$P_{3,1} = \frac{\mu}{r^2}. \tag{3.11}$$

2. From state S_3 to state S_2.

   Suppose we are given x_{i-1}, y_{i-1} in state S_3. Here we consider two cases after choosing $y_i \in N(y_{i-1})$ and count the pairs x_i, y_i, with $x_i \in N(x_{i-1})$ that satisfy the condition of transitioning to state S_2: $y_i \in N(y_{i-1})$ and $y_i \in N(x_{i-1})$; $y_i \in N(y_{i-1})$ and $y_i \notin N(x_{i-1})$.

Consider $y_i \in N(x_{i-1})$. The vertices y_i, x_{i-1} have λ common vertices in their neighbourhoods. Then there are λ pairs x_i, y_i such that x_i, y_i are distinct and adjacent. Now, the vertices y_i, x_{i-1} have μ common vertices in their neighbourhoods. Therefore, the total number of occurrences x_i, y_i such that $y_i \in N(x_{i-1})$, $y_i \neq x_i$ and y_i, x_i are adjacent is $\lambda \cdot \mu$.

Consider $y_i \notin N(x_{i-1})$. The vertices y_i, x_{i-1} have μ vertices in their neighbourhoods. So there are $r - \mu$ vertices y_i such that $y_i \notin N(x_{i-1})$. The total number of occurrences x_i, y_i such that $y_i \notin N(x_{i-1})$, $y_i \neq x_i$ and y_i, x_i are adjacent is $(r - \mu) \cdot \mu$.

Therefore, given the state S_3, the total number of pairs x_i, y_i such that $y_i \neq x_i$ and y_i, x_i are adjacent is:

$$\lambda \cdot \mu + (r - \mu) \cdot \mu.$$

The probability of transitioning from the state S_3 to the state S_2 is:

$$P_{3,2} = \frac{\lambda \cdot \mu + (r - \mu) \cdot \mu}{r^2}. \tag{3.12}$$

3. From state S_3 to state S_3.

   Suppose we are given x_{i-1}, y_{i-1} in state S_3. Here we consider two cases after choosing $y_i \in N(y_{i-1})$ and count the pairs x_i, y_i, with $x_i \in N(x_{i-1})$ that satisfy the condition of transitioning to state S_3: $y_i \in N(y_{i-1})$ and $y_i \in N(x_{i-1})$; $y_i \in N(y_{i-1})$ and $y_i \notin N(x_{i-1})$.

   Consider $y_i \in N(x_{i-1})$. There is a pair x_i, y_i such that $y_i = x_i$. We know that the vertices y_i, x_{i-1} have λ common vertices in their neighbourhoods. Therefore, we have $r - \lambda - 1$ pairs x_i, y_i where $y_i \neq x_i$ and y_i, x_i are non-adjacent. Now, the vertices y_i, x_{i-1} have μ common vertices in their neighbourhoods. So the total number of pairs x_i, y_i such that $y_i \in N(x_{i-1})$, $y_i \neq x_i$ and y_i, x_i are non-adjacent is $(r - \lambda - 1) \cdot \mu$.

Consider $y_i \notin N(x_{i-1})$. The vertices y_i, x_{i-1} have μ and $r - \mu$ common and not common vertices respectively in their neighbourhoods. We have $r - \mu$ vertices y_i such that $y_i \notin N(x_{i-1})$. So, the total number of pairs x_i, y_i such that $y_i \notin N(x_{i-1})$, $y_i \neq x_i$ and y_i, x_i are non-adjacent is $(r - \mu)^2$.

Therefore, given the state S_3, the total number of pairs x_i, y_i such that $y_i \neq x_i$ and y_i, x_i are non-adjacent is:

$$(r - \lambda - 1) \cdot \mu + (r - \mu)^2.$$

The probability of transitioning from state S_3 to state S_3 is:

$$P_{3,3} = \frac{(r - \lambda - 1) \cdot \mu + (r - \mu)^2}{r^2}. \tag{3.13}$$

We can now put together the transition matrix M as:

$$M = \frac{1}{r^2} \begin{pmatrix} r & \lambda r & r(r - \lambda - 1) \\ \lambda & r + \lambda^2 + (r - \lambda - 1)\mu & (r - \lambda - 1) \cdot (\lambda + (r - \mu)) \\ \mu & \lambda \cdot \mu + (r - \mu) \cdot \mu & (r - \lambda - 1)\mu + (r - \mu)^2 \end{pmatrix}. \tag{3.14}$$

Each row of M sum up to 1.

We now determine the initial distribution of the states.

1. The initial probability of being in state S_1: Need to find the probability of randomly picking a pair of vertices x_0, y_0 such that $x_0 = y_0$.

   Pick a vertex $x_0 \in V$ at random. There is one way of picking $y_0 \in V$ such that $x_0 = y_0$. Then,

   $$Pr(x_0 = y_0) = \frac{1}{m}. \tag{3.15}$$

2. The initial probability of being in state S_2: Need to find the probability of ran-

domly picking a pair of vertices x_0, y_0 such that $x_0 \neq y_0$ and x_0, y_0 are adjacent.

Pick a vertex $x_0 \in V$ at random. There are r vertices $y_0 \in N(x_0)$ with $x_0 \neq y_0$, therefore there are r choices of $y_0 \in V$ such that $x_0 \neq y_0$ and x_0, y_0 are adjacent. Then,

$$Pr(x_0 \neq y_0 \text{ and adjacent}) = \frac{r}{m}. \tag{3.16}$$

3. The initial probability of being in state S_3: Need to find the probability of randomly picking a pair of vertices x_0, y_0 such that $x_0 \neq y_0$ and x_0, y_0 are non-adjacent.

   Pick a vertex $x_0 \in V$ at random. Of the m vertices in V there are $m - r - 1$ vertices y_0 such that $y_0 \notin N(x_0)$ and $x_0 \neq y_0$. Then,

$$Pr(x_0 \neq y_0 \text{ and non-adjacent}) = \frac{m - r - 1}{m}. \tag{3.17}$$

Let π_0 denote the 1×3 matrix where the jth entry is the initial probability that a pair of vertices x_0, y_0 is in state S_j, $j = 1, 2, 3$. That is:

$$\pi_0 = \begin{pmatrix} \frac{1}{m} & \frac{r}{m} & \frac{m-r-1}{m} \end{pmatrix}. \tag{3.18}$$

The probability that x_i, y_i, $1 \leq i \leq v-1$, are in state S_j, $j = 1, 2, 3$, is given by the jth entry of the matrix $\pi_0 \cdot M^i$. In particular, the probability that the pair of random walks X, Y will visit the same vertex at time slot i, $Pr(x_i = y_i)$, $1 \leq i \leq v-1$, is given by the first entry of the matrix $\pi_0 \cdot M^i$.

Lemma 3.2.9. *Let G be an (m, r, λ, μ)-strongly regular graph. The transition and the initial probabilities matrices of G satisfy $\pi_0 \cdot M^i = \pi_0$*

Proof. The parameters of G satisfy [15]:

$$(m - r - 1)\mu = r(r - \lambda - 1). \tag{3.19}$$

Consider M and π_0 given in (3.14) and (3.18) respectively. Then we compute $\pi_0 \cdot M$. The 1st entry of $\pi_0 \cdot M$ is:

$$\begin{aligned}
&\frac{1}{m} \cdot \frac{r}{r^2} + \frac{r}{m} \cdot \frac{\lambda}{r^2} + \frac{m-r-1}{m} \cdot \frac{\mu}{r^2} \\
&= \frac{1}{m} \cdot \left(\frac{r}{r^2} + \frac{r\lambda}{r^2} + \frac{r(r-\lambda-1)}{r^2} \right) \\
&= \frac{1}{m} \cdot \left(\frac{r + r\lambda + r^2 - r\lambda - r}{r^2} \right) \\
&= \frac{1}{m}.
\end{aligned} \tag{3.20}$$

The 2nd entry of $\pi_0 \cdot M$ is:

$$\begin{aligned}
&\frac{1}{m} \cdot \frac{r\lambda}{r^2} + \frac{r}{m} \cdot \frac{(r + \lambda^2 + (r-\lambda-1)\mu)}{r^2} + \frac{m-r-1}{m} \cdot \frac{\lambda\mu + (r-\mu)\mu}{r^2} \\
&\frac{r}{m} \left(\frac{\lambda}{r^2} + \frac{r + \lambda^2 + (r-\lambda-1)\mu}{r^2} + \frac{\lambda(r-\lambda-1) + (r-\mu)(r-\lambda-1)}{r^2} \right) \\
&= \frac{r}{m}.
\end{aligned} \tag{3.21}$$

Finally, the 3rd entry of $\pi_0 \cdot M$ is:

$$\begin{aligned}
&\frac{1}{m} \cdot \frac{r(r-\lambda-1)}{r^2} + \frac{r}{m} \cdot \left(\frac{(r-\lambda-1)(r+\lambda-\mu)}{r^2} \right) + \frac{m-r-1}{m} \cdot \left(\frac{(r-\lambda-1)\mu + (r-\mu)^2}{r^2} \right) \\
&= \frac{1}{m} \cdot \frac{(m-r-1)\mu}{r^2} + \frac{1}{m} \cdot \left(\frac{(m-r-1)\mu(r+\lambda-\mu)}{r^2} \right) + \frac{m-r-1}{m} \cdot \left(\frac{(r-\lambda-1)\mu + (r-\mu)^2}{r^2} \right) \\
&= \frac{m-r-1}{m} \cdot \left(\frac{\mu}{r^2} + \frac{\mu(r+\lambda-\mu)}{r^2} + \frac{(r-\lambda-1)\mu + (r-\mu)^2}{r^2} \right) \\
&= \frac{m-r-1}{m}.
\end{aligned} \tag{3.22}$$

Therefore $\pi_0 \cdot M = \pi_0$. By the associative property of matrices we have $\pi_0 \cdot M^i = \pi_0$. □

Lemma 3.2.10. *Let G be an (m, r, λ, μ)-strongly regular graph. The probability $Pr(x_i =$*

y_i) that a pair of random walks X, Y will visit the same vertex at time slot i is:

$$Pr(x_i = y_i) = \frac{1}{m}, \qquad 0 \leq i \leq v - 1. \tag{3.23}$$

Let $p_i = Pr(x_i = y_i)$ and H be the number of collisions between a pair of random FH sequences X and Y. The probability of the event $H = h$ is:

$$Pr(H = h) = \binom{v}{h} p_i^h (1 - p_i)^{v-h} \tag{3.24}$$

The expected number of collisions between any two random sequences is given by:

$$E(H) = \sum_{h=0}^{v} h \cdot Pr(H = h), \tag{3.25}$$

where $Pr[H = h]$ is provided by Equation (3.24).

Example 3.2.11. *Consider a $(9, 4, 1, 2)$-strongly-regular graph $G = (V, E)$ [25]. Consider the set $\mathcal{S}$ of all random walks of length 10 on G, a $(10, 9 \times 49, 9)$-FHS. For any two random FH sequences X, Y, on G we have the following.*

The initial probabilities matrix π_0 is:

$$\pi_0 = \begin{pmatrix} 1/9 & 4/9 & 4/9 \end{pmatrix}.$$

The probability $Pr(x_i = y_i)$, that a pair of random walks X, Y will visit the same vertex at time slot i is:

$$Pr(x_i = y_i) = \frac{1}{9}. \tag{3.26}$$

Using Equation (3.25), the expected number of collisions between any pair of random walks on G is $E(H) = 1.111$.

Hamming group correlation

Let $\mathcal{S}$ be a $(v, m \times r^{v-1}, m)$-FHS. We estimate the Hamming group correlation as,

$$G(X,\mathcal{U}) \leq wE,$$

where $\mathcal{U} \subseteq \mathcal{S}$, $|\mathcal{U}| = w$, $X \in \mathcal{S} \setminus \mathcal{U}$ and E is the expected Hamming correlation provided in Equation (3.25). So the w-throughput of X is,

$$\rho_w(X,\mathcal{U}) \geq 1 - \frac{wE}{v}.$$

An estimation of the worst-case w-throughput of $\mathcal{S}$ can be obtained in a similar manner,

$$\begin{aligned}\hat{\rho}_w(\mathcal{S}) &= \min_{\mathcal{V}\subseteq\mathcal{S}} \left\{ \min_{X\in\mathcal{V}} \{\rho_w(X, \mathcal{V} \setminus \{X\})\} \right\} \\ &= 1 - \frac{wE}{v},\end{aligned}$$

where $X \in \mathcal{V}$, $\mathcal{V} = \mathcal{U} \cup \{X\}$ and $\rho_w(X, \mathcal{V} \setminus \{X\}) = 1 - \frac{G(X,\mathcal{V}\setminus\{X\})}{v}$.

3.2.4 Jamming resistance

Recall the (θ_1, θ_2)-adaptive jammer introduced in Section 2.5. The jammer eavesdrops on $\theta_1 m$ channels $0 \leq \theta_1 \leq 1$, and jams on $\theta_2 m$ channels $0 \leq \theta_2 < 1$. It changes its channel jamming strategy according to information it can acquire from eavesdropping.

We now analyse how a jammer's behaviour changes with respect to information of the channel it was eavesdropping on a particular time slot. We consider the following: eavesdropping on an active or inactive channel consecutively, and when a jammer switches from eavesdropping on an active to an inactive channel. We consider the situation where there is only one active FH sequence in use. We will provide details of the case of more than one active FH sequence, for an FH scheme in Chapter 6,

in the future work section. Now, introducing a $(1/m, 1/m)$-adaptive jammer in our $(v, m \times r^{v-1}, m)$-FHS, $\mathcal{S} = \{X_i : 0 \leq i \leq k-1\}$, X_i a random walk on a graph, we have the following:

J1 A jammer that eavesdrops on an active channel consecutively: At any time slot t that a jammer has eavesdropped on an active channel, this jammer removes all but the FH sequence containing the active channel at that particular time slot. Let $|\mathcal{S}_t^*|$ denote the size of the search space of a jammer at time slot t. With respect to the $(v, m \times r^{v-1}, m)$-FHS properties described in Section 3.2.2, at time slot $t = 0$ the jammer has $mr^{v-1} = |\mathcal{S}| = |\mathcal{S}_0^*|$ FH sequences in its search space. At any time slot $t \neq 0$, the jammer has r^{v-t}. Therefore, on the last time slot $t = v - 1$ there are r FH sequences in a jammer's. So, the jammer does not identify the active FH sequence.

J2 A jammer that eavesdrops on an inactive channel consecutively: At $t = 0$ we have $|\mathcal{S}_0^*| = m \cdot r^{v-1}$, all the FH sequences in the FH scheme. Suppose at $t = 0$ this jammer eavesdropped on channel f_0. Recall each channel appears r^{v-1} at each time slot in the FH scheme. So, discarding all inactive FH sequences with $x_0^j = f_0$, $0 \leq j \leq k-1$ the jammer has $|\mathcal{S}_1^*| = (m-1) \cdot r^{v-1}$. Now suppose it eavesdrops on an inactive channel f_1 at time slot $t = 1$. If $f_1 \notin \mathcal{N}(f_0)$ then f_1 appears on r^{v-1} FH sequences in $\mathcal{S}_1^*$. Otherwise, if $f_1 \in \mathcal{N}(f_0)$ then f_1 appears on $r^{v-1} - r^{v-2}$ FH sequences in $\mathcal{S}_1^*$. So, at any time slot $t \neq 0$, the jammer has $|\mathcal{S}^*| \leq mr^{v-1} - \sum_{i=1}^{t} r^{v-i}$. For $m \geq 2$, $r \geq 2$ then $mr^{v-1} - \sum_{i=1}^{t} r^{v-i} \neq 1$ at any time slot t, $1 \leq t \leq v-1$ and thus a jammer can not identify the active FH sequence.

J3 Mixed fate jammer: From the discussions on **J1** and **J2** a jammer that eavesdrops on an active channel consecutively reduces the search space at least as quickly as when it eavesdrops on an inactive channel consecutively. Further, neither of these jamming strategies enables a jammer to identify the active FH sequence. Now,

suppose we have a change of fate from eavesdropping an active FH sequence to that which is inactive. Then we still have $r^{v-t} \leq |\mathcal{S}^*| \leq mr^{v-1} - \sum_{i=1}^{t} r^{v-i}$ at any time slot t, $1 \leq t \leq v-1$. That is a change of fate will not make a jammer have a single FH sequence in $|\mathcal{S}^*|$: the active FH sequence is not identified.

We conclude with the following proposition.

Proposition 3.2.12. *Consider the set of all random walks as a $(v, m \times r^{v-1}, m)$-FHS with one active FH sequence. Let $m \geq 2$, $r \geq 2$. At any time slot t, $1 \leq t \leq v-1$ the jammer's search space $\mathcal{S}^*$ has the following number of FH sequences $r^{v-t} \leq |\mathcal{S}^*| \leq mr^{v-1} - \sum_{i=1}^{t} r^{v-i}$ and does not identify the active FH sequence.*

3.3 Difference packing

In this section we consider the construction by Fuji-Hara et al. [35, Section 4]. It is a combinatorial construction based on difference packing and cyclic resolvable balanced incomplete block designs. We point out that the authors provide several combinatorial constructions of FH sequences and we only consider one of them in this section. Ng and Paterson [70] showed that another construction [35, Section 3], based on projective geometry, provide the Lempel-Greenberger algebraic m-sequence transformation sequences. The Lempel-Greenberger sequences will be considered in Section 3.4.

3.3.1 Preliminaries

We first introduce difference packing, a combinatorial object that will be used to obtain an FH sequence.

Definition 3.3.1. *A collection $\mathcal{P} = \{B_0, B_1, \ldots, B_{m-1}\}$ of subsets of $\mathbb{Z}_v$ form a **difference packing** over $\mathbb{Z}_v$, denoted m-DP(v, K, λ), where $K = \{|B_i| : 0 \leq i \leq m-1\}$, if $|\{b - b' \pmod v : b \neq b', (b, b') \in B_i \times B_i, 0 \leq i \leq m-1\}| \leq \lambda$. It is denoted as m-DP(v, κ, λ) when $|B_i| = \kappa$ for all $i = 0, \ldots, m-1$.*

A collection $\mathcal{P}$ is called a *difference family* when among the differences $\{b-b' \pmod v : b, b' \in B_i, b \neq b', i = 0, \ldots, m-1\}$ each nonzero $g \in \mathbb{Z}_v$ occurs exactly λ times and it is denoted (v, K, λ)-difference family, where K is as previously defined in Definition 3.3.1.

Definition 3.3.2. *A difference packing over $\mathbb{Z}_v$ that partitions $\mathbb{Z}_v$ is called a* ***partition type difference packing****.*

Let $X = (x_0, x_1, \ldots, x_{v-1})$ be an FH sequence over $\mathcal{F}$, $|\mathcal{F}| = m$. Define m disjoint sets $B_0, B_1, \ldots, B_{m-1}$ using X, where each B_i is the *support* of i, $i \in \mathcal{F}$, corresponding to

$$B_i = supp_X(i) = \{t : x_t = i, 0 \leq t \leq v-1\}. \tag{3.27}$$

That is, each B_i specifies the position on which the frequency channel i appears in the FH sequence X.

Next, we define the rotational closure of an FH scheme.

Let $\beta^i X$ denote the cyclic shift of an FH sequence X to the right by i places:

$$\beta^i X = (x_{v-i}, x_{v-i+1}, \ldots, x_{v-1}x_0, x_1, \ldots x_{v-i-2}, x_{v-i-1}). \tag{3.28}$$

We have $\beta^i X = \beta^i(x_t) = (x_{t+i})$ and $\beta^{i'}(\beta^i X) = \beta^{i'+i}X$, $i, i' \in \{0, 1, \ldots, v-1\}$, where the operations of both the exponents and indices are conducted modulo v.

Definition 3.3.3. *Let $X = (x_t)_{t=0}^{v-1}$ be an FH sequence over $\mathcal{F}$, $|\mathcal{F}| = m$. Then X form a $(v, 1, m)$-FHS, $\mathcal{S}$. The* ***rotational closure*** *of $\mathcal{S}$ is the set:*

$$\overset{\Leftrightarrow}{\mathcal{S}} = \{\beta^i X : 0 \leq i \leq v-1\},$$

where $\beta^i X$ is as defined by Equation (3.28).

When we consider the rotational closure of a $(v, 1, m)$-FHS, $\mathcal{S}$ from Definition 3.3.3 as an FH scheme then we call $\overset{\Leftrightarrow}{\mathcal{S}}$ a rotational closure (v, v, m)-FHS.

Fuji-Hara [35], Theorem 2.3, provide a correspondence between FH sequences and

partition type difference packing. The authors provide several combinatorial constructions of partition type difference packings and thus construct FH schemes.

Theorem 3.3.4 (Theorem 2.3, [35]). *There exists an FH sequence of length v over a frequency library of size m with maximum Hamming auto-correlation λ if and only if there exists a partition type m-DP(v, K, λ), $\mathcal{P} = \{B_0, \ldots, B_{m-1}\}$, over $\mathbb{Z}_v$, where B_i, $0 \leq i \leq m-1$, is the support of frequency channel i, $K = \{|B_i| : 0 \leq i \leq m-1\}$.*

To discuss the construction of a partition type m-DP(v, K, λ) we first need to introduce block designs. We provide an introduction here to block designs and the relevant preliminaries which will be needed for the construction considered in this section. For references on block designs see [7, 12, 25, 97].

Definition 3.3.5. *A **design** is a pair $(\mathcal{X}, \mathcal{B})$ such that the following properties are satisfied:*

1. *$\mathcal{X}$ is a finite set of elements called **points**, and*
2. *$\mathcal{B}$ is a collection of nonempty subsets of $\mathcal{X}$ called **blocks**.*

We are interested in balanced incomplete block designs.

Definition 3.3.6. *Let v, κ, and λ be positive integers such that $v > \kappa \geq 2$. A 2-(v, κ, λ)-**balanced incomplete block design**, denoted 2-(v, κ, λ)-BIBD, is a design $(\mathcal{X}, \mathcal{B})$ such that the following properties are satisfied:*

1. *$|\mathcal{X}| = v$,*
2. *each block contain exactly κ points, and*
3. *every pair of distinct points is contained in exactly λ blocks.*

A 2-(v, κ, λ)-BIBD with $\lambda = 1$ is called a *Steiner design*. For simplicity we will denote a 2-(v, κ, λ)-BIBD as (v, κ, λ)-BIBD. We define an automorphism on a (v, κ, λ)-BIBD as follows.

Definition 3.3.7. *Suppose $(\mathcal{X}, \mathcal{B})$ is a design. If there exists a bijection $\tau : \mathcal{X} \to \mathcal{X}$ such that if we apply τ to the elements of any block of $\mathcal{B}$ we obtain a block of $\mathcal{B}$ again then the bijection τ is called an* ***automorphism****. The automorphism τ is a permutation of $\mathcal{X}$ and $\mathcal{B}$ the multiset of blocks can be written as:*

$$\mathcal{B} = \{\{\tau(x) : x \in B\} : B \in \mathcal{B}\},$$

where $\{\tau(x) : x \in B\}$ denote a block in $\mathcal{B}$.

The mapping $\tau(x) = x$, $x \in B$, $B \in \mathcal{B}$ is a trivial automorphism.

In the construction considered in this section we will use a cyclic BIBD.

Definition 3.3.8. *A (v, κ, λ)-BIBD design with an automorphism τ of order v is called a* ***cyclic*** *(v, κ, λ)-****BIBD****.*

The set of points of a cyclic (v, κ, λ)-BIBD can be identified with $\mathbb{Z}_v$. In this case the BIBD has an automorphism $\tau : i \to i + 1 \pmod{v}$. The *orbit* containing a block $B \in \mathcal{B}$ is the set of the distinct blocks:

$$\tau^i(B) = B + i = \{b_1 + i, \ldots, b_\kappa + i\} \pmod{v},$$

for $i \in \mathbb{Z}_v$. We sometimes denote an orbit containing a block B as $Orb(B)$. The *development* of a block B is the orbit containing the block. The *length* of an orbit is its cardinality. A *base block* is a block chosen arbitrarily from an orbit. An orbit containing a block of the form:

$$\frac{v}{\kappa}\mathbb{Z}_\kappa = \left\{0, \frac{v}{\kappa}, \ldots, (\kappa - 1)\frac{v}{\kappa}\right\}, \tag{3.29}$$

is called a *regular short orbit*. A base block of Equation (3.29) generate $\frac{v}{\kappa}$ blocks that are pairwise disjoint.

Consider a BIBD $(\mathcal{X}, \mathcal{B})$. We now define partitions of the blocks called resolution classes where each resolution class contains v distinct points: it forms a set of points $\mathcal{X}$.

This gets us closer to the correspondence between BIBD and partition type difference packings.

Definition 3.3.9. *A (v, κ, λ)-BIBD, $(\mathcal{V}, \mathcal{B})$, is **resolvable** if the blocks can be arranged into r classes $R_0, \ldots, R_{r-1}$ such that the $\frac{b}{r} = \frac{v}{\kappa}$ blocks (where $b = |\mathcal{B}|$) of each class are disjoint and every point of point set $\mathcal{V}$ is contained in exactly one block in each class.*

The classes R_i are called *resolution classes*. The set of resolution classes, $\mathcal{R} = \{R_0, \ldots, R_{r-1}\}$, is called a *resolution*.

Definition 3.3.10. *Suppose we have a cyclic resolvable BIBD, $(\mathcal{V}, \mathcal{B})$, with resolution $\mathcal{R} = \{R_0, \ldots, R_{r-1}\}$. Consider a resolution class $R_i \in \mathcal{R}$ and let $R_i + 1 = \{B + 1 \ (mod\ V) | B \in R_i\}$. If $\mathcal{R} + 1 = \{R_0 + 1, \ldots, R_{r-1} + 1\} = \mathcal{R}$ then the design is called a **cyclically resolvable BIBD**, denoted CRB-(v, κ, λ).*

A necessary and sufficient condition for the existence of a CRB-$(v, \kappa, 1)$ is that $v \equiv 1, \kappa \pmod{\kappa(\kappa-1)}$, [61]. A CRB-$(v, \kappa, 1)$ with $v \equiv 1 \pmod{\kappa(\kappa-1)}$ has no short orbit while a CRB-$(v, \kappa, 1)$ with $v \equiv \kappa \pmod{\kappa(\kappa-1)}$ has a single regular short orbit. It is known [61] that a CRB-$(v, \kappa, 1)$ with $v \equiv \kappa \pmod{\kappa(\kappa-1)}$ consists of $\frac{v-\kappa}{\kappa(\kappa-1)}$ full orbits and a single regular short orbit.

Example 3.3.11. *The following is a CRB-$(21, 3, 1)$:*

R_0 :	$\{1, 4, 16\}$	$\{8, 11, 2\}$	$\{15, 18, 9\}$	$\{19, 20, 3\}$	$\{5, 6, 10\}$	$\{12, 13, 17\}$	$\{0, 7, 14\}$
R_1 :	$\{2, 5, 17\}$	$\{9, 12, 3\}$	$\{16, 19, 10\}$	$\{20, 0, 4\}$	$\{6, 7, 11\}$	$\{13, 14, 18\}$	$\{1, 8, 15\}$
R_2 :	$\{3, 6, 18\}$	$\{10, 13, 4\}$	$\{17, 20, 11\}$	$\{0, 1, 5\}$	$\{7, 8, 12\}$	$\{14, 15, 19\}$	$\{2, 9, 16\}$
R_3 :	$\{4, 7, 19\}$	$\{11, 14, 5\}$	$\{18, 0, 12\}$	$\{1, 2, 6\}$	$\{8, 9, 13\}$	$\{15, 16, 20\}$	$\{3, 10, 17\}$
R_4 :	$\{5, 8, 20\}$	$\{12, 15, 6\}$	$\{19, 1, 13\}$	$\{2, 3, 7\}$	$\{9, 10, 14\}$	$\{16, 17, 0\}$	$\{4, 11, 18\}$
R_5 :	$\{6, 9, 0\}$	$\{13, 16, 7\}$	$\{20, 2, 14\}$	$\{3, 4, 8\}$	$\{10, 11, 15\}$	$\{17, 18, 1\}$	$\{5, 12, 19\}$
R_6 :	$\{7, 10, 1\}$	$\{14, 17, 8\}$	$\{0, 3, 15\}$	$\{4, 5, 9\}$	$\{11, 12, 16\}$	$\{18, 19, 2\}$	$\{6, 13, 20\}$

R_7 :	$\{1, 11, 9\}$	$\{4, 14, 12\}$	$\{7, 17, 15\}$	$\{10, 20, 18\}$	$\{13, 2, 0\}$	$\{16, 5, 3\}$	$\{19, 8, 6\}$
R_8 :	$\{2, 12, 10\}$	$\{5, 15, 13\}$	$\{8, 18, 16\}$	$\{11, 0, 19\}$	$\{14, 3, 1\}$	$\{17, 6, 4\}$	$\{20, 9, 7\}$
R_9 :	$\{3, 13, 11\}$	$\{6, 16, 14\}$	$\{9, 19, 17\}$	$\{12, 1, 20\}$	$\{15, 4, 2\}$	$\{18, 7, 5\}$	$\{0, 10, 8\}$

There are 10 *resolution classes. Each box represent an orbit. So there are three full orbits and one regular short orbit.*

3.3.2 Construction of FH sequences using a difference packing

In this section we consider the construction of FH sequences proposed by Fuji-Hara et al. [35] which use a CRB-$(\kappa m, \kappa, 1)$. We refer to Mishima and Jimbo [67] for the specific type of CRB-$(\kappa m, \kappa, 1)$, simply referred to as type $(T2)$ in the discussion of this section. The classification of the CRB-$(\kappa m, \kappa, 1)$ made by Mishimo and Jimbo is according to the relationship between the regular short orbit and the resolution classes of the CRB-$(\kappa m, \kappa, 1)$. In particular, a type $(T2)$ CRB-$(\kappa m, \kappa, 1)$ has a special property that every block in a regular short orbit belongs to a distinct resolution class.

Example 3.3.12. *The CRB-*$(21, 3, 1)$ *of Example 3.3.11 is of type* $(T2)$.

Construction 3.3.13 (Construction 4.1, [35])**.** *If there exists a CRB-*$(\kappa m, \kappa, 1)$ *of type* $(T2)$*, then there exists a rotational closure* $(\kappa m, \kappa m, m)$*-FHS with maximum out-of-phase Hamming auto-correlation* κ *(see Definition 2.2.4), optimal in the Lempel-Greenberger bound, derived from a partition type* m*-DP*$(\kappa m, \kappa, \kappa)$ *over* $\mathbb{Z}_{\kappa m}$*.*

Proof. A CRB-$(v, \kappa, 1)$ consists of $\frac{v-k}{k(k-1)}$ full orbits and a single regular short orbit. Suppose we have a CRB-$(v, \kappa, 1)$ of type $(T2)$. We know that a CRB-$(v, \kappa, 1)$ of this type has the property that each block in the regular short block orbit is in a distinct resolution class. There are m such resolution classes. The blocks of these m resolution classes make up $(m-1)/\kappa$ full orbits and a single regular short orbit. Each of these resolution classes with a block from a regular short orbit contain κ blocks from each of the full orbits and a single block from the regular short orbit.

Let B be a base block for an orbit $Orb(B)$. Then the set of differences $\{b - b' \pmod v : b, b' \in B_i\}$ is the same for all $B_i \in Orb(B)$. So, if each resolution class with a block from a regular short orbit contain κ blocks from each of the full orbits and a single block from the regular short orbit then each $b - b' \in \mathbb{Z}_v \setminus \{0\}$, where $b, b' \in B_i$ appears at most κ times in $B_0, \ldots, B_{v/\kappa}$. In particular some $d = b - b' \in \mathbb{Z}_v \setminus \{0\}$ appears either exactly κ times from the κ blocks in a full orbit or appears once from the block in the regular short orbit.

So, an arbitrary resolution class in a CRB-$(\kappa m, \kappa, 1)$ with a block from the regular short orbit can be viewed as a partition type m-DP$(\kappa m, \kappa, \kappa)$. By Theorem 3.3.4 an optimal rotational closure $(\kappa m, \kappa m, m)$-FHS can be derived from a partition type m-DP$(\kappa m, \kappa, \kappa)$. □

Example 3.3.14. *Consider the CRB-*$(21, 3, 1)$ *of Example 3.3.11. Any of the resolution classes* $R_0, R_1, \ldots, R_6$ *can be taken as a partition type* 7*-DP*$(21, 3, 3)$ *and thus obtain a rotational closure* $(21, 21, 7)$*-FHS with maximum Hamming autocorrelation of* 3.

Consider R_0 *as a 7-DP*$(21, 3, 3)$ *over* $\mathbb{Z}_{21}$*. Then we have the following FH sequence over* $\mathbb{Z}_7$*:*

$$(7, 1, 2, 4, 1, 5, 5, 7, 2, 3, 5, 2, 6, 6, 7, 3, 1, 6, 3, 4, 4).$$

3.3.3 Correlation

Construction 3.3.13 provides an FH sequence of length κm over $\mathcal{F}$, $|\mathcal{F}| = m$, whose maximum out-of-phase Hamming auto-correlation is κ. As was done in the previous Construction 3.2.6 using random walks on a graph, we can estimate the Hamming group correlation of a rotational closure $(\kappa m, \kappa m, m)$-FHS constructed using a CRB-$(\kappa m, \kappa, 1)$ as:

$$G(X, \mathcal{U}) \leq w\kappa,$$

where $\mathcal{U} \subseteq \mathcal{S}$, $|\mathcal{U}| = w$ and $X \in \mathcal{S} \setminus \mathcal{U}$. The w-throughput of an FH sequence X is:

$$\begin{aligned}\rho_w(X,\mathcal{U}) &= 1 - \frac{G(X,\mathcal{U})}{\kappa m} \\ &\geq 1 - \frac{w\kappa}{\kappa m} \\ &= 1 - \frac{w}{m}.\end{aligned}$$

Likewise the worst-case w-throughput of the scheme is:

$$\begin{aligned}\hat{\rho}_w(\mathcal{S}) &= \min_{\mathcal{V}\subseteq\mathcal{S}} \left\{ \min_{X\in\mathcal{V}} \{\rho_w(X, \mathcal{V} \setminus \{X\})\} \right\} \\ &= 1 - \frac{w}{m}.\end{aligned}$$

3.3.4 Jamming resistance

In this section we consider the presence of a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer in a $(\kappa m, \kappa m, m)$-FHS. We analyse the FH scheme's resistance to a jammer with respect to the jammer's activity at a time slot: a jammer that listens on an active FH channel at each time slot consecutively, listens on an inactive channel continuously and finally conclude with what happens when the jammer switches from listening on an active channel to listening on an inactive channel, and vice versa, between two consecutive time slots. We consider the situation where there is only one active FH sequence in use. We determine how long it takes a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer to identify the active FH sequence in the $(\kappa m, \kappa m, m)$-FHS.

- *Lucky jammer at every time slot consecutively:* Recall a CRB-$(\kappa m, \kappa, 1)$ of type $(T2)$ has the following property. A resolution class contains κ blocks from a full orbit and a single block from a regular short orbit. Suppose that at time 0 a jammer listens on an active channel i, whose corresponding block of position indices B_i belongs to the regular short orbit. At the first time slot 0, an active channel i will be on κ FH sequences (the size of the blocks B_i, $0 \leq i \leq m-1$, is

κ it means each channel $i \in \mathcal{F}$ appear κ times on the constructed FH sequence and the FH scheme take all cyclic shifts of it). Then at time 1 all the frequency channels appearing on the κ FH sequences with channel i from the previous time slot are distinct. Next, suppose that at time 0 a jammer listens on an active channel i whose block B_i belong to a full orbit. Further, suppose the resolution class contain the blocks $B_i + t, B_i + (t+1), \ldots, B_i + (t+\kappa-1)$. Then for κ time slots the jammer will be eavesdropping on an active channel appearing on κ FH sequences. Therefore it needs $\kappa + 1$ time slots to identify the active FH sequence. In conclusion, the worst case scenario for our FH scheme is that this type of jammer only needs to listen on two time slots to identify the active FH sequence.

- *Unlucky jammer consecutively at each time slot.* At any time slot t this jammer will have $|\mathcal{S}_t^*| = \kappa m - \kappa t$, $1 \leq t \leq m-1$, FH sequences in its search space. So, to force the jammer to be as fast as the jammer that listens on an active channels consecutively at each time slot, we should have $\kappa m - \kappa t$ active FH sequences for $2 \leq t \leq m-1$.

- Mixed fate jammer: If we have only one active FH sequence and such that $1 \leq \kappa m - \kappa t$, $2 \leq t \leq m-1$, then a mixed fate jammer will take at least two time slots to identify the active FH sequence. A mixed fate jammer was defined in terms of a jammer's luck changing from eavesdropping on an active channel to that which is inactive or vice versa.

3.4 Linear recurring sequences

In this section we consider an algebraic construction of an FH scheme provided by Lempel and Greenberger [55]. In this construction, a transformation of a maximum length sequence (m-sequence) provide optimal FH sequences in the Lempel-Greenberger bound (2.6). As described in Section 1.2.1 this bound and the analysis of the perfor-

mance of the FH sequences constructed by Lempel and Greenberger is based on Hamming correlation. We explore the performance of this FH scheme in terms of group-wise mutual interference. Further, we consider the effect of a (θ_1, θ_2)-adaptive jammer in the FH scheme.

3.4.1 Construction of m-sequences

We start by describing linear feedback shift registers, which are the building blocks of m-sequences. A *linear feedback shift register* (LFSR) is a device whose output value depends on a preceding input called the *state*. An LFSR can be used to generate a sequence satisfying a linear recurrence relation.

Definition 3.4.1. *Let p be a prime power. A sequence (x_t) of length $p^n - 1$, defined over $GF(p)$ satisfying the n-order linear recurring condition,*

$$x_{t+n} = c_0 x_t + c_1 x_{t+1} + \cdots + c_{n-1} x_{t+n-1}, c_i \in GF(p), c_{n-1} \neq 0,$$

is called a ***maximum length sequence*** *denoted m-sequence.*

To generate an m-sequence of order n over a finite field $GF(p)$ using a linear recurring sequence we need an *initial state* $B_0 = (b_0, b_1, \ldots, b_{n-1}) \neq (0, 0, \ldots, 0)$, where $b_i \in GF(p)$, $0 \leq i \leq n-1$. Note that if $B_0 = (b_0, b_1, \ldots, b_{n-1}) = (0, 0, \ldots, 0)$ then we get an all zero sequence since each output is a linear function of the previous state. An m-sequence has a maximum length of $p^n - 1$ with every n-state appearing once except the all zero n-state.

A formal construction of an m-sequence is as follows. Let p be a prime number. Let $GF(p)$ be a finite field of p elements. An **m-sequence** of degree n and period $v = p^n - 1$ is provided by:

$$B = \{b_j\}, \tag{3.30}$$

where $0 \leq j \leq v-1$ and b_j satisfies the linear recurrence relation:

$$\sum_{i=0}^{n} f_i b_{i+j} = 0,$$

where the coefficients are taken from the primitive polynomial over $GF(p)$:

$$f(z) = \sum_{i=0}^{n} f_i z^i.$$

Figure 3.3 depicts a feedback shift register (it is linear if the feedback function f is linear):

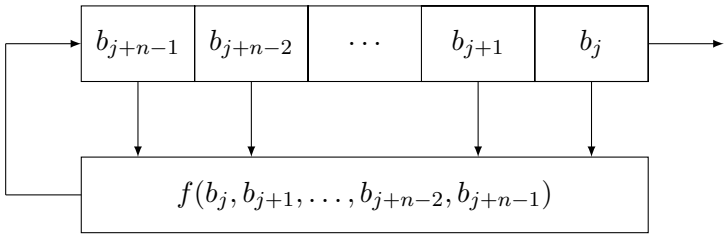

Figure 3.3: A feedback shift register.

Example 3.4.2. *Consider* $f(z) = 1 + 2z^2 + z^3$, *a primitive polynomial over* $\mathbb{F}_3$. *Then the linear recurrence of this primitive polynomial is:*

$$b_j + 2b_{j+2} + b_{j+3} = 0. \tag{3.31}$$

Expressing b_{j+3} *in Equation (3.31) in terms of preceding terms:*

$$b_{j+3} = b_{j+2} + 2b_j.$$

Let the string 100 *be an initial state, that is* $b_2 = 1, b_1 = 0, b_0 = 0$. *The m-sequence over* $\mathbb{F}_3$ *of degree* 3 *and period* 26 *is shown in Table 3.1:*

Time step, j	State, (b_{j+2}, b_{j+1}, b_j)	b_j
0	100	0
1	110	0
2	111	1
3	011	1
4	201	1
5	120	0
6	112	2
7	211	1
8	121	1
9	012	2
10	101	1
11	010	0
12	001	1
13	200	0
14	220	0
15	222	2
16	022	2
17	102	2
18	210	0
19	221	1
20	122	2
21	212	2
22	021	1
23	202	2
24	020	0
25	002	2

Table 3.1: Generating m-sequence of degree 3, period 26.

The m-sequence generated in Table 3.1 is:

$$X = (001110211210100222012212 02). \tag{3.32}$$

Example 3.4.3. *Consider* $f(z) = z^2 + 2z + 3$, *a primitive polynomial over* $\mathbb{F}_5$. *An m-sequence over* $\mathbb{F}_5$ *of degree* 2 *and length* 24 *with primitive polynomial* $f(z)$ *is:*

$$X = (013144134322042411021233). \tag{3.33}$$

3.4.2 Frequency hopping sequence: transform of an m-sequence

We now consider a construction of FH sequences using m-sequences.

Construction 3.4.4. *Let* p *be a prime number,* n *and* v *positive integers. Let* $X = (x_0, \ldots, x_{v-1})$ *be an m-sequence of degree* n *and length* $v = p^n - 1$ *over a prime field* $\mathbb{Z}_p$. *Let* i *be a positive integer such that* $1 \leq i \leq n$. *Let* $\mathbb{Z}_{p^i} = \{0, 1, \ldots, p^i - 1\}$ *and let* $\mathbb{Z}_p^i$ *be the set of all words of length* i *over* $\mathbb{Z}_p$. *Let* $X(t, i)$ *denote the* i*-tuple of successive elements in* X *starting from* x_t, *that is* $X(t, i) = x_t, x_{t+1}, \ldots, x_{t+i-1}$. *Define a sequence* $Y = (y_t)$ *of length* $v = p^n - 1$ *over* $\mathbb{Z}_{p^i}$ *as the* σ_i*-transform of an m-sequence* X*:*

$$y_t = X(t, i)\sigma_i = \sum_{k=0}^{i-1} x_{t+k} p^k, \tag{3.34}$$

where $0 \leq t < v$.

The σ_i-transform Y of an m-sequence X will be denoted by $Y = X\sigma_i$.

Example 3.4.5. *Consider the ternary m-sequence* X *of Equation (3.32). The* σ_i*-transform,* $i = 2, 3$, *of* X *over* $\mathbb{Z}_{3^2}$ *and* $\mathbb{Z}_{3^3}$ *respectively are:*

$$Y_1 = X\sigma_2 = (0, 3, 4, 4, 1, 6, 5, 4, 7, 5, 1, 3, 1, 0, 6, 8, 8, 2, 3, 7, 8, 5, 7, 2, 6, 2), \tag{3.35}$$

$$Y_2 = X\sigma_3 = (9, 12, 13, 4, 19, 15, 14, 22, 16, 5, 10, 3, 1, 18, 24, 26, 8, 11, 21, 25, 17, 23, 7, 20, 6, 2). \tag{3.36}$$

Construction 3.4.6. *Let Y be a σ_i-transform, $1 \leq i \leq n$, of an m-sequence of length $v = p^n - 1$. Then:*

$$\mathcal{S} = \overset{\Leftrightarrow}{Y}, \tag{3.37}$$

is a rotational closure $(p^n - 1, p^n - 1, m)$-FHS, where:

$$m = \begin{cases} p^i & \text{if } i < n, \\ p^i - 1 & \text{otherwise.} \end{cases}$$

Example 3.4.7. *Consider X to be the m-sequence of Equation (3.32). Given $Y = X\sigma_2$ of Equation (3.35), then $\overset{\Leftrightarrow}{Y}$ is a rotational closure $(26, 26, 9)$-FHS.*

3.4.3 Correlation

Let X be an m-sequence of length $v = p^n - 1$ over an alphabet of size p. For $i \geq n$, all the σ_i transforms of X provide sequences with distinct elements. So, cyclic shifts of the σ_i transform sequence for $i \geq n$ provide an FH scheme which is equivalent to a Latin square. A Latin square over an alphabet of size v is a square array such that each symbol occurs exactly once in each row and exactly once in each column. In Section 3.8 we consider a construction of FH sequences which uses Latin squares and they trivially satisfy the optimality criterion in terms of both Hamming correlation and Hamming group correlation. Henceforth, we consider $i \leq n$.

The *multiplicity* $\mu_X(x)$ of the i-tuple $x = X(t, i)$ in X is defined as:

$$\mu_X(x) = |\{t : x = X(t, i) \text{ in } X, 0 \leq t < v\}|.$$

That is $\mu_X(x)$ denotes the number of distinct positions t, for $0 \leq t < v$, where the i-tuple $x = X(t, i)$ appears in X.

Lemma 3.4.8. *(Lemple and Greenberger, Lemma 1, [55]). Consider an FH sequence Y defined over $\mathbb{Z}_{p^i}$, the σ_i transform of an m-sequence X, of length $v = p^n - 1$, where $1 \leq i \leq n$. Then each frequency $f_j \in \mathbb{Z}_{p^i}$ appears the following number of times on Y:*

$$\mu_Y(f_j) = \begin{cases} p^{n-i} - 1 & \text{if } f_j = 0, \\ p^{n-i} & \text{if } f_j \neq 0. \end{cases} \tag{3.38}$$

Proof. The proof is based on the fact that an m-sequence X has p^{n-i} distinct n-tuples $x' = x'_0, x'_1, \ldots, x'_{n-1}$ with $x = x'_0, x'_1, \ldots, x'_{i-1}$ and that the all-zero n-tuple does not exist on X. □

Lemma 3.4.9. *(Lempel and Greenberger, Lemma 3, [55]). Let Y be an FH sequence as defined in Construction 3.4.4. Then the Hamming correlation is:*

$$H_{YY}(t) = \begin{cases} v & \text{if } t = 0, \\ p^{n-i} - 1 & \text{if } t \neq 0. \end{cases} \tag{3.39}$$

Lemma 3.4.10. *Let $X = (x_t)$ be an m-sequence of length $v = p^n - 1$ over $\mathbb{Z}_p$, and let $Y = (y_t)$ be the σ_i-transform of X, for some $i \in \{0, 1, 2, \ldots, n-1\}$. Let $\mathcal{S} = \overleftrightarrow{Y}$ be a rotational closure $(p^n - 1, p^n - 1, p^i)$-FHS. For $Y_j, Y_{j'} \in \mathcal{S}$, $Y_j \neq Y_{j'}$, we have:*

$$G(Y_j, \{Y_{j'}\}) = p^{n-i} - 1.$$

Proof. Consider any two sequences $Y_j, Y_{j'} \in \mathcal{S}$, $j \neq j'$. Then the number of places in

which Y_j and $Y_{j'}$ are the same is provided by:

$$\begin{aligned} G(Y_j, \{Y_{j'}\}) &= H_{Y_j, Y_{j'}}(0) \\ &= \sum_{k=0}^{v-1} h[y_{k+j}, y_{k+j'}] \\ &= \sum_{k=0}^{v-1} h[y_k, y_{k+j'-j}] \\ &= H_{YY}(j'-j) \\ &= p^{n-i} - 1, \end{aligned}$$

since $j \neq j'$ and from Equation (3.39), $H_{YY}(t) = p^{n-i} - 1$ if $t \neq 0$. Therefore $G(Y_j, \{Y_{j'}\}) = p^{n-i} - 1$. □

Theorem 3.4.11. *Suppose $\mathcal{S} = \overleftrightarrow{Y}$ is a rotational closure $(p^n - 1, p^n - 1, p^i)$-FHS, where Y_j is a σ_i-transform of an m-sequence of length $v = p^n - 1$, $1 \leq i < n$. The worst-case w-throughput of $\mathcal{S}$ is at least*

$$1 - \frac{w(p^{n-i} - 1)}{p^n - 1}.$$

If $\hat{\rho}_w(\mathcal{S}) \geq 0$ then

$$w \leq \frac{p^n - 1}{(p^{n-i} - 1)}.$$

Proof. Suppose $\mathcal{U} \subseteq \mathcal{S}$, $|\mathcal{U}| = w$ and $Y_j \in \mathcal{S} \setminus \mathcal{U}$. Then for any $Y_{j'} \in \mathcal{U}$,

$$G(Y_j, \{Y_{j'}\}) = p^{n-i} - 1.$$

Then

$$G(Y_j, \mathcal{U}) \leq w(p^{n-i} - 1).$$

The w-throughput of an FH sequence Y_j in $\mathcal{V}$, $\mathcal{V} = \mathcal{U} \cup \{Y_j\}$ is:

$$\rho_w(Y_j, \mathcal{V} \setminus \{Y_j\}) = 1 - \frac{G(Y_j, \mathcal{V} \setminus \{Y_j\})}{v} \geq 1 - \frac{w(p^{n-i} - 1)}{p^n - 1}.$$

Then the worst-case w-throughput of $\mathcal{S}$ is:

$$\begin{aligned}\hat{\rho}_w(\mathcal{S}) &= \min_{\mathcal{V}\subseteq\mathcal{S}}\left\{\min_{Y_j\in\mathcal{V}}\{\rho_w(Y_j,\mathcal{V}\setminus\{Y_j\})\}\right\},\\ &= 1-\frac{w(p^{n-i}-1)}{p^n-1}.\end{aligned}$$

It must be the case that $w \leq \frac{p^n-1}{p^{n-i}-1}$, so that $\hat{\rho}_w(\mathcal{S}) \geq 0$.

□

3.4.4 Jamming resistance

In this section we look at how long it takes a $(\frac{1}{m},\frac{1}{m})$-adaptive jammer to identify an active FH sequence in an m-sequence transformation FH scheme of Construction 3.4.6.

We divide the discussion of the jamming resistance of the FH scheme into three parts. In Proposition 3.4.12 we consider a jammer that is lucky (listens on an active frequency channel) at each and every time slot consecutively. In Proposition 3.4.13 we consider a jammer that is unlucky (listens on an inactive frequency channel) at every time slot successively. Finally we conclude on the jamming resistance of the FH scheme in Theorem 3.4.14. We consider the situation where there is only one active FH sequence in use.

Proposition 3.4.12. *Consider the Lempel-Greenberger FH scheme in Construction 3.4.6. A jammer that is lucky at each and every time slot takes $n-i+1$ time slots to identify the active sequence.*

Proof. Let X be an m-sequence as previously defined. Without loss of generality we will consider non-zero i-tuples on m-sequence X.

Consider $b_j = (b_{j_0}, b_{j_1}, \ldots, b_{j_{i-1}})$, an i-tuple on X. Such an i-tuple appears p^{n-i} number of times on X if b_j is not the zero i-tuple.

Suppose at $t=0$ a jammer eavesdrops on an active channel $x_0 = f_j$, $f_j \in \mathcal{F}$, which is mapped under σ_i from b_j. From the relationship between X and Y, we know that at

$t = 1$ a jammer has p^{n-i} sequences in its search space, those with channel f_j at $t = 0$. The sequences discarded at this stage are inactive FH sequences.

Let b_{j+1} be the i-tuple succeeding b_j on X, that is $b_{j+1} = (b_{j_1}, \ldots, b_{j_{i-1}}, b_{j_i})$. There are p^{n-i-1} distinct i-tuples b_{j+1} with b_j as the preceding i-tuple. Then a jammer has p^{n-i-1} sequences in its search space at time slot $t = 2$ with an active channel that corresponds to b_{j+1} under σ_i. If we continue in this manner, at $t = n - i$ the jammer that is lucky at each of the $n - i$ preceding time slots will have FH sequences with distinct channels mapped from distinct i-tuples $b_{j+n-i} = (b_{n-i}, \ldots, b_{n-1})$.

Therefore a jammer that is lucky at each and every time slot can identify the active FH sequence in $n - i + 1$ time slots. □

Proposition 3.4.13. *If $w+1 \leq p^n - 1 - \sum_{j=0}^{n-i}(p-1)^j p^{n-i-j}$, a jammer that is unlucky at each and every time slot takes at least $n - i + 1$ time slots to identify the one active FH sequence.*

Proof. An unlucky jammer as previously described discards only sequences X_j with inactive frequency channels x_t at each time slot t. So,

at $t = 0$, $|\mathcal{S}_0^*| = p^n - 1$,

at $t = 1$, $|\mathcal{S}_1^*| = p^n - 1 - p^{n-i}$,

at $t = 2$, $|\mathcal{S}_2^*| = p^n - 1 - p^{n-i} - (p-1)p^{n-i-1}$,

at $t = 3$, $|\mathcal{S}_3^*| = p^n - 1 - p^{n-i} - (p-1)p^{n-i-1} - (p-1)^2 p^{n-i-2}$.

If we continue in this manner such that a jammer has been unlucky at each of the preceding κ time slots successively, $\kappa \in \{0, 1, \ldots, v-1\}$ then at $t = \kappa$, $|\mathcal{S}_\kappa^*| = p^n - 1 - \sum_{j=0}^{\kappa-1}(p-1)^j p^{n-i-j}$.

If we consider one active FH sequence, then taking $1 \leq p^n - 1 - \sum_{j=0}^{n-i}(p-1)^j p^{n-i-j}$ forces a jammer that is unlucky at each of the $n-i$ preceding time slots to take at least $n - i + 1$ time slots, as long as the all lucky jammer (discussed in Proposition 3.4.12), to identify an active FH sequence.

□

As discussed by Nyirenda, Ng and Martin [74], a mixed fate jammer will be as fast as either a jammer that is lucky or one which is unlucky at each and every time slot. A change in fate does not speed up things up for the (θ_1, θ_2)-adaptive jammer as it is forced to behave as an all lucky jammer; that is it can only start jamming if and only if there is one FH sequence in its search space.

We conclude the discussion of Propositions 3.4.12 and 3.4.13 with Theorem 3.4.14.

Theorem 3.4.14. *Consider Y, the σ_i transform of an m-sequence X of length $v = p^n - 1$, where $1 \leq i \leq n$. Consider $\mathcal{S} = \overleftrightarrow{Y}$ to be a rotational closure $(p^n - 1, p^n - 1, p^i)$-FHS. If we have one active FH sequence and $1 \leq p^n - 1 - \sum_{j=0}^{n-i}(m-1)^j p^{n-i-j}$, then a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer will identify an active sequence in at least $n - i + 1$ time slots.*

Example 3.4.15 illustrate Theorem 3.4.14.

Example 3.4.15. *Let X be a ternary m-sequence of Equation (3.32). Let Y be the σ_2-transform of X and $\mathcal{S} = \overleftrightarrow{Y}$ be a rotational closure $(26, 26, 9)$-FHS made up of Y and all its cyclic shifts. If we have one active FH sequence and since $1 < 26 - 3 = 23$, then $\gamma v \geq 2$.*

Consider a lucky jammer that eavesdrops on an active channel at each time slot consecutively. Suppose the jammer picks any symbol f on Y, which occurs 3 times (2 times if $f = 0$). However, the symbol that comes after f is always distinct. That is, if f occurs at time t_1, t_2, t_3, the symbols at time $t_1 + 1$, $t_2 + 1$, $t_3 + 1$ are always distinct. That means we can tell exactly where we are in a shift, that is we can tell which shifted sequence is being used if we can find two consecutive slots with active frequency channels.

Now we go further to determine the probability of identifying an active FH sequence in at least two time slots.

The probability that a jammer's first guess is active is:

$$Pr[\textit{ first guess is active }] = 1/26.$$

Next, the probability that the $(\frac{1}{m}, \frac{1}{m})$*-adaptive jammer's frequency channel guess on the second time slot is active given that it guessed correctly at the first time slot is:*

$$Pr[\ \textit{second guess is active} \mid \textit{first guess is active}\ ] = \begin{cases} 1/3 & \textit{if } f \neq 0 \textit{ at } t_0, \\ 1/2 & \textit{if } f = 0 \textit{ at } t_0. \end{cases}$$

Then the probability of identifying an active FH sequence in two time slots is:

$$\begin{aligned} & Pr[\ \textit{determining active sequence in 2 time slots}\ ] \\ & = Pr[\ \textit{first guess is active}\ ] * Pr[\ \textit{second guess is active}\ ] \\ & = \begin{cases} 1/26 * 1/3 & \textit{if } f \neq 0 \textit{ at } t_0, \\ 1/26 * 1/2 & \textit{if } f = 0 \textit{ at } t_0. \end{cases} \end{aligned}$$

That is $Pr[\ \textit{determining active sequence in 2 time slots}\ ] \geq 1/26 * 1/3$.

Therefore if we have one active FH sequence then $\gamma v \geq 2$ *for a* $(1/m, 1/m)$*-adaptive jammer,* $m = p^i$*, with probability greater than* $\frac{1}{78}$.

We conclude this section with a note on the worst-case w-throughput of a rotational closure (v, v, m)-FHS based on m-sequences and resistance against a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer of an FH scheme. There is a trade-off between the worst-case w-throughput of an FH scheme, which is an m-transform, and its resistance to a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer. From Theorem 3.4.11 we have $\hat{\rho}_w(\mathcal{S}) \geq 1 - \frac{w(p^{n-i}-1)}{p^n-1}$. So we would like i large in order to maximise $\hat{\rho}_w(\mathcal{S})$. On the other hand, we have the minimum number of time slots to resist a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer as $n - i + 1$. Therefore we would like i to be small so that the FH scheme resists the jammer longer.

3.5 Cyclotomy

In this section we consider the construction of FH schemes via cyclotomy.

The research that exists in the literature that employs cyclotomic numbers to con-

struct FH sequences includes [19, 22, 29, 40, 57, 87, 116, 117]. Chu and Colbourn [19] developed FH sequences over a prime field, $\mathbb{F}_p$. Using interleaving techniques Chung et al. [21] obtained FH sequences of twice the length of those obtained by Chu and Colbourn [19]. Ding and Yin [29] generalised Chu and Colbourn's construction to a prime power field, $\mathbb{F}_{p^n}$. Han and Yang [40] provided corrections to some of Ding and Yin's constructions. Zhang [117] used cyclotomy over $\mathbb{F}_{2^n}$ and the Chinese remainder theorem to construct FH sequences. Chung and Yang [22] obtained FH sequences with odd prime length. Zeng, Cai, Tang and Yang [115] also constructed FH sequences of odd length. Liu, Peng, Zhou and Tang [57] used generalized cyclotomy to construct FH sequences. Ren, Fu and Zhou [87] used cyclotomy and the Chinese remainder theorem to generalise some of the existing constructions [29] and [117]. Further, the authors of [87] also constructed sets of FH sequences.

In this section we look at the construction by Chu and Colbourn [19] as this is one of the early works employing cyclotomic numbers, and is a special case of most of the constructions that use cyclotomy to obtain FH sequences. The authors first construct FH sequences that meet the Lempel-Greenberger bound (2.6). That is, the FH sequences are optimal with respect to the maximum Hamming auto-correlation.

3.5.1 Cyclotomic classes

Let $v = mf + 1$ be an odd prime. Let $\mathbb{F}_v$ be a finite field and $\mathbb{F}_v^*$ the set of nonzero elements of $\mathbb{F}_v$.

Definition 3.5.1. *Let α be a primitive element of $\mathbb{F}_v$. The **cyclotomic classes** of $\mathbb{F}_v$ of order m:*

$$C_i = \{\alpha^{tm+i} : 0 \leq t \leq f-1\}, \qquad i = 0, 1, \ldots, m-1,$$

are the m disjoint subsets that partition $\mathbb{F}_v^*$.

Definition 3.5.2. *The **cyclotomic numbers** of order m are:*

$$(i,j) = |(C_i + 1) \cap C_j|,$$

where $0 \leq i, j \leq m-1$ and addition in a class is defined by:

$$C_i + 1 = \{c_i + 1 \ (mod\ v) : c_i \in C_i\}.$$

The cyclotomic numbers (i,j), $0 \leq i,j \leq m-1$, of order m, are the number of solutions to the equation:

$$c_i + 1 = c_j, \qquad c_i \in C_i, c_j \in C_j.$$

That is, (i,j) is the number of ordered pairs s,t such that:

$$\alpha^{ms+i} + 1 = \alpha^{mt+j}, \qquad 0 \leq s,t \leq f-1.$$

For the interested reader see [100] for an introduction to cyclotomy.

3.5.2 Construction of FH sequences with cyclotomic classes

In this section we will use the combinatorial characterisation of an FH sequence which was introduced in Section 3.3.1. We associate an FH sequence $X = (x_0, x_1, \ldots, x_{v-1})$ defined over an alphabet $\mathcal{F}$, $|\mathcal{F}| = m$, with m disjoint sets $B_0, B_1, \ldots, B_{m-1}$, where each B_i is the *support* of i, $i \in \mathcal{F}$ defined in Equation (3.27).

Construction 3.5.3. *Let $v = mf + 1$. Let $\mathcal{F} = \mathbb{Z}_m$ be a frequency library. Let $C_0, C_1, \ldots, C_{m-1}$ be the cyclotomic classes of $\mathbb{F}_v$ of order m. An FH sequence $X =$*

$(x_0, x_1, \ldots, x_{v-1})$ over $\mathcal{F}$ is given as:

$$\begin{aligned} B_0 &= C_0 \cup \{0\}, \\ B_i &= C_i, \qquad 1 \le i \le m-1, \end{aligned} \tag{3.40}$$

with the sets B_0, B_i, $1 \le i \le m-1$ as previously defined. The FH sequence together with all its cyclic shifts form an $(mf+1, mf+1, m)$-FHS.

Note that the FH sequence $X = (x_t)$ can also be written as:

$$x_t = \begin{cases} 0 & \text{if } t = 0, \\ i & \text{if } t \in C_i. \end{cases}$$

Example 3.5.4. *Let $|\mathcal{F}| = 7$ and $v = 29$. The cyclotomic classes of $\mathbb{F}_{29}$ of order 7 are:*

$C_0 = \{1, 12, 28, 17\}$, $C_1 = \{2, 24, 27, 5\}$, $C_2 = \{4, 19, 25, 10\}$, $C_3 = \{8, 9, 21, 20\}$,
$C_4 = \{16, 18, 13, 11\}$, $C_5 = \{3, 7, 26, 22\}$, $C_6 = \{6, 14, 23, 15\}$.

An FH sequence of length 29 over $\mathcal{F}$ is:

$$X = (0, 0, 1, 5, 2, 1, 6, 5, 3, 3, 2, 4, 0, 4, 6, 6, 4, 0, 4, 2, 3, 3, 5, 6, 1, 2, 5, 1, 0).$$

Example 3.5.5. *Let $|\mathcal{F}| = 23$ and $v = 47$. The cyclotomic classes of $\mathbb{F}_{47}$ of order 23 are:*

$C_0 = \{1, 46\}$, $C_1 = \{5, 42\}$, $C_2 = \{22, 25\}$, $C_3 = \{16, 31\}$, $C_4 = \{14, 33\}$,
$C_5 = \{23, 24\}$, $C_6 = \{21, 26\}$, $C_7 = \{11, 36\}$, $C_8 = \{8, 39\}$, $C_9 = \{7, 40\}$,
$C_{10} = \{12, 35\}$, $C_{11} = \{13, 34\}$, $C_{12} = \{18, 29\}$, $C_{13} = \{4, 43\}$, $C_{14} = \{20, 27\}$,
$C_{15} = \{6, 41\}$, $C_{16} = \{17, 30\}$, $C_{17} = \{9, 38\}$, $C_{18} = \{2, 45\}$, $C_{19} = \{10, 37\}$,
$C_{20} = \{3, 44\}$, $C_{21} = \{15, 32\}$, $C_{22} = \{19, 28\}$.

Then an FH sequence of length 47 *over an alphabet of size 23 is:*

$$X = (0, 0, 18, 20, 13, 1, 15, 9, 8, 17, 19, 7, 10, 11, 4, 21, 3, 16, 12, 22, 14, 6, 2, 5, 5,$$
$$2, 6, 14, 22, 12, 16, 3, 21, 4, 11, 10, 7, 19, 17, 8, 9, 15, 1, 13, 20, 18, 0).$$

3.5.3 Correlation

Lemma 3.5.6 is used in the determination of the maximum Hamming auto-correlation of an FH sequence constructed using cyclotomic techniques. Lemma 3.5.6 exists in the literature [19] without proof, so we provide a proof here.

Lemma 3.5.6. *Let* $\mathbb{F}_v$ *be a finite field,* $v = mf+1$ *an odd prime. The cyclotomic classes* C_i, $0 \leq i \leq m-1$, *of* $\mathbb{F}_v$ *of order* m *satisfy the following property,* $|(C_i + w) \cap C_j| = |(w^{-1}C_i + 1) \cap w^{-1}C_j|$. *If* $w^{-1} \in C_h$, *then:*

$$|(C_i + w) \cap C_j| = (i + h, j + h).$$

Proof. For all $0 \leq i \leq m-1$, the cyclotomic classes C_i can be written in terms of the cyclotomic class C_0:

$$\begin{aligned} C_0 &= \langle \alpha^m \rangle \\ &= \{\alpha^{mt} : 0 \leq t \leq f-1\}; \\ C_i &= \alpha^i C_0 \\ &= \{\alpha^i \cdot \alpha^{mt} : 0 \leq t \leq f-1\} \\ &= \{\alpha^{mt+i} : 0 \leq t \leq f-1\}. \end{aligned}$$

If $w^{-1} \in C_h$ then $w^{-1} = \alpha^{mt_1+h}$ for some $t_1 \in \{0, \ldots, f-1\}$. Now,

$$w^{-1}C_j = \{\alpha^{m(t_1+t_2)+h+j} : 0 \leq t_2 \leq f-1\},$$

$$w^{-1}C_i + 1 = \{\alpha^{m(t_1+t_3)+h+i} + 1 : 0 \leq t_3 \leq f-1\}.$$

Next,

$$C_{j+h} = \{\alpha^{mt_4+h+j} : 0 \leq t_4 \leq f-1\},$$

$$C_{i+h} = \{\alpha^{mt_5+h+i} : 0 \leq t_5 \leq f-1\}.$$

For any $w^{-1} \in C_h$ we have $w^{-1}C_j = C_{j+h}$. Therefore,

$$|(w^{-1}C_i + 1) \cap w^{-1}C_j| = |(C_{i+h} + 1) \cap C_{j+h}| = (i+h, j+h).$$

The conclusion then follows:

$$|(C_i + w) \cap C_j| = |(w^{-1}C_i + 1) \cap w^{-1}C_j| = (i+h, j+h).$$

□

Theorem 3.5.7 provide the maximum Hamming correlation of the FH sequence (3.40). We make a correction on the lower limit of the summation for the formula of maximum Hamming correlation provided by Chu et al. [19] and we provide a proof of the theorem.

Theorem 3.5.7. *(Theorem 1, [19]). Let X be an FH sequence of length $v = mf + 1$ given in Construction 3.5.3. Then X is a Lempel-Greenberger optimal FH sequence (Definition 2.2.12), where the maximum Hamming auto-correlation is:*

$$H(X) = \begin{cases} \sum_{i=1}^{m-1}(i,i) + 1 & \text{if } f \text{ odd}, \\ \sum_{i=1}^{m-1}(i,i) + 2 & \text{if } f \text{ even}. \end{cases} \tag{3.41}$$

Proof. The maximum Hamming auto-correlation is:

$$H(X) = \max_{1 \leq t \leq v-1} \{H_{X,X}(t)\},$$

where $H_{X,X}(t)$ is the intersection of X and its t cyclic shift to the right given by:

$$\begin{aligned} H_{X,X}(t) &= \sum_{i=0}^{m-1} |(B_i + t) \cap B_i| \\ &= |B_0 \cap (B_0 + t)| + \sum_{i=1}^{m-1} |(B_i + t) \cap B_i|. \end{aligned} \tag{3.42}$$

By definition, from Equation (3.40), $B_0 = C_0 \cup \{0\}$, $B_i = C_i$, $1 \leq i \leq m-1$.

The shifted version of B_0 to the right by t places is $B_0 + t = (C_0 + t) \cup \{0 + t\}$. The number of places in which $B_0 + t$ and B_0 intersect is:

$$\begin{aligned} (B_0 + t) \cap B_0 &= |(C_0 \cup \{0\}) \cap ((C_0 + t) \cup \{0 + t\})| \\ &= |(C_0 \cup \{0\}) \cap ((C_0 + t) \cup \{t\})| \\ &= |\,((C_0 \cup \{0\}) \cap (C_0 + t)) \cup ((C_0 \cup \{0\}) \cap \{t\})\,| \\ &= |\,((C_0 + t) \cap C_0) \cup ((C_0 + t) \cap \{0\}) \cup (\{t\} \cap C_0) \cup (\{t\} \cap \{0\})\,|. \end{aligned}$$

For all $t \neq 0$,

$$\begin{aligned} ((C_0 + t) \cap C_0) &= \emptyset, \\ (\{t\} \cap \{0\}) &= \emptyset, \\ \text{and } ((C_0 + t) \cap \{0\}) \cap (\{t\} \cap C_0) &= \emptyset. \end{aligned}$$

So,

$$|\,((C_0 + t) \cap \{0\}) \cup (\{t\} \cap C_0)\,| = |\,((C_0 + t) \cap \{0\})\,| + |\,(\{t\} \cap C_0)\,|.$$

Therefore,

$$(B_0 + t) \cap B_0 = |\,((C_0 + t) \cap \{0\})\,| + |\,(\{t\} \cap C_0)\,|.$$

Then

$$H_{X,X}(t) = |\{t\} \cap C_0| + |\{0\} \cap (C_0 + t)| + \sum_{i=1}^{m-1} |(C_i + t) \cap C_i|.$$

From Lemma 3.5.6, if $t^{-1} \in C_h$ then

$$\sum_{i=1}^{m-1} |(C_i + t) \cap C_i| = \sum_{i=1}^{m-1} (i+h, i+h) = \sum_{i=1}^{m-1} (i, i).$$

Finally, $|\{t\} \cap C_0| + |\{0\} \cap (C_0 + t)|$ is maximum when f is even where $t, -t \in C_0$. That is:

$$|\{t\} \cap C_0| + |\{0\} \cap (C_0 + t)| = 2$$

when f is even. On the other hand when f is odd:

$$|\{t\} \cap C_0| + |\{0\} \cap (C_0 + t)| = 1.$$

This completes the proof. □

It was shown in [19] that the FH sequences in Construction 3.5.3 are optimal with respect to the Lempel-Greenberger bound (2.6) on the maximum out-of-phase Hamming auto-correlation.

Hamming Group correlation. Let $\mathcal{S}$ be a $(mf+1, mf+1, m)$-FHS of Construction 3.5.3. The Hamming group correlation can be estimated as:

$$G(X, \mathcal{U}) \leq wH(X),$$

where $\mathcal{U} \subseteq \mathcal{S}$, $|\mathcal{U}| = w$, $X \in \mathcal{S} \backslash \mathcal{U}$ and $H(X)$ is the maximum Hamming auto-correlation given in Equation (3.41). Then the lower bound for the w-throughput of X is:

$$\rho_w(X, \mathcal{U}) \geq 1 - \frac{wH(X)}{mf+1}.$$

Further, the worst-case w-throughput of $\mathcal{S}$ is:

$$\begin{aligned}\hat{\rho}_w(\mathcal{S}) &= \min_{\mathcal{V}\subseteq\mathcal{S}}\left\{\min_{X\in\mathcal{V}}\{\rho_w(X,\mathcal{V}\setminus\{X\})\}\right\}\\ &= 1-\frac{w(H(X))}{mf+1},\end{aligned}$$

where $X\in\mathcal{V}$, $\mathcal{V}=\mathcal{U}\cup\{X\}$ and $\rho_w(X,\mathcal{V}\setminus\{X\})=1-\frac{G(X,\mathcal{V}\setminus\{X\})}{v}$.

3.5.4 Jamming resistance

In the definition of an FH sequence, the size of the supports of frequency channels are $|B_0|=f+1$ and $|B_i|=f$, $1\leq i\leq m-1$, with B_0,B_i as previously defined. That is every frequency channel, except 0, appears f number of times in the FH sequence. The 0 channel appears one time slot more than the others. Then the probability that a $(\frac{1}{m},\frac{1}{m})$-adaptive jammer listens on an active frequency channel was given in Equation (2.39):

$$Prob(i \text{ is active}) = 1-\binom{k-a_i}{w+1}\Big/\binom{k}{w+1},$$

where a_i is the number of times that frequency channel i appears at a particular time slot of interest, and w is the number of active FH sequences. For the FH scheme in Construction 3.5.3 we have:

$$Prob(i \text{ is active}) \geq 1-\binom{mf+1-f}{w+1}\Big/\binom{mf+1}{w+1}. \tag{3.43}$$

3.6 Trace functions

A number of FH sequence constructions based on trace functions have been proposed over the years, [27, 28, 37, 109]. In this section we consider a construction by Ge et al. [37], which is a generalisation of some known FH sequences constructions that use trace functions.

3.6.1 Preliminaries

Definition 3.6.1. *For $\beta \in \mathbb{F}_{m^n}$ and $\mathbb{F}_{m^\kappa}$, $\kappa|n$, the **trace function** $Tr_{m^n/m^\kappa}(\beta)$ of β over $\mathbb{F}_{m^\kappa}$ is the map defined by:*

$$Tr_{m^n/m^\kappa}(\beta) = \beta + \beta^{m^\kappa} + \ldots + \beta^{m^{\kappa(\frac{n}{\kappa}-1)}},$$

*from $\mathbb{F}_{m^n}$ to the subfield $\mathbb{F}_{m^\kappa}$. If $\mathbb{F}_{m^\kappa}$ is the prime subfield of $\mathbb{F}_{m^n}$, then $Tr_{m^n/m^\kappa}(\beta)$ is called the **absolute trace** function, which will be simply called the trace function in this section as it is the only trace function we consider and is denoted by $Tr_{m^n}(\beta)$.*

A trace function is a map that enables a transfer of elements from a finite field to its subfield.

Let $F = \mathbb{F}_{m^n}$ and $K = \mathbb{F}_m$. For the remainder of this section we will denote the trace function as $Tr_{F/K}(\beta)$. We state Lemmas 3.6.2 and 3.6.3 of properties of trace functions [56], which will be used in the subsequent sections.

Lemma 3.6.2. *The trace function satisfies the following properties:*

i $Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$ *for all* $\alpha, \beta \in F$;

ii $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha)$ *for all* $c \in K$, $\alpha \in F$;

iii $Tr_{F/K}(c) = nc$, *for all* $c \in K$;

iv $Tr_{F/K}(\alpha^m) = Tr_{F/K}(\alpha)$, *for all* $\alpha \in F$.

Lemma 3.6.3. *The trace function is an m^{n-1}-to-1 map.*

3.6.2 Frequency hopping sequences obtained using trace functions

In this section we consider the construction of Ge et al. [37, Section V] which provided more parameters and is a generalization of many other constructions that use trace functions.

Construction 3.6.4. *Let $m = p^r$, p be a prime and r be some positive integer. Let n, l be two positive integers such that $l|(m^n - 1)$ and $gcd(\frac{m^n-1}{m-1}, l) = 1$. Let α be a primitive element of the field $F = \mathbb{F}_{m^n}$. Let s be a positive integer such that $gcd(s, m^n - 1) = 1$ and $\beta = \alpha^{ls}$. Let $v = \frac{m^n-1}{l}$. An FH sequence over the field $K = \mathbb{F}_m$ of length v is defined as*

$$X_g = (Tr_{F/K}(g), Tr_{F/K}(g\beta), \ldots, Tr_{F/K}(g\beta^{v-1})), \tag{3.44}$$

for all $g \in F$. The FH scheme defined by Equation (3.44):

$$\mathcal{S} = \{X_g : 0 \leq g \leq m^n - 1\},$$

form a rotational closure $(\frac{m^n-1}{l}, \frac{m^n-1}{l}, m)$-FHS.

3.6.3 Correlation

Lemma 3.6.5 provides the Hamming correlation of the sequence defined in Equation (3.44).

Lemma 3.6.5. *(Ge et al., [37],Lemma 4.3). Let X_g be an FH sequence defined in Equation (3.44). Its maximum out-of-phase Hamming correlation is:*

$$H(X_g) = \frac{m^{n-1} - 1}{l}, \tag{3.45}$$

with $g \in \mathbb{F}^*_{m^n}$.

Now we consider the maximum Hamming cross-correlation of two distinct FH sequences X_g, X_h.

Theorem 3.6.6. *(Ge et al., [37],Theorem 4.5). If g, h belong to distinct cyclotomic classes of order l in $\mathbb{F}_{m^n}$, then X_g and X_h constitute a Lempel-Greenberger optimal pair (Definition 2.2.13) of FH sequences where the maximum Hamming cross-correlation is $\frac{m^{n-1}-1}{l}$.*

Note that if g, h as defined in Theorem 3.6.6 belong to the same cyclotomic classes then $H(X_g, X_h) = \frac{m^n-1}{l} = v$. Then Ge et al. [37] provided a revision of Construction 3.6.4 to consider a subset of the FH sequences so that the maximum Hamming cross-correlation is improved.

Construction 3.6.7. *(Ge et al., [37],Theorem 4.7). Let $\{g_0, g_1, \ldots, g_{l-1}\}$ be a complete set of representatives for the cyclotomic classes of order l in $\mathbb{F}_{m^n}$. Then:*

$$\mathcal{S} = \{X_{g_0}, X_{g_1}, \ldots, X_{g_{l-1}}\},$$

is a $(\frac{m^n-1}{l}, l, m)$-FHS with maximum Hamming correlation $\frac{m^{n-1}-1}{l}$.

Example 3.6.8. *Let $m = |\mathcal{F}|$, $m \equiv 1 \pmod 4$, $n = 2$, $l = 2(m-1)$, $v = \frac{m+1}{2}$. Then Construction 3.6.7 provides a $(\frac{m+1}{2}, m^2, m)$-FHS with Hamming correlation 1.*

Theorem 3.6.9. *For a $(\frac{m^n-1}{l}, l, m)$-FHS given by Equation (3.44), the worst-case w-throughput is at least $1 - \frac{w(m^{n-1}-1)}{m^n-1}$.*

Example 3.6.10. *Let $m = p = 23$. If $n = 2$ then consider $l = 11$ and $v = 48$. We have a $(48, 11, 23)$-FHS with Hamming correlation 2 and a worst-case w-throughput of at least $1 - \frac{w}{24}$.*

Hamming group correlation. Let $\mathcal{S}$ be a rotational closure $(\frac{m^n-1}{l}, \frac{m^n-1}{l}, m)$-FHS of Construction 3.6.4. The Hamming group correlation can be estimated as:

$$G(X,\mathcal{U}) \leq wH(X),$$

where $\mathcal{U} \subseteq \mathcal{S}$, $|\mathcal{U}| = w$, $X \in \mathcal{S} \backslash \mathcal{U}$ and $H(X)$ is the maximum Hamming auto-correlation given in Equation (3.45). Then the lower bound for the w-throughput of X is:

$$\rho_w(X,\mathcal{U}) \geq 1 - \frac{wH(X)}{v} \tag{3.46}$$

$$= 1 - \frac{w(m^{n-1}-1)}{m^n-1}. \tag{3.47}$$

Further, the worst-case w-throughput of $\mathcal{S}$ is:

$$\begin{aligned}\hat{\rho}_w(\mathcal{S}) &= \min_{\mathcal{V}\subseteq\mathcal{S}}\left\{\min_{X\in\mathcal{V}}\{\rho_w(X,\mathcal{V}\setminus\{X\})\}\right\}\\ &= 1-\frac{w(H(X))}{v}\\ &= 1-\frac{w(m^{n-1}-1)}{m^n-1}\end{aligned}$$

where $X\in\mathcal{V}$, $\mathcal{V}=\mathcal{U}\cup\{X\}$ and $\rho_w(X,\mathcal{V}\setminus\{X\})=1-\frac{G(X,\mathcal{V}\setminus\{X\})}{v}$.

3.6.4 Jamming resistance

Consider Construction 3.6.4. From Lemma 3.6.3 we deduce that each channel in $\mathcal{F}$ appears m^{n-1} number of times at each time slot. We now consider how a $(\frac{1}{m},\frac{1}{m})$-adaptive jammer will affect an FH scheme at a single time slot.

The probability that a $(\frac{1}{m},\frac{1}{m})$-adaptive jammer listens on an active channel was given in Equation (2.39):

$$Prob(i \text{ is active}) = 1-\binom{k-a_i}{w+1}\Big/\binom{k}{w+1},$$

where a_i is the number of times that frequency channel i appears at a particular time slot of interest. For the construction considered in this section we have:

$$Prob(i \text{ is active}) = 1-\binom{m^n-m^{n-1}}{w+1}\Big/\binom{m^n}{w+1}. \tag{3.48}$$

Now consider the modified FH scheme of Construction 3.6.7, a $(\frac{m^n-1}{l},l,m)$-FHS. Recall that the l representatives for the cyclotomic classes of order l in $\mathbb{F}_{m^n}$ are chosen randomly. Then we have $1\leq a_i\leq\min\{m^{n-1},l\}$ and Equation (3.48) can be modified accordingly.

3.6.5 Comparison with m-sequences

It is well known that m-sequences can be defined in terms of the trace function. Let $X = (x_t)$ be an m-sequence of length $v = m^n - 1$ over $GF(m^n)$. Let α be a primitive element of the field $GF(m^n)$, that is an element of order $m^n - 1$. Then $x_t = a\alpha^t + (a\alpha^t)^m + (a\alpha^t)^{m^2} + \ldots (a\alpha^t)^{m^{n-1}}$ and thus an i-tuple of X is given as:

$$(x_t, x_{t+1}, \ldots, x_{t+i-1}) = (Tr(\delta), Tr(\delta\alpha), \ldots, Tr(\delta\alpha^{i-1})),$$

where $\delta = a\alpha^t$, $a \in GF(m^n) \setminus \{0\}$.

Recall the FH sequence construction considered in this section, Construction 3.6.4, provides the FH sequence:

$$X_g = (Tr_{F/K}(g), Tr_{F/K}(g\beta), \ldots, Tr_{F/K}(g\beta^{v-1})), \tag{3.49}$$

where $\beta = \alpha^{ls}$. Note that when $l = 1$ and $s = 1$, Equation (3.49) provides an m-sequence.

Example 3.6.11. *Let $p = 3$, $n = 3$ and $\mathbb{F}_{3^3}$ be an extension field of $\mathbb{F}_3$. Let α be a primitive element of $\mathbb{F}_{3^3}$. Using Construction 3.6.4, we can obtain the following FH sequence of length 26 defined over $\mathbb{F}_3$:*

$$X_i = (Tr_{3^2/3}(\alpha^t)),$$

where $0 \leq t \leq v - 1$. Then:

$$X_i = (0, 0, 2, 0, 2, 1, 2, 2, 1, 0, 2, 2, 2, 0, 0, 1, 0, 1, 2, 1, 1, 2, 0, 1, 1, 1),$$

is an m-sequence.

3.7 Reed-Solomon codes

In this section we consider FH scheme constructions which use Reed-Solomon codes [27, 91, 94, 114]. The FH schemes obtained in this section are subcodes of Reed-Solomon codes. A *subcode* is a code contained in another code.

3.7.1 Preliminaries

We first define a Reed-Solomon code.

Definition 3.7.1. *Let v and κ be integers where $v \geq 2$ and $\kappa \geq 2$. Let m be a prime power such that $m \geq v$. Let $\mathcal{F}$ be the finite field of cardinality m and α a primitive element. Let $f(x) = f_0 + f_1 x + \ldots + f_{\kappa-1}x^{\kappa-1}$ be a polynomial, where $f_i \in \mathcal{F}$ for all $0 \leq i \leq \kappa - 1$. A length v and κ dimensional Reed-Solomon code, denoted (v, κ)-Reed-Solomon code, $\mathcal{S}$ over $\mathcal{F}$ is:*

$$\mathcal{S} = \left\{ \left(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{v-1}) \right) \right\}, \tag{3.50}$$

where the generator matrix of the code is represented as:

$$G = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{v-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(v-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{\kappa-1} & \alpha^{2(\kappa-1)} & \cdots & \alpha^{(\kappa-1)(v-1)} \end{pmatrix}.$$

3.7.2 Subcode of Reed-Solomon code as an FH scheme

Consider a (v, κ)-Reed-Solomon code C. Define an equivalence relation on the codewords of C such that two codewords X, Y are said to be *equivalent* if one codeword can be obtained from the other by some cyclic shifts, that is $Y = \beta^i X$ and $X = \beta^j Y$, for some $i, j \in \{0, 1, \ldots, v-1\}$ and where β is a cyclic permutation function defined in

Equation (3.28). An equivalence class obtained by this relation contains all codewords $\beta^i X$, $0 \leq i \leq v-1$, $X \in C$. The codewords in an equivalence class are said to be *cyclic equivalent codewords*.

Let C be a (v, κ)-Reed-Solomon code with parameters as previously defined. By choosing one codeword from each equivalence class of C, we can obtain a subcode of C, which we denote C'. The subcode C' has a property that any two distinct codewords have the same symbols in at most $\kappa - 1$ corresponding coordinates.

We are interested in representative codewords with full period. A codeword is said to have *full period* if $\beta^i X \neq \beta^j X$, for $0 \leq i, j \leq v-1$. So, we consider equivalence classes of maximum size v. So, let C'' be a subset of C' containing codewords of full period. In the literature the subcode C'' of C formed by picking one element from each equivalence class of full order is called a *cyclically permutable code*. The subcode C'' has an additional property that any two distinct cyclic shifts of a single codeword have the same symbols in at most $\kappa - 1$ corresponding coordinates. That is, the maximum out-of-phase Hamming auto-correlation of a codeword is $\kappa - 1$.

Corollary 3.7.2 provides the size of the subcode C''.

Corollary 3.7.2. *(Song and Golomb, [94], Corollary 2.1) Given m and κ such that $1 \leq \kappa \leq m-2$, let $N = |\{i : \gcd(i, m-1) = 1, 1 \leq i \leq \kappa\}|$. If $m-1$ is a prime power then:*

$$|C''| = \frac{m^\kappa - m^{\kappa - N}}{m-1}. \tag{3.51}$$

Construction 3.7.3. *Consider a (v, κ)-Reed Solomon C with parameters as previously defined. A subcode C'' of C made up of representative codewords from each equivalence classes of maximum size v is considered as a (v, k, m)-FHS where $v = m-1$ and k is given by Equation (3.51).*

Several authors have obtained FH schemes with Construction 3.7.3. Reed [86, 91] obtained FH schemes using Construction 3.7.3 with $k \geq m^{\kappa-1}$ FH sequences. Ding et al. [27] consider the same construction when $m-1$ is a prime number and thus obtain

a $(v, \frac{m^\kappa-1}{m-1}, m)$-FHS. Yang, Tang, Parampalli and Peng [114] used the same idea of Construction 3.7.3 to obtain an FH scheme from punctured Reed-Solomon codes. For the remainder of this section we consider Reed's construction [86] since it does not put any restriction on the length of the FH sequences or the size of the FH scheme (there is no restriction on the alphabet on which the Reed-Solomon code is defined).

Example 3.7.4. *Let C be a $(m-1, 2)$-Reed-Solomon code with generator matrix*

$$G = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{m-2} \end{pmatrix},$$

where α is a primitive element of a field $\mathcal{F}$, $|\mathcal{F}| = m$. Using Reed's construction [86], we have m FH sequences:

$$X_i = (\delta_i, \delta_i, \ldots, \delta_i) + (1, \alpha, \alpha^2, \ldots, \alpha^{m-2}), \tag{3.52}$$

for $\delta_i \in \mathcal{F}$ and $0 \leq i \leq m-1$.

As a specific case of Construction 3.7.3, we have the following FH sequences over an alphabet of size 23, using a $(22, 2)$-Reed-Solomon code, where a random codeword was selected from each equivalence class of maximum size:

$$(1, 5, 2, 10, 4, 20, 8, 17, 16, 11, 9, 22, 18, 21, 13, 19, 3, 15, 6, 7, 12, 14),$$
$$(2, 6, 3, 11, 5, 21, 9, 18, 17, 12, 10, 0, 19, 22, 14, 20, 4, 16, 7, 8, 13, 15),$$
$$(3, 7, 4, 12, 6, 22, 10, 19, 18, 13, 11, 1, 20, 0, 15, 21, 5, 17, 8, 9, 14, 16),$$
$$(4, 8, 5, 13, 7, 0, 11, 20, 19, 14, 12, 2, 21, 1, 16, 22, 6, 18, 9, 10, 15, 17),$$
$$(5, 9, 6, 14, 8, 1, 12, 21, 20, 15, 13, 3, 22, 2, 17, 0, 7, 19, 10, 11, 16, 18),$$
$$(6, 10, 7, 15, 9, 2, 13, 22, 21, 16, 14, 4, 0, 3, 18, 1, 8, 20, 11, 12, 17, 19),$$
$$(7, 11, 8, 16, 10, 3, 14, 0, 22, 17, 15, 5, 1, 4, 19, 2, 9, 21, 12, 13, 18, 20),$$
$$(8, 12, 9, 17, 11, 4, 15, 1, 0, 18, 16, 6, 2, 5, 20, 3, 10, 22, 13, 14, 19, 21),$$
$$(9, 13, 10, 18, 12, 5, 16, 2, 1, 19, 17, 7, 3, 6, 21, 4, 11, 0, 14, 15, 20, 22),$$
$$(10, 14, 11, 19, 13, 6, 17, 3, 2, 20, 18, 8, 4, 7, 22, 5, 12, 1, 15, 16, 21, 0),$$

$$(11, 15, 12, 20, 14, 7, 18, 4, 3, 21, 19, 9, 5, 8, 0, 6, 13, 2, 16, 17, 22, 1),$$
$$(12, 16, 13, 21, 15, 8, 19, 5, 4, 22, 20, 10, 6, 9, 1, 7, 14, 3, 17, 18, 0, 2),$$
$$(13, 17, 14, 22, 16, 9, 20, 6, 5, 0, 21, 11, 7, 10, 2, 8, 15, 4, 18, 19, 1, 3),$$
$$(14, 18, 15, 0, 17, 10, 21, 7, 6, 1, 22, 12, 8, 11, 3, 9, 16, 5, 19, 20, 2, 4),$$
$$(15, 19, 16, 1, 18, 11, 22, 8, 7, 2, 0, 13, 9, 12, 4, 10, 17, 6, 20, 21, 3, 5),$$
$$(16, 20, 17, 2, 19, 12, 0, 9, 8, 3, 1, 14, 10, 13, 5, 11, 18, 7, 21, 22, 4, 6),$$
$$(17, 21, 18, 3, 20, 13, 1, 10, 9, 4, 2, 15, 11, 14, 6, 12, 19, 8, 22, 0, 5, 7),$$
$$(18, 22, 19, 4, 21, 14, 2, 11, 10, 5, 3, 16, 12, 15, 7, 13, 20, 9, 0, 1, 6, 8),$$
$$(19, 0, 20, 5, 22, 15, 3, 12, 11, 6, 4, 17, 13, 16, 8, 14, 21, 10, 1, 2, 7, 9),$$
$$(20, 1, 21, 6, 0, 16, 4, 13, 12, 7, 5, 18, 14, 17, 9, 15, 22, 11, 2, 3, 8, 10),$$
$$(21, 2, 22, 7, 1, 17, 5, 14, 13, 8, 6, 19, 15, 18, 10, 16, 0, 12, 3, 4, 9, 11),$$
$$(0, 4, 1, 9, 3, 19, 7, 16, 15, 10, 8, 21, 17, 20, 12, 18, 2, 14, 5, 6, 11, 13).$$

Note that taking C'', the FH scheme using Construction 3.7.3, together with the cyclic shifts of the FH sequences in the set, we do not get the Reed-Solomon code back.

3.7.3 Correlation

Hamming correlation: The notion of Hamming correlation is related to the Hamming distance when we consider codes (or their subcodes) as FH schemes, as is shown in Proposition 3.7.5.

Proposition 3.7.5. *Given C a (v, κ)-MDS code and C'' as previously defined. The maximum Hamming correlation of C'' is at most $\kappa - 1$.*

Proof. The code C has the following codewords. Constant codewords, $X = (c, \ldots, c)$, where $c \in \mathcal{F}$. Constant codewords have the property $\beta^i X = X$, $\forall 1 \leq i \leq v - 1$. Next, there are codewords with non-full period, $C_{n_1} = \overset{\Leftrightarrow}{X}$, where $1 < |C_{n_1}| < v$. Finally, there are codewords with full period, $C_{n_2} = \overset{\Leftrightarrow}{X}$, where $|C_{n_2}| = v$. Any two codewords in C_{n_2} are not the same.

We know that the minimum distance of a $[v, \kappa, m]$-MDS code is $d(C) = v - \kappa + 1$. That is $d(X, Y) \geq d(C) = v - \kappa + 1$, $\forall\ X, Y \in C$. Therefore the Hamming correlation is $h(X, Y) \leq v - (v - \kappa + 1) = \kappa - 1\ \forall\ X, Y \in C$. By definition, the FH sequences in C'' (Construction 3.7.3) are obtained as representative codewords from each each subcode C_{n_2}. Consider $X \in C''$. Then there exist $X' \in C_{n_2}$, for some $C_{n_2} \subset C$, such that $X' = \beta^i X\ \forall 1 \leq i \leq v - 1$, because codewords in C'' have full period. Therefore we can find the maximum out-of-phase Hamming auto-correlation of each FH sequence $X \in C''$, $H(X) \leq \kappa - 1$. Further, for any two distinct codewords $X, Y \in C''$, $d(X, Y) \geq d(C) = v - \kappa + 1$ and the maximum Hamming cross-correlation is $H(X, Y) \leq \kappa - 1$. Then the maximum Hamming correlation $H_m(\mathcal{S}) = \max_{X,Y \in C''}\{H(X), H(Y), H(X, Y)\} \leq \kappa - 1$. □

Hamming group correlation The maximum Hamming correlation given in Proposition 3.7.5, $H_m(\mathcal{S}) \leq \kappa - 1$, allows us to estimate the throughput measures of an FH scheme based on Reed-Solomon codes considered in this section.

Let C be a Reed-Solomon code and C'' its subcode as previously defined. The Hamming group correlation of a Reed-Solomon code based FH scheme C'' is:

$$G(X, \mathcal{U}) \leq w(\kappa - 1),$$

where $\mathcal{U} \subseteq C''$, $|\mathcal{U}| = w$ and $X \in C'' \setminus \mathcal{U}$. Then the w-throughput of an FH sequence X is:

$$\begin{aligned} \rho_w(X, \mathcal{U}) &= 1 - \frac{G(X, \mathcal{U})}{v} \\ &\geq 1 - \frac{w(\kappa - 1)}{v}, \end{aligned}$$

and the worst-case w-throughput of the scheme is:

$$\begin{aligned}\hat{\rho}_w(\mathcal{S}) &= \min_{\mathcal{V}\subseteq\mathcal{S}}\left\{\min_{X_i\in\mathcal{V}}\{\rho_w(X_i,\mathcal{V}\setminus\{X_i\})\}\right\}\\ &= 1-\frac{w(\kappa-1)}{v}.\end{aligned}$$

3.7.4 Jamming resistance

Recall that the FH sequences in C'' are randomly chosen from the code C. An explicit way of obtaining the subcode C'' is difficult to present. So, the resistance of the FH scheme against a $(\frac{1}{m},\frac{1}{m})$-adaptive jammer will depend on the FH sequences obtained from the code. However, we consider Proposition 3.7.6.

Proposition 3.7.6. *If $w+1\neq|C''|$ then a $(\frac{1}{m},\frac{1}{m})$-adaptive jammer will need at least a single time slot to determine an active FH sequence.*

Proof. The proof is based on the fact that if only a fraction of the codewords are active, then a $(\frac{1}{m},\frac{1}{m})$-adaptive jammer is forced to eavesdrop on at least one time slot. □

Consider a $(22,2)$-Reed-Solomon code. In the remainder of this section we use this code as an illustration to determine its resistance against a $(\frac{1}{m},\frac{1}{m})$-adaptive jammer.

Example 3.7.7. *Consider C a $(22,2)$-Reed-Solomon code from Example 3.7.4. Let C'' be a $(22,22,22)$-FHS obtained using Construction 3.7.3. A $(\frac{1}{m},\frac{1}{m})$-adaptive jammer takes at least two time slots to establish an active codeword.*

We know that any two codewords X,Y in C'', $X\neq Y$ are distinct, that is $X\neq\beta^iY$ for all $0\leq i\leq 21$. However, for any channel x_t on codeword X, there exist some $Y\in C''$ such that $x_t=y_{t'}$, $0\leq t,t'\leq 21$. In fact there exist some $\beta^iY\in C$, where $t=i+t'\ (mod\ v)$. As the codewords in C'' are randomly selected from the Reed-Solomon code we have the following. Suppose $x_t\neq y_t$ for all codewords in C''. In this case a $(\frac{1}{m},\frac{1}{m})$-adaptive jammer only needs to eavesdrop on at least a single time slot to identify an active codeword. On the other hand suppose $x_t=y_t$ for all codewords in

C''. That is all the codewords have the same frequency channel at time slot t. However, for any two consecutive time slots $(x_t, x_{t+1}) \neq (y_{t'}, y_{t'+1})$, $0 \leq t, t' \leq v-1$. Therefore in the worst-case scenario, it can take a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer at least two time slots to establish an active codeword.

3.8 Bag-Ruj-Roy scheme

In this section we discuss the Bag-Ruj-Roy (BRR) scheme constructed by Bag et al. [9]. The FH sequences in the BRR scheme are derived using a pair of orthogonal Latin squares. We provide an interpretation of the BRR scheme in our model. The FH sequences are pseudorandom and form another FH scheme that provides maximum throughput of one for any FH sequence in the presence of other mutual interfering FH sequences. However, they can withstand an adversary for only one time slot.

3.8.1 Preliminaries

The FH schemes considered in this section use a combinatorial structure called a Latin square, which is described using a $v \times v$ array.

Definition 3.8.1. *Let Z be a set of size v. A **Latin square** of order v defined over Z is a $v \times v$ array L such that no element of Z appears more than once in any row or in any column of L.*

Example 3.8.2. *Consider the group $\mathbb{Z}_7$, integers modulo 7. The following is a Latin square of order 7 over $\mathbb{Z}_7$:*

0	1	2	3	4	5	6
6	0	1	2	3	4	5
5	6	0	1	2	3	4
4	5	6	0	1	2	3
3	4	5	6	0	1	2
2	3	4	5	6	0	1
1	2	3	4	5	6	0

.

Note that a Latin square defined over $\mathbb{Z}_v$ is equivalent to a (v, v, v)-MDS code up to renaming the alphabet symbols if necessary and a combination of permutation of alphabet symbols in a particular coordinate position and/or permuting the coordinate positions of the codewords.

Lemma 3.8.3 shows that adding an element from the set defining a Latin square to all the entries of the Latin square returns a Latin square. In other words it is a permutation of the original Latin square.

Lemma 3.8.3. *Let $L = [\alpha_{ij}]_{v\times v}$ be a Latin square of order v over $\mathbb{Z}_v$. Suppose $x \in \mathbb{Z}_v$. Let $L + x = [\beta_{ij}]_{v\times v}$, where $\beta_{ij} = \alpha_{ij} + x \pmod v$. Then $L + x$ is also a Latin square.*

Next we define orthogonality of a pair of Latin squares.

Definition 3.8.4. *Let $L_1 = [\alpha_{ij}]_{v\times v}$ is a Latin square of order v with entries from a set Z_1 of cardinality v and $L_2 = [\beta_{ij}]_{v\times v}$ be a Latin square of order v with entries from a set Z_2 of cardinality v. We say that L_1 and L_2 are **orthogonal Latin squares** if the v^2 ordered pairs $(\alpha_{ij}, \beta_{ij})$ are distinct.*

Example 3.8.5. *A pair of orthogonal Latin squares, L_1, L_2 of order 7:*

$$L_1 = \begin{array}{|c|c|c|c|c|c|c|}\hline 0&1&2&3&4&5&6\\\hline 1&2&3&4&5&6&0\\\hline 2&3&4&5&6&0&1\\\hline 3&4&5&6&0&1&2\\\hline 4&5&6&0&1&2&3\\\hline 5&6&0&1&2&3&4\\\hline 6&0&1&2&3&4&5\\\hline\end{array}, \qquad L_2 = \begin{array}{|c|c|c|c|c|c|c|}\hline 0&6&5&4&3&2&1\\\hline 1&0&6&5&4&3&2\\\hline 2&1&0&6&5&4&3\\\hline 3&2&1&0&6&5&4\\\hline 4&3&2&1&0&6&5\\\hline 5&4&3&2&1&0&6\\\hline 6&5&4&3&2&1&0\\\hline\end{array}.$$

Lemma 3.8.6 extends Lemma 3.8.3 in that adding an element from the set on which the orthogonal Latin squares are defined to all the entries in the Latin squares preserves their orthogonality.

Lemma 3.8.6. *Let $L_1 = [\alpha_{ij}]_{v\times v}$ and $L_2 = [\beta_{ij}]_{v\times v}$ be a pair of orthogonal Latin squares of order v over $\mathbb{Z}_v$. Suppose $x, y \in \mathbb{Z}_v$. Then $L_1 + x$ and $L_2 + y$ are orthogonal Latin squares.*

The existence of orthogonal Latin squares is assured in Theorem 3.8.7.

Theorem 3.8.7. *For every odd integer $v > 1$, there exists a pair of orthogonal Latin squares of order v.*

A set of s Latin squares of order v, any pair of which are orthogonal, is called a set of *mutually orthogonal* Latin squares denoted MOLS(v, s) (in other literature they are sometimes referred to as *pairwise orthogonal* Latin squares, abbreviated POL(v, s)).

Theorem 3.8.8. *Let $N(v)$ denote the maximum number of MOLS(v, s), $v \geq 2$.*

1. *$N(6) = 1$. If $v \neq 2, 6$, then $N(v) \geq 2$.*
2. *$N(v) \leq v - 1$, with equality if and only if there exists a projective plane of order v.*
3. *$N(v) = v - 1$, if v is a prime power number.*

For construction of orthogonal Latin squares we refer the reader to [43, 97].

3.8.2 Construction

The Bag-Ruj-Roy (BRR) [9] scheme is as follows.

Consider an FH scheme with m users $\{N_0, \ldots, N_{m-1}\}$ and a frequency library of size m. We can identify the frequency channels with $\mathcal{F} = \mathbb{Z}_m$. Let F_1 and F_2 be pseudo-random functions where the input-output of an instance is computationally indistinguishable from that of a random function. The two-input functions F_1 and F_2 takes K, s, a long term key and a session number respectively. As defined in Section 2.3, a *session* is a number of pre-defined time slots and made up of v time slots, each the length of a single sequence. The values K and s are shared by all users. All users generate shared session keys $x, y \in \mathbb{Z}_m$ which are the outputs of the pseudo-random function denoted $x = F_1(K, s)$ and $y = F_2(K, s)$.

The BRR FH scheme is modelled for unicast communication at each time slot. In more detail, at each time slot a single user (otherwise termed as a device) sends information on frequency channels to a particular receiver in the system. In a single session each user transmits to every other user in the system. A single user is equipped with both a sending and a receiving sequence. On each time slot a sending sequence defines the channel and the recipient of data to be sent. On the other hand a receiving sequence defines a channel and the sender of information at each time slot.

Construction 3.8.9. *(BRR FH scheme) Let* $L_1 = [\alpha_{ij}]_{m\times m}$ *and* $L_2 = [\beta_{ij}]_{m\times m}$ *be a pair of orthogonal Latin squares of order* m*. Let* $L_3 = [(L_1(i,j), L_2(i,j))]_{m\times m}$ *be a Latin square that is the superposition of* L_1 *and* L_2*. From* L_3 *user* N_i *is given* i^{th} *row* $R_i = \{(\alpha_{i0}, \beta_{i0}), (\alpha_{i1}, \beta_{i1}), \ldots, (\alpha_{im-1}, \beta_{im-1})\}$ *and* i^{th} *column* $C_i = \{(\alpha_{0j}, \beta_{0j}), (\alpha_{1j}, \beta_{1j}), \ldots, (\alpha_{m-1j}, \beta_{m-1j})\}$ *for* $1 \leq i \leq m$*. A row and column* (R_i, C_i) *are used to derive the sending and receiving FH sequences respectively. Let* x, y *be session keys and* $L_4 = [(L_1(i,j) + x, L_2(i,j) + y)]_{m\times m}$ *be an array which is* $L_1 + x$ *superimposed (see Example 3.8.10) with* $L_2 + y$*. At each session, the sending FH sequences of length* m

over $\mathcal{F} = \mathbb{Z}_m$ *are derived from:*

$$R_i^* = \{(\alpha_{ij} + x, \beta_{ij} + y, j) : 0 \leq j \leq m-1\},$$

where $(\alpha_{ij} + x, \beta_{ij} + y, j)$ *corresponds to the (frequency channel, time slot, identity of receiver). For a sending FH sequence the entry* $(\alpha_{ij} + x, \beta_{ij} + y, j)$ *means that user* N_i *transmits to user* N_j *on frequency channel* $\alpha_{ij} + x$ *at time slot* $\beta_{ij} + y$*. The receiving FH sequence is obtained likewise using:*

$$C_i^* = \{(\alpha_{ij} + x, \beta_{ij} + y, j) : 0 \leq j \leq m-1\}.$$

User N_i *receives data from user* N_j *on frequency channel* $\alpha_{ij} + x$ *at time slot* $\beta_{ij} + y$*.*

The sender and receiver both have the same $(\alpha_{ij} + x, \beta_{ij})$*. Therefore the receiver-sender pair will be on the same channel at the same time.*

We use Example 3.8.10 to illustrate Construction 3.8.9 in the model of Section 2.3 used in this thesis.

Example 3.8.10. *Consider* L_1, L_2*, the pair of orthogonal Latin squares in Example 3.8.5. The Latin square* L_3 *is the superposition of* L_1 *and* L_2*:*

$L_3 =$

(0, 0)	(1, 6)	(2, 5)	(3, 4)	(4, 3)	(5, 2)	(6, 1)
(1, 1)	(2, 0)	(3, 6)	(4, 5)	(5, 4)	(6, 3)	(0, 2)
(2, 2)	(3, 1)	(4, 0)	(5, 6)	(6, 5)	(0, 4)	(1, 3)
(3, 3)	(4, 2)	(5, 1)	(6, 0)	(0, 6)	(1, 5)	(2, 4)
(4, 4)	(5, 3)	(6, 2)	(0, 1)	(1, 0)	(2, 6)	(3, 5)
(5, 5)	(6, 4)	(0, 3)	(1, 2)	(2, 1)	(3, 0)	(4, 6)
(6, 6)	(0, 5)	(1, 4)	(2, 3)	(3, 2)	(4, 1)	(5, 0)

Let $x = 4$ *and* $y = 6$ *be the session keys. Then the Latin square* L_4 *is the superposition of the pair of orthogonal Latin squares* $L_1 + x$ *and* $L_2 + y$*:*

$L_4 =$

(4, 6)	(5, 5)	(6, 4)	(0, 3)	(1, 2)	(2, 1)	(3, 0)
(5, 0)	(6, 6)	(0, 5)	(1, 4)	(2, 3)	(3, 2)	(4, 1)
(6, 1)	(0, 0)	(1, 6)	(2, 5)	(3, 4)	(4, 3)	(5, 2)
(0, 2)	(1, 1)	(2, 0)	(3, 6)	(4, 5)	(5, 4)	(6, 3)
(1, 3)	(2, 2)	(3, 1)	(4, 0)	(5, 6)	(6, 5)	(0, 4)
(2, 4)	(3, 3)	(4, 2)	(5, 1)	(6, 0)	(0, 6)	(1, 5)
(3, 5)	(4, 4)	(5, 3)	(6, 2)	(0, 1)	(1, 0)	(2, 6)

.

Table 3.3 provides the sending and receiving FH sequences for N_0 and N_6:

	N_0	N_6
R_i^*	$\{(4,6,0),(5,5,1),(6,4,2),(0,3,3),(1,2,4),(2,1,5),\underline{(3,0,6)}\}$	$\{\underline{(3,5,0)},(4,4,1),(5,3,2),(6,2,3),(0,1,4),(1,0,5),(2,6,6)\}$
C_i^*	$\{\underline{(4,6,0)},(5,0,1),(6,1,2),(0,2,3),(1,3,4),(2,4,5),\underline{(3,5,6)}\}$	$\{\underline{(3,0,0)},(4,1,1),(5,2,2),(6,3,3),(0,4,4),(1,5,5),(2,6,6)\}$
FH sequence for sending	$(3,2,1,0,6,5,4)$	$(1,0,6,5,4,3,2)$
FH sequence for receiving	$(5,6,0,1,2,3,4)$	$(3,4,5,6,0,1,2)$

.

Table 3.3: Sending and receiving FH sequences for users N_0 and N_6 in a Latin square based FH scheme.

From Table 3.3, $(3,0,6) \in R_i^*$ for N_0 means N_0 will send data on channel 3 at time 0 to N_6, and $(3,0,0) \in C_i^*$ for N_6 means N_6 will switch to channel 3 at time 0 to receive data from N_0. Likewise for $(3,5,0) \in R_i^*$ for N_6, N_6 will be transmitting on channel 3 at time slot 5 to N_0, and $(3,5,6) \in C_i^*$ for N_0, N_0 will be listening on channel 3 at time slot 5 for messages from N_6.

Note that the FH sequences for sending and receiving are arranged in the format used in this thesis $(x_0, x_1, \ldots, x_{v-1})$, where the indices are time slots in R_i^* and C_i^* accordingly.

In the system model of this thesis (Section 2.3) we consider only sending FH sequences. Therefore the FH scheme in Construction 3.8.9 is considered as an (m, m, m)-FHS.

3.8.3 Correlation

In this section we consider the correlation and throughput of the (m, m, m)-FHS obtained from Construction 3.8.9.

Theorem 3.8.11. *Consider $\mathcal{S}$ to be the (m, m, m)-FHS obtained from Construction 3.8.9. The w-throughput of any FH sequence in $\mathcal{S}$ is 1 for any w, $0 \leq w < m$.*

Proof. Let $\mathcal{S}$ be an (m, m, m)-FHS with FH sequences from Construction 3.8.9. Consider L_1 and L_2, a pair of orthogonal Latin squares of order m defined over $\mathbb{Z}_m$. From Lemma 3.8.6 we have: $L_1 + x$ and $L_2 + y$ are orthogonal Latin squares for any $x, y \in \mathbb{Z}_m$. Consider the superposition of a pair of orthogonal Latin squares $L_1 + x = [\alpha'_{ij}]_{m\times m}$, $L_2 + y = [\beta'_{ij}]_{m\times m}$, where $\alpha'_{ij} = \alpha_{ij} + x$ and $\beta'_{ij} = \beta_{ij} + y$. There exist a unique cell (i, j) with the ordered pair $(\alpha_{ij} + x, \beta_{ij} + y)$. Therefore, for all FH sequences $X_i \in \mathcal{S}$ derived using X_i^*, $0 \leq i \leq m-1$, all the frequency channels at each time slot are distinct. That is, at any time slot t, the multiset $\mathcal{F}_t$ has distinct channels and $a_i = 1$ for all $i \in \mathcal{F}$. This implies that there is no mutual interference at each time slot for any FH sequence $X_i \in \mathcal{S}$ in the presence of other FH sequences $X_{i'} \in \mathcal{S}$, $i \neq i'$. Hence the w-throughput of any FH sequence X_i in the presence of other FH sequences $X_{i'} \in \mathcal{U} \subset \mathcal{S}$ is

$$\rho_w(X_i, \mathcal{U}) = 1.$$

□

From Theorem 3.8.11, we can deduce that the worst-case w-throughput of $\mathcal{S}$ is:

$$\hat{\rho}_w(\mathcal{S}) = 1.$$

Therefore $\mathcal{S}$ is an $(m, m, m; 1)$-FHS.

Despite the fact that FH sequences in $\mathcal{S}$, the $(m, m, m; 1)$-FHS, achieve maximum w-throughput of one, this does not resist a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer. In Section 3.8.4

it will be shown that a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer eavesdropping at one time slot will be able to identify all the FH sequences of the FH scheme.

3.8.4 Jamming resistance

Using the jammer model introduced in Chapter 2, a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer knows $\mathcal{N}$, $\mathcal{F}$ and the Latin square L_3 is public. Further we can assume that a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer knows time zero of the FH scheme, $t = 0$.

As observed in all the previous FH schemes that have been considered thus far in this thesis, when all the FH sequences are active a jammer can jam any FH sequence from the start and thus reduce the worst-case w-throughput of the FH scheme to zero. We have Theorem 3.8.12 for the case when the number of active FH sequences is less than the size of the FH scheme.

Theorem 3.8.12. *Consider $\mathcal{S}$ to be the (m, m, m)-FHS obtained from Construction 3.8.9. If $w+1 \leq m-1$ then a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer needs at least one time slot to identify an active FH sequence.*

Proof. Let $\mathcal{S}$ be the (m, m, m)-FHS obtained from Construction 3.8.9. From the discussion in the proof of Theorem 3.8.11, we have that at any time slot t, the multiset $\mathcal{F}_t$ has distinct channels and so $a_i = 1$ for all $i \in \mathcal{F}$.

Suppose that at time slot $t = 0$ the $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer eavesdrops on an active channel. Since the channels are distinct, then the jammer has found an active FH sequences. Hence it starts jamming this particular active FH sequence from time slot $t = 1$ and onwards.

On the other hand, suppose at time slot $t = 0$ the $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer eavesdrops on an inactive channel. If $w + 1 = m - 1$, the jammer will have all the active FH sequences in its search space after removing the single inactive FH sequence from its search space. However, if $w + 1 < m - 1$, then the jammer is forced to continue eavesdropping on the succeeding time slot $t = 1$.

We conclude that if $w+1 \leq m-1$ then a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer needs at least 1 time slot to identify an active FH sequence. □

We now show how a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer can trivially construct any FH sequence of the FH scheme.

Suppose a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer eavesdrops on frequency α' at time slot β', where user N_i was transmitting to user N_j. The jammer discovers one hop element, $(\alpha', \beta', j) = (\alpha_{ij} + x, \beta_{ij} + y, j)$. Then the jammer can retrieve the session keys x and y as follows:

$$\begin{aligned} \alpha'_{ij} &= \alpha_{ij} + x \\ \beta'_{ij} &= \beta_{ij} + y \\ x &= (\alpha'_{ij} - \alpha_{ij}) \pmod{n} \\ y &= (\beta'_{ij} - \beta_{ij}) \pmod{n}. \end{aligned}$$

The values α_{ij} and β_{ij} are obtained from L_3.

Knowledge of x, y enables the jammer to derive subsequent hops, or in fact the whole FH sequence of any user and then jam accordingly. A jammer can pick α_{ij+1} and β_{ij+1} from the public Latin square L_3, to compute α'_{ij+1} and β'_{ij+1} as follows:

$$\begin{aligned} \alpha'_{ij+1} &= \alpha_{ij+1} + (\alpha'_{ij} - \alpha_{ij}) \\ \beta'_{ij+1} &= \beta_{ij+1} + (\beta'_{ij} - \beta_{ij}). \end{aligned}$$

Suppose a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer obtains the session keys x, y on the first time slot. Then the BRR FH scheme has thus $\gamma v = 1$ resistance against a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer.

In Chapter 5 we provide a fix to the problem observed with the BRR FH scheme: that the BRR FH scheme can not withstand a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer for more than

a single time slot.

3.8.5 IEEE 802.11: Latin square based FH scheme, a practical example

Recall that in Section 1.1.5 we described frequency hopping spread spectrum as defined in the IEEE 802.11 wireless LAN [5]. The standard provides four ways in which FH sequences can be obtained: HCC, EHCC, random generation and using FH sequences in a fixed table.

The HCC method defines an FH sequence $X_i = (x_t)$ of length v over a frequency library of size v as

$$x_t = \frac{i}{t} \pmod{(v+1)},$$

where $v+1$ is a prime number, $1 \leq i, t \leq v$. So, the HCC method provides a (v, v, v)-FHS.

The EHCC FH sequences are obtained by deleting the diagonal entries of the FH sequences given by the HCC method. So, the EHCC method provide a $(v-1, v, v-1)$-FHS.

It can be observed that the FH sequences obtained using the HCC, EHCC and the fixed table methods form an FH scheme that is equivalent to a Latin square. So each of the FH schemes achieve a maximum throughput of one as for the BRR FH scheme.

Note that the generation of the FH sequences do not use pseudorandom numbers, but rather fixed parameters. Suppose the number of active FH sequences is less than the size of the FH scheme. Then the resistance of the FH schemes is based on the fact that a (θ_1, θ_2)-adaptive jammer has no knowledge of the active FH sequences. However, as was the case with the BRR FH scheme, it should take a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer at least a single time slot to identify an active FH sequence in the HCC, EHCC and the fixed table.

3.9 Recursive combinatorial construction

Several authors have constructed FH schemes from existing ones. Fuji-Hara et al. [35] obtain an FH sequence using difference matrices and difference packing. The new FH sequence is of composite length, v_1v_2, where v_1 and v_2 are the lengths of old FH sequences. Ding et al. [27] extend the construction of Fuji-Hara et al. [35]. The authors use two FH schemes to obtain a new FH scheme of composite length with the size of the new FH scheme as the minimum of the sizes of the two old FH schemes. Chung et al. [21] use interleaving techniques to obtain a new FH scheme from another FH scheme. In this construction the new FH scheme is defined on the same frequency library as the old one and the size is the minimum of the sizes of the old FH schemes. Zeng et al. [115] (interleaving technique) get new FH schemes with a preserved number of FH sequences but increased frequency library size. Chung, Gong and Yang [20] use the Chinese remainder theorem to present an FH scheme with preserved maximum Hamming correlation but increased length and size of the frequency library.

The recursive constructions mentioned thus far, each provide new parameters that could not be otherwise obtained using the old FH schemes. In this section we consider Ding et al. [27] recursive construction, which is a generalisation of the Fuji-Hara et al. [35] construction. The construction uses a combinatorial matrix called the cyclic difference matrix.

3.9.1 Difference matrices

Definition 3.9.1. *Let G be an abelian group of order p. A **difference matrix**, denoted $(p, n; \lambda)$-DM, is an $n \times \lambda p$ matrix $A = [\alpha_{ij}]$ such that $\alpha_{ij} \in G$ and for each pair of two distinct rows i and i', $1 \leq i, i' \leq n$, every element of G occurs exactly λ times among the differences $\{(\alpha_{ij} - \alpha_{i'j}) \pmod p : 1 \leq j \leq \lambda p\}$. If $G = \mathbb{Z}_p$ then the difference matrix is called a cyclic difference matrix, denoted $(p, n; \lambda)$-CDM.*

Theorem 3.9.2 (Existence theorem, Theorem 2.2, [49])**.** *Let D be a (p, n, λ)-difference*

matrix. Then $n \leq \lambda p$.

Removing a row from a (p, n, λ)-difference matrix provides a $(p, n-1, \lambda)$-difference matrix. A difference matrix with all zero first row is said to be *normalized*. A *homogeneous* difference matrix is obtained from a normalized difference matrix by deleting the all zero row. A homogeneous difference matrix has the property that every element of $\mathbb{Z}_p$ appears in every row exactly λ times.

Lemma 3.9.1 is a construction of a homogeneous $(p, n; 1)$-DM.

Lemma 3.9.3 (Lemma 1.2, [8]). *Let* p *and* n *be positive integers such that* $\gcd(p, (n-1)!) = 1$, *and let* $\alpha_{ij} = ij \pmod p$ *for* $0 \leq i \leq n-1$ *and* $0 \leq j \leq p-1$. *Then* $D = [\alpha_{ij}]$ *is a normalized* $(p, n; 1)$*-difference matrix. In particular, if* p *is an odd prime number, then there exists a* $(p, n; 1)$*-difference matrix for any integer* $n \leq p-1$.

We consider the recursive construction of Ding et al. [27]. The authors use cyclic difference matrices with $\lambda = 1$.

Let $\mathcal{S}$ be a (v, k, m)-FHS with the property that for each $X \in \mathcal{S}$, there exists f such that $x_t = f$ for precisely one single time slot t.

Let $\mu_X(f)$ denote the multiplicity of frequency channel f on FH sequence X. Let $\mu_{\mathcal{S}}(f) = \sum_{X \in \mathcal{S}} \mu_X(f)$, the number of occurrences of frequency channel f in the FH scheme $\mathcal{S}$. Finally, the maximum occurrence of frequency channels in $\mathcal{S}$ the (v, k, m)-FHS is denoted $\bar{\mu}_{\mathcal{S}} = \max_{f \in \mathcal{F}} \mu_{\mathcal{S}}(f)$.

The authors also use $\mathcal{S}$, a (v, k, m)-FHS with the following property. The frequency channel 0 appears only at the first time slot on all the FH sequences in $\mathcal{S}$. Further, for any pair of FH sequences $X, Y \in \mathcal{S}$, $h(x_i, y_i) = 0$ for $i = 1, \ldots, v-1$, where $h(x_t, y_t)$ is as previously defined for Hamming correlation in Definition 2.2.3. Therefore $H_{X,Y}(0) = 1$.

Let $\lambda_a = H(X)$ and $\lambda_c = H(X, Y)$ denote the maximum out-of-phase Hamming auto-correlation and maximum Hamming cross-correlation defined in Equations (2.2) and (2.3) respectively. Construction 3.9.4 follows closely [27, Theorem 13]. We have additional conditions for the use of a particular FH scheme and we have also clear notation on

the construction of support blocks for ease of understanding.

Construction 3.9.4. *Let $v \equiv 1 \pmod{k(k-1)}$. Let $\mathcal{V}$ be a (v,k,m)-FHS defined over $\mathbb{F}_m$, with correlation values λ_a and λ_c. Further, for any $X,Y \in \mathcal{V}$, $x_0 = y_0 = 0$, $h(x_0,y_0) = 1$ and $h(x_i,y_i) = 0$ for $i = 1,\ldots,v-1$. Let $\mathcal{U}$ be a (v',k',m')-FHS defined over $\mathbb{F}_{m'}$, and given its correlation values λ'_a and λ'_c. Further, for any $X,Y \in \mathcal{U}$, $h(x_i,y_i) = 0$ for $i = 0,\ldots,v-1$. If there exists a homogeneous cyclic difference matrix $(v',\bar{\mu}_{\mathcal{V}};1)$-CDM, then there exists $\mathcal{S}$ a $(vv',\min\{k,k'\},(m-1)v'+m')$-FHS with maximum out-of-phase Hamming auto-correlation and maximum cross-correlation $\max\{\lambda_a,\lambda'_a\}$ and $\max\{\lambda_c,\lambda'_c\}$ respectively.*

Let $D = [\alpha_{ij}]_{\bar{\mu}_{\mathcal{V}} \times v'}$ be a $(v',\bar{\mu}_{\mathcal{V}};1)$-CDM. For each block $B_i^j = \{b_{i1}^j,\ldots,b_{ik_j}^j\}$, a support (see Equation (3.27)) for frequency channel $i \in \mathbb{F}_m \setminus \{0\}$, on FH sequence $X_j \in \mathcal{V}$ construct v' blocks,

$$B_i^j(l) = \{b_{i1}^j + \alpha_{1l}v,\ldots,b_{ik_j}^j + \alpha_{k_jl}v\}, \qquad 0 \le l \le v'-1.$$

For each block $C_{i'}^j = \{c_{i'1}^j,\ldots,c_{i'k_j}^j\}$, a support block for frequency channel $i' \in \mathbb{F}_{m'}$ on FH sequence $Y_j \in \mathcal{U}$ construct a block,

$$C_{i'}^j v = \{c_{i'1}^j v,\ldots,c_{i'k_j}^j v\}.$$

Construct an FH sequence of length vv' defined over a frequency library $\mathcal{F}$, $|\mathcal{F}| = (m-1)v'+m'$ using the following set of support blocks $\mathcal{P} = \{B_i^j(l), C_{i'}^j v : 0 \le j \le \min\{k-1,k'-1\}, 1 \le i \le m-1, 0 \le i' \le m'-1\}$.

Example 3.9.5 illustrates Construction 3.9.4.

Example 3.9.5. *Consider $\mathcal{V}$ a $(7,3,6)$-FHS,*

$$\mathcal{V} = \{(0,1,4,5,5,2,3),(0,4,1,2,2,5,1),(0,2,2,1,3,4,2)\},$$

$\mathcal{U}$ a $(5,2,4)$-FHS,

$$\mathcal{U} = \{(1,3,2,3,1),(0,2,1,1,3)\},$$

and D a homogeneous $(5,3;1)$-CDM,

$$D = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 0 & 3 & 1 & 4 & 2 \end{pmatrix}.$$

Then:

$$7D = \begin{pmatrix} 0 & 7 & 14 & 21 & 28 \\ 0 & 14 & 28 & 7 & 21 \\ 0 & 21 & 7 & 28 & 14 \end{pmatrix}.$$

Consider $Y_1 = (0,1,4,5,5,2,3)$. Then $B_1^1 = \{1\}, B_2^1 = \{5\}, B_3^1 = \{6\}, B_4^1 = \{2\}, B_5^1 = \{3,4\}$. The 25 blocks from the B_i^1, $1 \le i \le m-1$ are as follows:

$$\begin{array}{lllll}
B_1^1(0) = \{1\}, & B_1^1(1) = \{8\}, & B_1^1(2) = \{15\}, & B_1^1(3) = \{22\}, & B_1^1(4) = \{29\}, \\
B_2^1(0) = \{5\}, & B_2^1(1) = \{12\}, & B_2^1(2) = \{19\}, & B_2^1(3) = \{26\}, & B_2^1(4) = \{33\}, \\
B_3^1(0) = \{6\}, & B_3^1(1) = \{13\}, & B_3^1(2) = \{20\}, & B_3^1(3) = \{27\}, & B_3^1(4) = \{34\}, \\
B_4^1(0) = \{2\}, & B_4^1(1) = \{9\}, & B_4^1(2) = \{16\}, & B_4^1(3) = \{23\}, & B_4^1(4) = \{30\}, \\
B_5^1(0) = \{3,4\}, & B_5^1(1) = \{10,18\}, & B_5^1(2) = \{17,32\}, & B_5^1(3) = \{24,11\}, & B_5^1(4) = \{31,25\}.
\end{array}$$

Consider $U_1 = (1,3,2,3,1)$. We have

$$C_0^1 = \emptyset, C_1^1 = \{0,4\}, C_2^1 = \{2\}, C_3^1 = \{1,3\},$$

and

$$C_0^1\beta = \emptyset, C_1^1\beta = \{0,28\}, C_2^1\beta = \{14\}, C_3^1\beta = \{7,21\}.$$

Table 3.4 shows the support $B_i^j(l)$ and $C_{i'}^j$ $0 \le j \le 1, 1 \le i \le 5, 0 \le i' \le 3$ with the corresponding frequency channel number.

$B_i^j(l)$	$B_1^1(0)$	$B_1^1(1)$	$B_1^1(2)$	$B_1^1(3)$	$B_1^1(4)$
No.	0	1	2	3	4
$B_i^j(l)$	$B_2^1(0)$	$B_2^1(1)$	$B_2^1(2)$	$B_2^1(3)$	$B_2^1(4)$
No.	5	6	7	8	9
$B_i^j(l)$	$B_3^1(0)$	$B_3^1(1)$	$B_3^1(2)$	$B_3^1(3)$	$B_3^1(4)$
No.	10	11	12	13	14
$B_i^j(l)$	$B_4^1(0)$	$B_4^1(1)$	$B_4^1(2)$	$B_4^1(3)$	$B_4^1(4)$
No.	15	16	17	18	19
$B_i^j(l)$	$B_5^1(0)$	$B_5^1(1)$	$B_5^1(2)$	$B_5^1(3)$	$B_5^1(4)$
No.	20	21	22	23	24
$C_{i'}^1\beta$	$C_0^1\beta$	$C_1^1\beta$	$C_2^1\beta$	$C_3^1\beta$	
No.	25	26	27	28	

Table 3.4: Frequency channel assignment for a recursive FH scheme construction.

A new FH sequence of length 35 *over a frequency library of size* 29 *is:*

$$\begin{aligned} X \quad = \quad & (26, 0, 15, 20, 20, 5, 10, 28, 1, 16, 21, 23, 6, 11, 27, 2, 17, 22, 21, 7, 12, 28, \\ & 3, 18, 23, 24, 8, 13, 26, 4, 19, 24, 22, 9, 14) \end{aligned} \tag{3.53}$$

3.9.2 Correlation

In this section we consider the Hamming correlation and Hamming group correlation of the FH scheme of Construction 3.9.4.

Hamming correlation: Let $\mathcal{V}$ and $\mathcal{U}$ be FH schemes with parameters as given in Construction 3.9.4. Let $\mathcal{S}$ be a $(vv', \min\{k, k'\}, (m-1)v'+m')$-FHS be a recursively constructed FH scheme from Construction 3.9.4. Then $\mathcal{S}$ is an FH scheme with maximum out-of-phase Hamming auto-correlation and maximum cross-correlation $\max\{\lambda_a, \lambda_{a'}\}$

and $\max\{\lambda_c, \lambda_{c'}\}$ respectively. Then the maximum Hamming correlation of the set $\mathcal{S}$ is:

$$H_m(\mathcal{S}) = \max\{\max\{\lambda_a, \lambda_{a'}\}, \max\{\lambda_c, \lambda_{c'}\}\}. \tag{3.54}$$

Hamming group correlation: Let $\mathcal{S}$ be an FH scheme as previously defined. Then the Hamming group correlation is:

$$G(X,\mathcal{U}) \leq wH_m(\mathcal{S}),$$

where $\mathcal{U} \subseteq \mathcal{S}$, $|\mathcal{U}| = w$, $X \in \mathcal{S} \setminus \mathcal{U}$ and $H(\mathcal{S})$ is as given in Equation (3.54). Then the w-throughput of an FH sequence $X \in \mathcal{S}$, $\rho_w(X,\mathcal{U})$, and the worst-case w-throughput of the scheme, $\hat{\rho}_w(\mathcal{S})$ can be defined in a similar manner to the previous constructions considered in Sections 3.2.3, 3.3.3, 3.4.3, 3.5.3, 3.6.3, 3.7.3, where the Hamming group correlation has been estimated using the maximum Hamming correlation.

3.9.3 Jamming resistance

We note that the channel number assignment for a frequency library used in Construction 3.9.4 is arbitrary. That is, any $A_i^j(l)$ for $1 \leq j \leq k$, $0 \leq i \leq m-1$ can be a support set of any frequency channel in $\mathcal{F}_{(m-1)v'+m'}$. Without loss of generality, we assume that at time slot t there exists a frequency channel that appears at least once. That is, $a_i \geq 1$ for any frequency channel i appearing on FH sequence(s) at time slot t. So, to determine the jamming resistance of an FH scheme we take the probability that a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer is jamming on an active frequency channel i at a particular time slot t as:

$$\begin{aligned} Prob(i \text{ is active}) &= 1 - \binom{k-a_i}{w+1} / \binom{k}{w+1} \\ &\geq 1 - \binom{k-1}{w+1} / \binom{k}{w+1}. \end{aligned}$$

3.10 Comparison of FH schemes

Having discussed a large number of FH schemes in the preceding sections, we now present a comparison in terms of their performance in the presence of mutual interfering FH sequences. We also compare the FH schemes according to the resistance against a (θ_1, θ_2)-adaptive jammer. We compare FH schemes with approximately the same frequency library size. It is reasonable to fix the size of the frequency library because it is the parameter that is regulated and constrained in practice. Without loss of generality, we consider the size of the frequency library comparable to those used for IEEE 802.11 networks [5]. We consider the case $|\mathcal{F}| \approx 23, 79$. We have seen that the parameters v, k, m for a (v, k, m)-FHS have constraints and can be related in most cases. So, when we fix m, the choice of v and k will follow. However, it was mentioned in Section 2.3 that FH sequences can be used periodically. Therefore for a fixed m, we can define a (v, k, m)-FHS and then extend it to a (v', k, m)-FHS, where $v' = v \cdot n + r$, where n, r are integers and v' is the desired length. We mention this because due to computational limitations we use a random walk of length three, a $(3, 23 \cdot 8^2, 23)$-FHS, in our comparison. However, the $(3, 23 \cdot 8^2, 23)$-FHS can be used periodically until a desired length is obtained.

Tables 3.5 and 3.6 show the parameters of the FH schemes that we use for the comparison in Sections 3.10.1 and 3.10.2. Further, the tables also shows the sections in which each FH scheme was described in this chapter.

Mathematical tool	**Abbreviation**	**Parameters**
Random walks, Section 3.2	RW	$(3, 23 \cdot 8^2, 23)$-FHS
Difference packing, Section 3.3	DP	$(23^2, 23^2, 23)$-FHS
m-sequences, Sections 3.4	LG	$(23^3 - 1, 23^3 - 1, 23)$-FHS
Cyclotomy, Section 3.5	CC	$(47, 47, 23)$-FHS
Trace functions, Section 3.6	TF	$(48, 11, 23)$-FHS
Reed-Solomon code, Section 3.7	RS	$(23, 23, 23)$-FHS
Latin square, Section 3.8	LS	$(23, 23, 23)$-FHS
Recursive, Section 3.9	RC	$(65, 3, 23)$-FHS

Table 3.5: Parameters of $(v, k, 23)$-FHS.

Mathematical tool	**Abbreviation**	**Parameters**
Random walks, Section 3.2	RW2	$(3, 79 * 22^2, 79)$-FHS
Difference packing, Section 3.3	DP2	$(79^2, 79^2, 79)$-FHS
m-sequences, Section 3.4	LG2	$(79^2 - 1, 79^2 - 1, 79)$-FHS
Cyclotomic classes, Section 3.5	CC2	$(79, 79, 78)$-FHS
Trace functions, Section 3.6	TF2	$(79^2 - 1, 39, 79)$-FHS
Reed-Solomon code, Section 3.7	RS2	$(79, 79, 79)$-FHS
Latin square, Section 3.8	LS2	$(79, 79, 79)$-FHS
Recursive, Section 3.9	RC2	$(844, 15, 79)$

Table 3.6: Parameters of $(v, k, \approx 79)$-FHS.

3.10.1 Throughput comparison

In this section we compare the worst-case w-throughput of the (v, k, m)-FHS considered in this chapter in the presence of mutual interference only. We will make a comparison of the resistance of the (v, k, m)-FHS in the presence of a (θ_1, θ_2)-adaptive jammer in

Section 3.10.2.

Recall the worst-case w-throughput for $\mathcal{S}$ a (v, k, m)-FHS defined by Equation (2.38):

$$\hat{\rho}_w(\mathcal{S}) = \min_{\mathcal{V} \subseteq \mathcal{S}} \left\{ \min_{X_i \in \mathcal{V}} \{\rho_w(X_i, \mathcal{V} \setminus \{X_i\})\} \right\},$$

where $X_i \in \mathcal{V}$, $\mathcal{V} = \mathcal{U} \cup \{X_i\}$, $\mathcal{U} \subset \mathcal{S}$ and $\rho_w(X_i, \mathcal{V} \setminus \{X_i\}) = 1 - \frac{G(X_i, \mathcal{V} \setminus \{X_i\})}{v}$. The Hamming group correlation is $G(X_i, \mathcal{V} \setminus \{X_i\}) \leq w \cdot H_m(\mathcal{S})$, where $H_m(\mathcal{S})$ is the maximum Hamming correlation of a set, Equation (2.14). We approximate the worst-case w-throughput of a set $\mathcal{S}$ using:

$$\hat{\rho}_w(\mathcal{S}) \geq 1 - \frac{w \cdot H_m(\mathcal{S})}{v}. \tag{3.55}$$

With Equation (3.55), we suppose that the time slots on which each additional mutual interfering FH sequence contributes towards Hamming group correlation are distinct. Table 3.7 summarises the formulae of approximate worst-case w-throughput for FH schemes from Table 3.5 with respect to the number of mutual interfering FH sequences.

(v, k, m)-FHS, $\mathcal{S}$	Approximate $\hat{\rho}_w(\mathcal{S})$
RW, $(3, 23 \cdot 8^2, 23)$-FHS	$1 - w/3$
DP, $(23^2, 23^2, 23)$-FHS	$1 - w/23$
LG, $(23^3 - 1, 23^3 - 1, 23)$-FHS	$1 - (23^2 - 1)w/23^3 - 1$
CC, $(47, 47, 23)$-FHS	$1 - 2w/47$
TF, $(48, 11, 23)$-FHS	$1 - 2w/48$
RS, $(23, 23, 23)$-FHS	$1 - 2w/23$
LS, $(23, 23, 23)$-FHS	1
RC, $(65, 3, 23)$	$1 - 3w/65$

Table 3.7: Approximate worst-case throughput formula of $(v, k, 23)$-FHS.

The results presented in Table 3.8 use the formulae in Table 3.7, where we have considered the presence of at most 6 mutual interfering FH sequences in a (v, k, m)-FHS. The results of RC $(65, 3, 23)$-FHS in Table 3.8 include up to two mutual interfering FH sequences since there are only three FH sequences in the FH scheme. We also approximate similarly the worst-case w-throughput for FH schemes from Table 3.6 and provide the results in Table 3.9.

FHS\ w	1	2	3	4	5	6
RW	0.66667	0.33333	0	0	0	0
DP	0.95652	0.91304	0.86957	0.82609	0.78261	0.73913
LG	0.95660	0.9132	0.8698	0.8264	0.7830	0.7396
CC	0.957	0.915	0.872	0.83	0.787	0.745
TF	0.95833	0.91667	0.875	0.83333	0.79167	0.75
RS	0.91304	0.82609	0.73913	0.65217	0.56522	0.47826
LS	1	1	1	1	1	1
RC	0.95385	0.90769	-	-	-	-

Table 3.8: Throughput of $(v, k, 23)$-FHS.

FHS\ w	1	2	3	4	5	6
RW2	0.66667	0.33333	0	0	0	0
DP2,CC2,RS2	0.98734	0.97468	0.96203	0.94937	0.93671	0.92405
LG2	0.9875	0.975	0.9625	0.9500	0.9375	0.9250
TF2	0.97468	0.94937	0.92405	0.89873	0.87342	0.84810
LS2	1	1	1	1	1	1
RC2	0.99882	0.99763	0.99645	0.99526	0.99408	0.99289

Table 3.9: Throughput of $(v, k, \approx 79)$-FHS.

The results in Table 3.8 show that LS $(23, 23, 23)$-FHS achieves maximum worst-case w-throughput of one for any w, $1 \leq w \leq 6$. The TF $(48, 11, 23)$-FHS is the next best in performance, while the RW $(3, 23 \cdot 8^2, 23)$-FHS performs poorly.

For large $m = 79$, the LS $(79, 79, 79)$-FHS is still the best with maximum w-throughput of one. However, the performance of TF2 $(79^2 - 1, 39, 79)$-FHS fare less than its counterpart TF $(48, 11, 23)$-FHS. The RC2 $(844, 15, 79)$-FHS performance is considerably better than the remaining FH schemes.

We also consider how many of the FH sequences in a (v, k, m)-FHS can be active in a session such that the w-throughput of an FH sequence in the presence of mutual interfering FH sequences is not zero. This is useful in defining the maximum size of an FHMA. It can also be useful in instances where storage space is limited such as wireless sensors. In this case not all the FH sequences need to be stored when only a small fraction of them can be usable and active. A central controlling authority can be used to distribute FH sequences to be used. Tables 3.10 and 3.11 provide the minimum number of active FH sequences such that the worst-case throughput is not zero. This information is also presented as a percentage of the total number of FH sequences in the (v, k, m)-FHS.

FHS	RW	DP	LG	CC	TF	RS	LS	RC
Usable active FH sequences	3	24	26	24	11	12	23	3
Percentage	0.203	4.54	0.21	51.06	100	52.17	100	100

Table 3.10: Approximate number of active FH sequences for positive worst-case throughput for $(v, k, 23)$-FHS.

FHS	RW2	DP2	LG2	CC2	TF2	RS2	LS2	RC2
Usable active FH sequences	3	80	81	79	39	79	79	15
Percentage	0.00784	1.28	1.3	100	100	100	100	100

Table 3.11: Approximate number of active FH sequences for positive worst-case throughput for $(v, k, \approx 79)$-FHS.

Tables 3.10 and 3.11 shows that LG and LG2 can accommodate more active FH sequences (26 and 81 respectively) than the rest of the FH schemes. Due to the nature of shift registers, the elements of active FH sequences which are transformations of m-sequences can be generated at a particular time slot. This makes LG and LG2 more attractive as storage of all the FH sequences is not required. Now the FH schemes, TF, LS, RC, CC2, TF2, RS2, LS2, RC2 can have all the FH sequences in them being active in a session.

3.10.2 Comparing jamming resistance

Recall in Chapter 2 that we introduced a (θ_1, θ_2)-adaptive jammer. We considered the jamming resistance of a (v, k, m)-FHS at a particular time slot. We gave the probability that a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer is eavesdropping on an active frequency channel in Equation (2.39):

$$Prob(i \text{ is active}) = 1 - \binom{k - a_i}{w+1} / \binom{k}{w+1}, \tag{3.56}$$

where $a_i = |\{j : x_t^j = i\}|$, the number of times that frequency channel i on which a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer is jamming appears at a particular time slot t of interest in a (v, k, m)-FHS, and $w+1$ is the number of active FH sequences. Note that at any time slot t:

$$Prob(i \text{ is active}) \geq 1 - \binom{k - a_j}{w+1} / \binom{k}{w+1},$$

for $i \in \mathcal{F}_t = \{x_t^0, \ldots, x_t^{k-1}\}$, the multiset of all frequency channels that appear in all the FH sequences at time slot t and $a_j = \min\{a_i : a_i > 0, 0 \leq i \leq m-1\}$. In some of the FH schemes considered in this chapter we went on to find the minimum number of time slots a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer needs to identify an active FH sequence. However, as this was not possible for all the FH schemes, in this section we compare jamming resistance using Equation 3.56.

Figures 3.4 and 3.6 (with Figures 3.5 and 3.7 showing a magnification of Figures 3.4 and 3.6 respectively at some coordinate for clarity) compares $Prob(i \text{ is active})$, denoted PR_{a_i}, with respect to $w+1$, the number of active FH sequences, for the FH schemes in Tables 3.5 and 3.6 respectively.

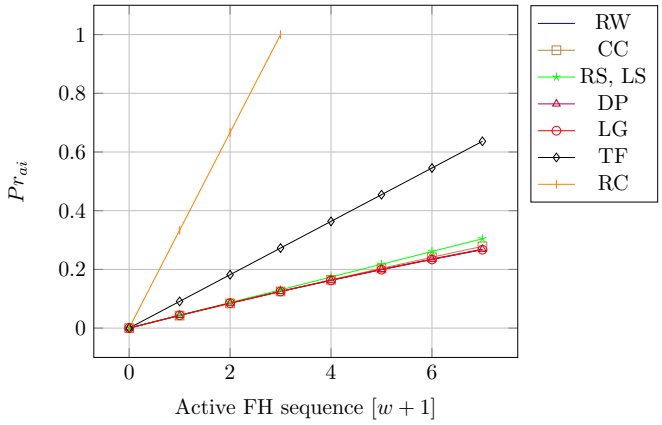

Figure 3.4: Jamming resistance at a time slot for $(v, k, 23)$-FHS.

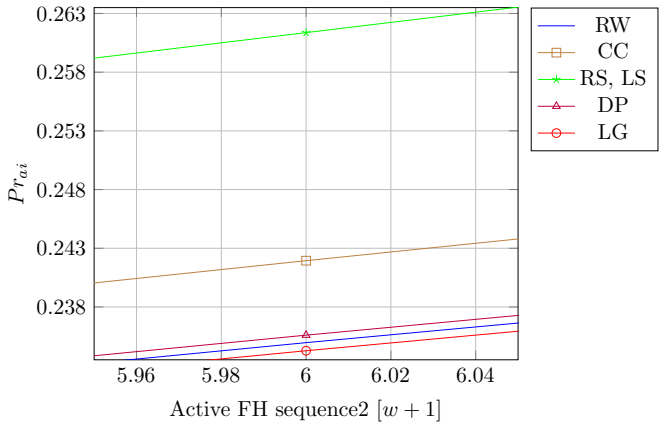

Figure 3.5: Jamming resistance at a time slot for $(v, k, 23)$-FHS.

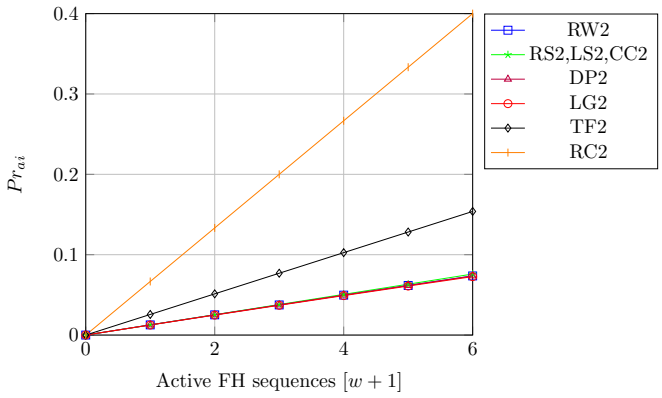

Figure 3.6: Jamming resistance at a time slot for $(v, k, \approx 79)$-FHSs.

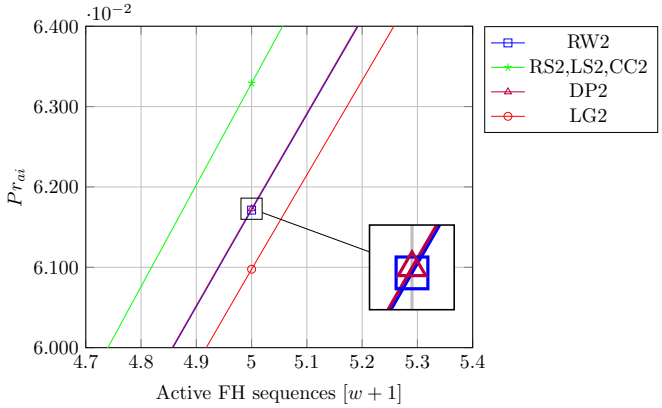

Figure 3.7: Jamming resistance at a time slot for $(v, k, \approx 79)$-FHSs.

The results in Figures 3.4 and 3.6 show that the resistance of (v, k, m)-FHS with small k against a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer is poor. This is because the jammer's chances of identifying an active FH sequence, given that there are only few FH sequences in the scheme is high.

3.11 Conclusion on comparison of FH schemes

Numerous FH schemes exist in the literature. In this chapter we have discussed some of these existing FH schemes. In Section 3.10 we have compared them with respect to throughput and jamming resistance.

In Section 3.10.1 we compared the worst-case w-throughput of FH schemes. We note that the size of the frequency library has an impact on the worst-case w-throughput of an FH scheme. The FH schemes whose size is small, $k \leq m$, perform well where there are minimal interference at each time slot. For example the LS $(23, 23, 23)$-FHS have $k = m$ and each frequency channel appears once at each time slot making it achieve maximum worst-case w-throughput of one.

In Section 3.10.2 we compared the jamming resstance of the FH schemes. In particular, we considered the probability of a (θ_1, θ_2)-adaptive jammer jamming on an active frequency channel. We saw that a (v, k, m)-FHS's jamming resistance is affected by a_i, the number of times that each frequency channel appears at a time slot in all the FH sequences of the FH scheme. It was mentioned in Chapter 2 that a jammer can choose i, where $a_i \geq a_j$ for all $i \neq j$, so that it maximises its chances of jamming an active channel. However, if a_i is uniform at each time slot, then each frequency channel is equally likely to be an active channel and thus a jammer would not be at an advantage.

Now, a_i creates a trade-off the between worst-case w-throughput and jamming resistance of an FH scheme. When $a_i = 1$ or small, then we have the best or better w-throughput respectively. On the other hand, if $a_i = 1$ or small then the jamming resistance of an FH scheme against a (θ_1, θ_2)-adaptive jammer is poor. In Chapter 4

we consider a (v, k, m)-FHS such that a (θ_1, θ_2)-adaptive jammer is forced to randomly choose a frequency channel to jam, since each frequency channel appears the same number of times at each time slot. Further, the (v, k, m)-FHS to be considered in Chapter 4 has the property that we can tell the minimum number of time slots it can withstand a (θ_1, θ_2)-adaptive jammer, as well as a lower bound on the worst-case w-throughput.

3.12 Summary

In this chapter we have considered several existing FH schemes in the new model developed in Chapter 2: FH schemes that use random walks in Section 3.2, difference packing in Section 3.3, m-sequences in Section 3.4, cyclotomic classes in Section 3.5, trace functions in Section 3.6, Reed-Solomon codes in Section 3.7, Latin squares in Section 3.8 and we have also considered recursive constructions in Section 3.9. We looked at the throughput of these FH schemes, in particular the throughput of FH sequences and the worst-case throughput of the FH schemes in the presence of mutual interference. We have also considered how long the FH schemes can withstand an adaptive jammer. In instances where we were not able to determine a lower bound on the number of time slots it can take an adaptive jammer to identify an active FH sequence, we have considered the probability of jamming an active frequency channel at a single time slot. In Section 3.10 we have compared the FH schemes: first with respect to their worst-case throughput in the presence of mutual interference, and second against their resistance to an adaptive jammer at each time slot. It is desirable to determine the worst-case throughput of an FH scheme in the presence of mutual interference, as well as its resistance against jamming, in particular the number of time slots required to identify an active FH sequence. In Section 3.10 we have only dealt with approximations. In Chapter 4 we introduce an FH scheme in which we can tell the worst-case throughput in the presence of mutual interference, as well as how long

it can withstand an adaptive jammer.

Chapter 4

Cover-free codes

Contents

4.1 Introduction

In this chapter we make the third major contribution of this thesis: we discuss the interpretation of cover-free codes as FH schemes. Preliminaries are covered in Section 4.2. In Section 4.3 we point out a correspondence between a cover-free code and an FH scheme. We note that when a cover-free code is considered as an FH scheme, a user can successfully transmit in at least a specified fraction of time in the presence of a given number of interfering FH sequences. To the best of our knowledge, we are the first to make this observation. In Section 4.4 we introduce a jammer in the cover-free code. We examine necessary and desirable additional properties of cover-free codes such that they can be used in the presence of adversarial interference.

4.2 Preliminaries

We begin with definitions and preliminaries on codes.

Definition 4.2.1. *Let $A = \{a_0, a_1, \ldots, a_{m-1}\}$ be an **alphabet**. A **code** $\mathcal{C}$ of length v over the alphabet A is a subset of A^v. An element $c \in \mathcal{C}$ is called a **codeword**. The **size** of the code, $|\mathcal{C}|$, is the number of elements in the code $\mathcal{C}$. A code $\mathcal{C} \subseteq A^v$ of size k is called a (v, k, m)-code.*

A code of length v that is a linear vector space of dimension $\kappa = \log_m k$ over a field $\mathcal{F}$, $|\mathcal{F}| = m$ is called a $[v, \kappa, m]$-*code*.

The Hamming distance of a code helps in analysing errors introduced in codewords. That is, the Hamming distance is a measure of how different a codeword c that was sent is from a word x that was received.

Definition 4.2.2. *Let $X = (x_0, x_1, \ldots, x_{v-1})$ and $Y = (y_0, y_1, \ldots, y_{v-1})$. The **Hamming distance** between X and Y is the number of coordinates in which they are different:*

$$d(X, Y) = \sum_{i=0}^{v-1} d(x_i, y_i),$$

where

$$d(x_i, y_i) = \begin{cases} 0 & \text{if } x_i = y_i, \\ 1 & \text{if } x_i \neq y_i. \end{cases}$$

Definition 4.2.3. *The **minimum Hamming distance** of a code $\mathcal{C} \subseteq \mathcal{F}^v$, $\mathcal{F}$ an alphabet is:*

$$d(\mathcal{C}) = \min\{\, d(X, Y) : X, Y \in \mathcal{C}, X \neq Y \,\}.$$

Definition 4.2.4. *A code $\mathcal{C} \subseteq \mathcal{F}^v$, $|\mathcal{F}| = m$, with k codewords and minimum Hamming distance d is denoted as a $(v, k, m; d)$-**code**, or as a (v, k, m)-code when d is unspecified.*

Suppose we consider FH sequences as codewords. Then a (v, k, m)-FHS can be treated as a (v, k, m)-code when the FH sequences are considered as codewords and vice versa.

In this chapter we consider a cover-free code as an FH scheme. Cover-free codes have been used in numerous contexts. Several authors [30, 44, 54], and the references therein, defined cover-free codes in the context of binary codes as follows.

Definition 4.2.5. *An $N \times T$ binary matrix C is called a (w, r)-**cover-free code** if for any pair of disjoint subsets $J_1, J_2 \subset [T]$, $|J_1| = w$ and $|J_2| = r$, there exists a row $i \in [N]$ such that $c_{ij} = 1$ for all $j \in J_1$, and $c_{ij} = 0$ for all $j \in J_2$.*

Stinson and Wei [99] discuss a related concept to cover-free codes.

Definition 4.2.6. *Let w, r and d be positive integers. A set system $X, \mathscr{F}$ is called a (w, r, d)-**cover-free family** (or (w, r, d)-CFF) provided that, for any w blocks $B_0, \ldots, B_{w-1} \in \mathscr{F}$ and any other r blocks $A_0, \ldots, A_{r-1} \in \mathscr{F}$, we have that*

$$\left| \left(\bigcap_{i=0}^{w-1} B_i \right) \setminus \left(\bigcup_{j=0}^{r-1} A_j \right) \right| \geq d.$$

Note that Definition 4.2.6 is defined in terms of a set system called a cover free family and not codes.

In this thesis we use the definition of cover-free codes of Staddon, Stinson and Wei [95] with a slight modification. The authors define a cover-free code as a code with a property that any codeword of the code is not covered in more than αv coordinates by a subset of w codewords of the code. As will be explained later, this definition provides one of the measures of performance of a cover-free code.

Definition 4.2.7. *Suppose that $\mathcal{S}$ is a (v, k, m)-code. For any subset $\mathcal{S}' \subseteq \mathcal{S}$ and any $X \in \mathcal{F}^v$, define:*

$$I(X, \mathcal{S}') = \{i : x_i = y_i \text{ for some } Y \in \mathcal{S}'\}. \tag{4.1}$$

*Then $\mathcal{S}$ is called (w, α)-**cover-free code**, denoted (w, α)-CFC, if $|I(Z, \mathcal{S}')| \leq (1 - \alpha)v$ for any $\mathcal{S}' \subseteq \mathcal{S}$, $|\mathcal{S}'| = w$ and any $Z \in \mathcal{S} \setminus \mathcal{S}'$.*

The difference in Definition 4.2.7 to that of Staddon [95] (Definition 4.1) is that we

have allowed equality at the size of the set of coordinates that covers a codeword for reasons that will become apparent later.

Note that a $(v, k, m; d)$-code is a $(1, d/v)$-CFC. We are interested in the case where $w > 1$.

The concept of cover-free codes as given by Staddon [95] has applications in black-listing, traitor tracing schemes and digital fingerprinting [46, 52, 95].

4.3 Cover-free codes as FH schemes

There is a direct correspondence between an FH scheme with a given Hamming group correlation and a cover-free code. Theorem 4.3.1 shows this correspondence.

Theorem 4.3.1. *Suppose $\mathcal{S}$ is a (v, k, m)-code over $\mathcal{F}$, $|\mathcal{F}| = m$. Then $\mathcal{S}$ is a (w, α)-CFC if and only if $\mathcal{S}$ is a (v, m, k)-FHS with worst-case w-throughput at least α.*

Proof. Suppose $\mathcal{S}$ is a (w, α)-CFC. In a cover-free code any codeword agrees in at most $(1-\alpha)v$ places with any other w codewords. Now, let us view the codewords of $\mathcal{S}$ as FH sequences of a (v, k, m)-FHS. Then we have $G(X, \mathcal{S}') = |I(X, \mathcal{S}')| \leq (1 - \alpha)v$, for any $\mathcal{S}' \subseteq \mathcal{S}$, $|\mathcal{S}'| = w$ and any $X \in \mathcal{S} \backslash \mathcal{S}'$. That is, any FH sequence experiences interference in at most $(1 - \alpha)v$ time slots from any other w FH sequences of the (v, k, m)-FHS. Then $\hat{\rho}_w(X, \mathcal{S}') \geq \alpha$ for all $X, \mathcal{S}'$. Therefore the worst-case w-throughput of the FH scheme is at least α, $\hat{\rho}_w(\mathcal{S}) \geq \alpha$.

Conversely, suppose we have a (v, k, m)-FHS, $\mathcal{S}$, such that $\hat{\rho}_w(\mathcal{S}) \geq \alpha$. Clearly we have $\rho_w(X, \mathcal{S}') \geq \alpha$ for any $X \in \mathcal{S}$ and any $\mathcal{S}' \subseteq \mathcal{S} \backslash \{X\}, |\mathcal{S}'| = w$. Again, if we consider the FH sequences in $\mathcal{S}$ as codewords, we have the following. Any codeword in $\mathcal{S}$ has at most $(1 - \alpha)v$ positions in which corresponding symbols are the same as those of any w codewords of the code, $1 - \frac{G(X, \mathcal{S}')}{v} \geq \alpha, \forall X, \mathcal{S}'$. Then we have $(1 - \alpha)v \geq G(X, \mathcal{S}')$. This implies $|I(X, \mathcal{S}')| \leq (1 - \alpha)v$. Therefore $\mathcal{S}$ is a (w, α)-CFC. □

The following trivial example illustrates Theorem 4.3.1.

Example 4.3.2. *Consider $\mathcal{S} \subset F^v$, the set of codewords of weight 1, that is the words of F^v with exactly one nonzero component. This is a $(w, \frac{1}{5})$-CFC for any w, it is a $(v, v(m-1), m)$-FHS with worst-case w-throughput at least $\frac{1}{5}$.*

Suppose we have the alphabet $\mathcal{F} = \{0, 1, 2, 3\}$. Then the code $\mathcal{S}$ defined over $\mathcal{F}^5$ has the following codewords:

$$(0,0,0,0,1),\ (0,0,0,0,2),\ (0,0,0,0,3),\ (0,0,0,1,0),\ (0,0,0,2,0),\ (0,0,0,3,0),$$
$$(0,0,1,0,0),\ (0,0,2,0,0),\ (0,0,3,0,0),\ (0,1,0,0,0),\ (0,2,0,0,0),\ (0,3,0,0,0),$$
$$(1,0,0,0,0),\ (2,0,0,0,0),\ (3,0,0,0,0).$$

Note that for any number of interfering FH sequences w, any codeword will transmit in one time slot. Therefore the worst-case w-throughput of $\mathcal{S}$ is $\frac{1}{5}$. Then $\mathcal{S}$ is a $(w, \frac{1}{5})$-CFC for any w.

It was proved in [95] (Theorem 4.3) that codes with large minimum distance are cover-free codes.

Theorem 4.3.3. *Suppose that $\mathcal{S}$ is a $(v, k, m; d)$-code such that $d \geq v(1 - \frac{1}{w^2})$. Then $\mathcal{S}$ is a $(w, 1 - \frac{1}{w})$-CFC.*

Proof. Suppose $\mathcal{S}$ is a $(v, k, m; d)$-code with minimum Hamming distance $d \geq v(1-\frac{1}{w^2})$. That is any pair of codewords have at least $v(1-\frac{1}{w^2})$ different corresponding coordinates and that they are the same in at most $\frac{v}{w^2}$ coordinates. Consider $\mathcal{U} \subseteq \mathcal{S}$, $|\mathcal{U}| = w$. For a codeword $Z \in \mathcal{S} \setminus \mathcal{U}$ and for any $Y \in \mathcal{S}$, $Y \neq Z$, then $v(1 - \frac{1}{w^2}) \leq d(\mathcal{S}) \leq d(Y, Z)$. Let I denote the set of coordinates in which they agree:

$$I(Y, Z) \leq v - v(1 - \frac{1}{w^2}) = \frac{v}{w^2}.$$

Note that Z agrees in at most $\frac{v}{w^2}$ coordinates with each codeword in $\mathcal{U}$. Thus:

$$I(Z, \mathcal{U}) \leq w \cdot \frac{v}{w^2} = (1 - (1 - \frac{1}{w}))v.$$

Hence $\mathcal{S}$ is a $(w, 1 - \frac{1}{w})$-CFC. □

We have the following as a corollary of Theorems 4.3.1 and 4.3.3.

Corollary 4.3.4. *A $(v, k, m; d)$-code with $d \geq v(1 - \frac{1}{w^2})$ provides a (v, m, k)-FHS with worst-case w-throughput at least $1 - 1/w$.*

Reed-Solomon codes are codes with large minimum distance and are described in the following example to illustrate Corollary 4.3.4.

Example 4.3.5. *Let v and w be integers where $v \geq 2$ and $w \geq 2$. Let m be a prime power such that $m \geq v$. Let $\mathcal{F}$ be a finite field of cardinality m and α a primitive element. Define a length v and w dimensional Reed-Solomon code $\mathcal{S}$ over $\mathcal{F}$ by,*

$$\mathcal{S} = \left\{ \left(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{v-1}) \right) : f \in \mathcal{F}[x] \text{ and } \deg f < \left\lceil \frac{v}{w} \right\rceil \right\}. \tag{4.2}$$

The code $\mathcal{S}$ is a $(w, 1 - 1/w)$-CFC code, which is a $(v, m^{\lceil \frac{v}{w^2} \rceil}, m)$-FHS with worst-case w-throughput at least $1 - 1/w$.

Recall in Section 3.7, Construction 3.7.3, we considered a particular subcode of a Reed-Solomon code as an FH scheme. Construction 3.7.3 is a special case of Example 4.3.5 and thus of a cover-free code when $v = m, m - 1, \lceil \frac{v}{w^2} \rceil = 1$.

4.4 Jamming resistance properties for cover-free codes

We now consider the throughput of cover free codes in the presence of both mutual interference and a jammer. We delve into further properties that cover-free codes should have to mitigate a (θ_1, θ_2)-adaptive jammer. For simplicity, we assume $\theta_1 m = \theta_2 m = 1$.

Consider $\mathcal{S}$ a (w, α)-CFC and $\mathcal{V} \subseteq \mathcal{S}$ a set of active FH sequences. A $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer can trivially reduce the worst-case w-throughput of $\mathcal{S}$ to 0 if $\mathcal{V} = \mathcal{S}$. If $\mathcal{V} = \mathcal{S}$, then all codewords in the cover-free code are active codewords. A jammer can choose any codeword $X \in \mathcal{S}$ and jam this codeword from the beginning of the session until the end, at each and every time slot. As a mitigation strategy we have:

M1 Use only a fraction of $\mathcal{S}$, that is $\mathcal{V} \subset \mathcal{S}$.

Recall the jammer does not know $\mathcal{F}_t^{active}$ or M_t^{active} the multisets of active frequency channels and multiplicity of active channels respectively. Then it can always guess which frequency channel to eavesdrop on using Equation (2.39). Recall the probability in (2.39) is maximum when the jammer selects a frequency channel i such that $a_i \geq a_j$ for all $i \neq j$. Therefore, if there exists some i such that $a_i \geq a_j$ for all $i \neq j$, then a jammer will choose frequency channel i to jam. A jammer follows the same strategy at any time slot t, $0 \leq t \leq v-1$. As a mitigation strategy against a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer we propose that:

M2 A (v, k, m)-FHS should have the property that all frequency channels used at any time slot t are uniformly distributed, that is we must have $a_0 = a_1 = \ldots = a_{m-1}$.

Recall, for a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer what happens at time t informs its next action at time $t+1$, therefore we also propose that:

M3 For all FH sequences with frequency channel i at time slot t, all frequency channels on the next time slot $t+1$ should be uniformly distributed. This forces a jammer to guess randomly at any time slot.

Properties **M2** and **M3** describe an orthogonal array.

Definition 4.4.1 (Hedayat, Sloane and Stufken, [43]). *A $k \times v$ array A with entries from $\mathcal{F}$ is said to be an **orthogonal array** with m **levels**, **strength** t', $0 \leq t' \leq v-1$, and **index** λ if every $k \times t'$ subarray of A contains each t' tuple based on $\mathcal{F}$ exactly λ times as a row and is denoted $OA_\lambda(k, v, m, t')$.*

It is well known that an orthogonal array of certain parameters are MDS codes as given by Theorem 4.4.2.

Theorem 4.4.2 (Hedayat, Sloane and Stufken, [43], Theorem 4.21). *An $OA_1(m^{t'}, v, m, t')$ (or simply $OA(m^{t'}, v, m, t')$), A, is a $(v, m^{t'}, m; v-t'+1)$-MDS code.*

Suppose we treat our $(v, m^{t'}, m; v - t' + 1)$ MDS code as a $(v, m, m^{t'})$-FHS. Then the properties of the $(v, m, m^{t'})$-FHS are as follows. Consider any t' consecutive time slots, for simplicity, $0, \ldots, t' - 1$. Any frequency channel in $\mathcal{F}$ appears $m^{t'-1}$ number of times at time slot 0. Next consider any $m^{t'-1}$ FH sequences with a frequency channel in $\mathcal{F}$ that appears at time slot 0. Then at time slot 1, any frequency channel in $\mathcal{F}$ appears $m^{t'-2}$ number of times on the $m^{t'-1}$ FH sequences of interest. Finally, at time slot $t' - 1$ any frequency channel in $\mathcal{F}$ appears once on FH sequences with a particular frequency channel at time slot $t' - 2$.

Now we introduce a $(\frac{1}{m}, \frac{1}{m})$-jammer in our $(v, m^{t'}, m; v - t' + 1)$-MDS code. We consider the situation where there is only one active FH sequence in use. At any time slot t, $0 \leq t \leq v - 1$, the number of times any symbol in $\mathcal{F}$ is used is uniform, a jammer randomly guesses a symbol to eavesdrop on. For any active symbol in $\mathcal{F}$ that it eavesdrops on, a jammer will have successfully identified an active codeword if the multiplicity of that frequency channel is 1. Otherwise, at time slot $t + 1$ its search is concentrated on the codewords with that particular symbol that appeared at the previous time slot. However, for any inactive symbol in $\mathcal{F}$ that it eavesdrops on at any time slot t, it removes from its search space the codewords with that specific symbol and on $t + 1$ continues its search on the remaining codewords at time t. The jammer continues this action until either of the following happens:

1. One active codeword is identified, or the size of its search space is at most the number of active codewords.

2. The session ends.

Searching until the end of the session means the jammer failed to identify an active codeword within the session.

Consider a $(v, m^{t'}, m; v - t' + 1)$-MDS code, $\mathcal{S}$. Recall $\mathcal{S}_t^*$ is the search space of a jammer at time slot t. Suppose that at time slot t, $0 \leq t \leq t'$, the jammer picks a channel x_t^j to eavesdrop on for some $X_j \in \mathcal{S}_t^*$. If this channel is active then $|S_{t+1}^*| =$

$\frac{1}{m}|\mathcal{S}_t^*|$, where S_{t+1}^* has all FH sequences with the active channel x_t^j and the FH sequences discarded at this stage are inactive FH sequences. On the other hand, if x_t^j is inactive then $|S_{t+1}^*| = \frac{m-1}{m}|\mathcal{S}_t^*|$ and again inactive FH sequences with x_t^j are discarded at this stage. Note that a lucky jammer always reduces the search space at least as quickly as an unlucky jammer. At any time slot t, $0 \leq t \leq t'$, $|\mathcal{S}_t^*| = (m-1)^B m^{t'-t}$, where B, $0 \leq B \leq t \leq t'$, is the number of time slots on which a jammer has been unlucky. Consider time slot t'. We now discuss what different values of B means with respect to the size of the jammer's search space and how long it takes to identify an active FH sequence:

1. If $B = 0$, that is a jammer has been lucky at all the t' time slots, then $|\mathcal{S}_{t'}^*| = 1$. Only one active FH sequence remains in the jammer's search space at this time slot, thereby successfully identifying the active FH sequence.

2. If $B = t'$, that is a jammer has been unlucky at all the t' time slots, then $|\mathcal{S}_{t'}^*| = (m-1)^{t'}$. Inactive FH sequences are discarded from the jammer's search space at each of the t' time slots.

3. For any other value of B such that $B \neq 0, t'$ we have $|\mathcal{S}_{t'}^*| = (m-1)^B > 1$. So, a change of luck does not speed up the time to identify an active FH sequence as it will take at least as long as the jammer that is always lucky at every time slot.

Table 4.1 considers FH schemes defined over frequency libraries of sizes comparable to those in the IEEE 802.11 standard [5]. It shows the performance of a (v, k, m)-FHS when $w+1$ FH sequences are used in the presence of mutual interferences and when a single active FH sequence is used in the presence of adversarial interference from a $(1/m, 1/m)$-adaptive jammer. We have a guaranteed worst-case w-throughput of at least α and the FH scheme can withstand a $(1/m, 1/m)$-adaptive jammer for at least γv time slots respectively.

(v, k, m)-FHS	(w, α)	γv
$(23, 23^3, 23)$	$(3, 0.6667)$	3
$(23, 23^2, 23)$	$(4, 0.75)$	2
$(23, 23^1, 23)$	$(22, 1)$	1
$(37, 37^5, 37)$	$(3, 0.6667)$	5
$(37, 37^3, 37)$	$(4, 0.75)$	3
$(37, 37^2, 37)$	$(5, 0.80)$	2
$(59, 59^7, 59)$	$(3, 0.6667)$	7
$(59, 59^4, 59)$	$(4, 0.75)$	4
$(59, 59^3, 59)$	$(5, 0.80)$	3
$(79, 79^9, 79)$	$(3, 0.6667)$	9
$(79, 79^5, 79)$	$(4, 0.75)$	5
$(79, 79^4, 79)$	$(5, 0.80)$	4

Table 4.1: Performance of (v, k, m)-cover-free codes.

From Table 4.1 it can be seen that there is a trade-off between α, the lower bound of the worst-case w-throughput in the presence of mutual interference, and γv, how long it takes a jammer to identify an active FH sequence. Note that by increasing the number of FH sequences, k, while the length, v, and the size of the frequency library, m, is fixed, then α diminishes while the resistance of the FH scheme against an adaptive jammer improves. However, the FH scheme does not withstand our jammer for long. A solution to this dilemma would be to restart the FH scheme every γv time slots. This will be elaborated further in Chapter 5, where an FH scheme is constructed that guarantees a w-throughput of one in the presence of mutual interference and withstands a jammer for an entire session.

4.5 Summary

In this chapter cover-free codes have been considered as FH schemes. Further we have seen that cover-free codes provide a defined lower bound on the worst-case w-throughput of an FH scheme.

Further we considered mitigating strategies for cover-free codes to be used in the presence of both mutual and adversarial interference. However, we showed that in the presence of our adaptive adversary, the cover-free code based FH schemes do not withstand the adaptive jammer for long. We will describe the secure Bag-Ruj-Roy (S-BRR) scheme in Chapter 5 that can be viewed as a cover-free code used in conjunction with pseudorandomness. This scheme provides an FH scheme with throughput one that can be used in the presence of an adaptive jammer and can withstand the adaptive jammer an entire session.

Chapter 5

A secure and efficient FH scheme

Contents

5.1 Introduction

We have seen that an FH scheme with the property that every frequency channel appears the same number of times at a single time slot has an improved resistance against a (θ_1, θ_2)-adaptive jammer. However it has been shown that even a (v, k, m)-FHS with this uniform number of channels at each time slot does not withstand a

(θ_1, θ_2)-adaptive jammer for a very long time. In this chapter we propose FH schemes that employ pseudorandomness.

In Section 5.2 we propose a secure-BRR (S-BRR) FH scheme. The S-BRR FH scheme uses a pair of orthogonal Latin squares to derive FH sequences as in the BRR FH scheme discussed in Section 3.8. The S-BRR FH scheme addresses the limitations of the BRR FH scheme in that it is more resistant to a (θ_1, θ_2)-adaptive jammer than the BRR FH scheme: it can withstand a (θ_1, θ_2)-adaptive jammer for the entire session of the FH scheme. In Section 5.3 we propose a pseudorandom Latin square (PR-LS) FH scheme. The PR-LS FH scheme uses a single Latin square to obtain FH sequences. This PR-LS FH scheme not only has the maximum w-throughput of one but is also secure in the presence of a (θ_1, θ_2)-adaptive jammer, as well as being attractive for use in resource-constrained devices.

5.2 Secure Bag-Ruj-Roy (S-BRR) FH scheme

The (v, k, m)-FHS of this section can be considered as a BRR FH scheme that resists a (θ_1, θ_2)-adaptive jammer for an entire session. We propose a desirable property, some form of pseudorandomness, which is introduced in a BRR FH scheme such that it can withstand the attack of a (θ_1, θ_2)-adaptive jammer.

Construction 5.2.1. *(S-BRR FH scheme). Let F_3 and F_4 be pseudorandom functions that take as input the long term key K, the session number s and the time slot t. The K and s are shared among all the users of the FH scheme. All users generate new keys at each time slot called* ***slot keys****: $x_t = F_3(K, s, t)$ and $y_t = F_4(K, s, t)$, $0 \leq t \leq m-1$.*

Let $L_1 = [\alpha_{ij}]_{v \times v}$ and $L_2 = [\beta_{ij}]_{v \times v}$ be a pair of orthogonal Latin squares of order m defined over $\mathbb{Z}_m$. At each time slot t, $0 \leq t \leq m-1$, user N_i looks up row i in L_2 to find the column j such that $\beta_{ij} = y_t$. Then it will looks up α_{ij} in L_1. Let L_3 be the superposition of L_1 and L_2. In each session a user N_i derives an FH sequence of

length m over $\mathbb{Z}_m$ from:

$$R_i^* = \{(\alpha_{ij}, \beta_{ij}) : \beta_{ij} = y_t, 0 \leq t \leq m-1\},$$

where $(\alpha_{ij}, \beta_{ij}) \in L_3$, $\alpha_{ij} \in L_1$ and $\beta_{ij} \in L_2$. A frequency hop at each time slot t, $0 \leq t \leq m-1$, is given by $\alpha_{ij} + x_t$. That is the FH sequence is:

$$X_i = (\alpha_{ij} + x_t).$$

The (v, k, m)-FHS in Construction 5.2.1 is an (m, m, m)-FHS. Essentially this FH scheme generates a new BRR FH scheme at each time slot.

Example 5.2.2. *Consider L_1 and L_2 a pair of orthogonal Latin squares of order 7:*

$$L_1 = \begin{array}{|c|c|c|c|c|c|c|}\hline 0&1&2&3&4&5&6\\\hline 1&2&3&4&5&6&0\\\hline 2&3&4&5&6&0&1\\\hline 3&4&5&6&0&1&2\\\hline 4&5&6&0&1&2&3\\\hline 5&6&0&1&2&3&4\\\hline 6&0&1&2&3&4&5\\\hline\end{array}, \qquad L_2 = \begin{array}{|c|c|c|c|c|c|c|}\hline 0&6&5&4&3&2&1\\\hline 1&0&6&5&4&3&2\\\hline 2&1&0&6&5&4&3\\\hline 3&2&1&0&6&5&4\\\hline 4&3&2&1&0&6&5\\\hline 5&4&3&2&1&0&6\\\hline 6&5&4&3&2&1&0\\\hline\end{array}.$$

Suppose we have the following slot keys:

t	0	1	2	3	4	5	6
x_t	5	6	4	5	5	4	2
y_t	3	2	6	6	4	4	0

.

Consider a Latin square L_3, the superposition of L_1 and L_2:

$L_3 =$

(0, 0)	(1, 6)	(2, 5)	(3, 4)	**(4, 3)**	(5, 2)	(6, 1)
(1, 1)	(2, 0)	(3, 6)	(4, 5)	(5, 4)	**(6, 3)**	(0, 2)
(2, 2)	(3, 1)	(4, 0)	(5, 6)	(6, 5)	(0, 4)	**(1, 3)**
(3, 3)	(4, 2)	(5, 1)	(6, 0)	(0, 6)	(1, 5)	(2, 4)
(4, 4)	**(5, 3)**	(6, 2)	(0, 1)	(1, 0)	(2, 6)	(3, 5)
(5, 5)	(6, 4)	**(0, 3)**	(1, 2)	(2, 1)	(3, 0)	(4, 6)
(6, 6)	(0, 5)	(1, 4)	**(2, 3)**	(3, 2)	(4, 1)	(5, 0)

.

In L_3 we have highlighted the entries that are used by all the users N_i, $0 \leq i \leq m-1$, on $t = 0$, the first time slot.

Consider user N_0. To determine the frequency channel to be used on $t = 0$ it employs $(4, 3)$ the entry in row $i = 0$ with $y_t = 3$. Then the frequency hop on $t = 0$ is:

$$4 + 5 \equiv 2 \mod 7.$$

In a similar manner, we can determine the frequency channels employed by all users at the first time slot. The frequency channels $2, 4, 6, 1, 3, 5, 0$ are used during the first time by users $N_0, N_1, N_2, N_3, N_4, N_5, N_6$ respectively. Note that we have distinct frequency channels at each time slot.

We now derive an FH sequence for N_0:

	User N_0
R_i^*	$\{(4,3,5),(5,2,6),(1,6,2),(1,6,2),(3,4,4),(3,4,4),(0,0,1)\}$
FH sequence	$(2,4,5,3,3,0,2)$

.

Therefore in our notation, an FH sequence for user N_0 is $(2, 4, 5, 3, 3, 0, 2)$.

5.2.1 Correlation

Consider $\mathcal{S}$ to be an S-BRR (m, m, m)-FHS of Construction 5.2.1. In the S-BRR FH scheme we have introduced slot keys which are shared by all users of the FH scheme. Let y_t be a slot key for time slot t. By definition each N_i look up row i in L_2 to find

column j such that $\beta_{ij} = y_t$. As L_2 is a Latin square, β_{ij} appears on m distinct columns. By the orthogonality property of L_1 and L_2, we have that all m tuples $(\alpha_{ij}, \beta_{ij})$, where $\alpha_{ij} \in L_1$, $\beta_{ij} \in L_2$, are distinct. Therefore each frequency channel $\alpha_{ij} + x_t$ used by N_i is again distinct. So, for any FH sequences there is no mutual interference in the presence of other users at each time slot. Therefore the S-BRR FH scheme has the same throughput as the BRR FH scheme. That is, the w-throughput of any FH sequence X_i in the presence of other FH sequences in $\mathcal{U} \subset \mathcal{S}$ is:

$$\rho_w(X_i, \mathcal{U}) = 1. \tag{5.1}$$

It follows from Equation (5.1) that the worst-case w-throughput of $\mathcal{S}$ is $\hat{\rho}_w(\mathcal{S}) = 1$.

5.2.2 Jamming resistance

Consider an S-BRR (m, m, m)-FHS of Construction 5.2.1. Assume that all the FH sequences are active.

Without loss of generality, consider a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer. Suppose a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer can identify α_{ij+x_t}, an active channel at a particular time slot t, $0 \leq t \leq m-1$. Knowledge of α_{ij+x_t} will not be used to derive any FH sequence since the slot keys, x_t, are updated at every time slot. Therefore a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer cannot derive any FH sequence as long as the pseudorandom number generator is secure. Hence the S-BRR is secure for an entire session.

5.3 A secure and efficient FH scheme

The (v, k, m)-FHS discussed in Chapters 3 and 4 have been shown to be insecure when used in the presence of a (θ_1, θ_2)-adaptive jammer. In Section 5.2 we proposed the S-BRR FH scheme where a new BRR FH scheme (see Section 3.8) is generated at each time slot. The S-BRR is better than the BRR FH scheme in that it not only achieve the maximum worst-case w-throughput of one but is also secure when used in the presence

of an adaptive jammer. However, the fact that the S-BRR FH scheme generates a new BRR FH scheme renders it costly in terms of the additional computations to be done by users, as well as storage resources since it stores two Latin squares. Therefore in this section we propose a pseudorandom Latin square (PR-LS) FH scheme that is both secure and efficient. The PR-LS attains a maximum worst-case w-throughput of one, it can withstand a (θ_1, θ_2)-adaptive jammer for the entire session, and it is more efficient than the S-BRR FH scheme.

5.3.1 Pseudorandom Latin square (PR-LS) FH scheme

Let F be a pseudorandom function that takes inputs K the long term key, s the session number, and t the current time slot. The key K and s are shared by all legitimate users. A slot key x_t, $0 \leq t \leq m-1$, is generated at each time slot as $x_t = F(K, s, t)$.

Construction 5.3.1. *(PR-LS FH scheme). Let $L = [\alpha_{ij}]_{m\times m}$ be a Latin square defined on $\mathbb{Z}_m$. The FH sequences of length m over $\mathcal{F} = \mathbb{Z}_m$ for a PR-LS FH scheme are:*

$$X_i = (\beta_{ij}),$$

where $\beta_{ij} = \alpha_{ij} + x_t \mod v$, $x_t = F(K, s, t)$, and $0 \leq i, j, t \leq m-1$.

The FH scheme in Construction 5.3.1 is an (m, m, m)-FHS.

Unlike the S-BRR FH scheme the newly proposed PR-LS FH scheme has reduced overhead in terms of the following:

1. Storage constraints: by definition the S-BRR FH scheme needs two Latin squares, while the PR-LS FH scheme uses only one Latin square. Therefore the PR-LS FH scheme is attractive for storage-constrained users, for example in wireless sensor networks.

2. Computational costs: suppose the existence of a central controlling authority (CA) that assigns FH sequences to each user in a network. In an S-BRR FH

scheme, the CA computes a new BRR FH scheme at each time slot to assign a frequency channel to each user and uses the pseudorandom function twice (for generating x_t and y_t). In a PR-LS FH scheme, on the other hand, the CA only calls the only pseudorandom function for generating x_t. Therefore, it is expensive to run the pseudorandom function for the S-BRR. If individual users generate their own FH sequences then we consider the difference in the running time of the FH scheme, which is described next.

3. Running time of the FH scheme: in the S-BRR FH scheme each user searches for a column such that $y_t = \beta_{ij}$, then finds α_{ij}. This is not the case with the PR-LS, where only α_{ij} is needed. Therefore the PR-LS FH scheme has a better running time.

We now provide an example of the construction of a PR-LS FH scheme.

Example 5.3.2. *Consider L_1 a Latin square of order 7 over $\mathbb{Z}_7$:*

$$L_1 = \begin{array}{|c|c|c|c|c|c|c|} \hline 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ \hline 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ \hline 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ \hline 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ \hline 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ \hline \end{array} .$$

Consider the following slot keys:

t	0	1	2	3	4	5	6
x_t	5	6	4	5	5	4	2

.

An FH sequence for user N_0 is $X_1 = (5, 0, 6, 1, 2, 2, 1)$.

It is interesting to note that a PR-LS FH scheme can also be interpreted in terms of codes in two ways:

1. A collection of m (m, m, m)-FHS, which are (m, m, m)-MDS codes of minimum distance m, where each FH scheme is used only once.

2. An MDS code with minimum distance one, that is an (m, m^m, m)-FHS. Only m sequences are used and these are determined by the pseudorandom number generator.

5.3.2 Correlation

Let $\mathcal{S}$ be a PR-LS FH scheme. It is easy to see that at each time slot t, $0 \leq t \leq m-1$, all the frequency channels $\alpha_{it} + x_t$, $0 \leq i \leq m-1$ are distinct. So, there is no mutual group interference at each time slot. Therefore we have the maximum achievable w-throughput of one for any w, $1 \leq w < m$,

$$\rho_w(X_i, \mathcal{U}) = 1,$$

where $X_i \in \mathcal{S}$ and $\mathcal{U} \subset \mathcal{S}$. As in both the BRR and S-BRR FH schemes, the worst-case w-throughput of $\mathcal{S}$ is $\hat{\rho}_w(\mathcal{S}) = 1$.

5.3.3 Jamming resistance

Consider a PR-LS FH scheme. By definition, we have introduced pseudorandomness at each time slot for all the FH sequences in the FH scheme. Suppose all the FH sequences are active. Now, consider the presence of a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer. The jammer has no knowledge of K, the long term key, as it is shared by only the legitimate users. Further, a fresh pseudorandom number x_t is generated at each time slot, which means a new Latin square is generated at each time slot. Suppose a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer eavesdrops on an active channel at time slot t. Then the jammer obtains $\alpha_{ij}+x_t$. Notice that the jammer cannot use x_t to derive any FH sequence since at the succeeding time slot $t+1$ all users generate a new pseudorandom slot key x_{t+1} and use it to determine the new hop $\alpha_{ij} + x_{t+1}$. Therefore a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer cannot identify an active

FH sequence for an entire session, where all the FH sequences in the FH scheme are allowed to be active. So we have an FH scheme that achieves maximum w-throughput of one and can withstand a $(\frac{1}{m}, \frac{1}{m})$-adaptive jammer for an entire session.

5.4 Summary

In this chapter, we proposed two new FH schemes: S-BRR and PR-LS FH schemes. These FH schemes use Latin squares to derive FH sequences. We have shown that Latin squares can be used to derive FH schemes that achieve both maximum throughput of one, as well as resist an adaptive jammer for an entire session at the expense of computation. The S-BRR FH scheme, which can be considered as generating a new BRR at each time slot, is efficient in terms of both throughput, as well as resistance against an adaptive jammer. Finally, the PR-LS FH scheme, which is also efficient in throughput and jamming resistance, is defined using a single Latin square, unlike the BRR FH scheme and the S-BRR FH scheme, which use a pair of Latin squares. By using a single Latin square, the PR-LS FH scheme may be desirable in resource-constrained networks.

Chapter 6

Conclusion and future work

Contents

6.1 Conclusion

In this thesis we have discussed frequency hopping schemes which are used in frequency hopping multiple access systems.

In Chapter 1 we introduced the theory of spread spectrum techniques. In more detail, we looked at direct sequence and frequency hopping spread spectrum techniques. We considered some existing frequency hopping schemes and pointed out the deficiency in the analysis of their performance.

In Chapter 2 we developed a new model of analysing the performance of a (v, k, m)-FHS in the presence of interference. We showed that it is inadequate to consider the performance of frequency hopping schemes based on either Hamming correlation or jamming, but not both, as has been the case with most of the existing research in the literature. So, in this thesis we have considered both group-wise mutual interference and adversarial interference (jamming), bearing in mind that more than two

users can be transmitting simultaneously in the presence of an adversary. We defined Hamming group correlation in Definition 2.4.1, from which many throughput measures were developed. Further, we modelled a jammer's strategy as frequency hopping sequences defined on the same frequency library as legitimate users. We then re-defined the throughput measure, bearing in mind the presence of both mutual interfering frequency hopping sequences, as well as jamming frequency hopping sequences.

In Chapter 3 we performed an extensive analysis of some of the existing frequency hopping schemes in the new model proposed in Chapter 2. We considered frequency hopping schemes constructed using the following mathematical structures: random walks on a graph, difference packing, m-sequences, cyclotomy, trace functions, Reed-Solomon codes, Latin squares, as well recursively constructed frequency hopping schemes. These frequency hopping schemes are optimal in the bounds in which they were analysed: Lempel and Greenberger, as well as Peng and Fan bounds. However, we were interested in analysing them in the presence of group-wise mutual interference, as well as jamming. For each of the frequency hopping schemes we investigated:

1. the w-throughput of a frequency hopping sequence in the presence of group-wise mutual interference, as well as worst-case w-throughput of a frequency hopping scheme.

2. the performance of a frequency hopping scheme in the presence of a (θ_1, θ_2)-adaptive jammer. In some frequency hopping schemes it was possible to determine the minimum number of time slots a jammer can take to identify an active frequency hopping sequence. In the BRR scheme, in particular, we showed that it is insecure as a jammer only needs to listen on a single time slot to identify an active frequency hopping sequence. Otherwise, we considered the probability of jamming on a channel that is being used at a specific time slot.

Next we compared the performance of all the frequency hopping schemes in terms of worst-case w-throughput. Then we considered the probability of jamming an active

channel. The results of the comparison of worst-case w-throughput in the presence of group-wise mutual interference showed that the frequency hopping scheme based on Latin squares (BRR frequency hopping scheme) is overall good compared to the other frequency hopping schemes as it achieve a maximum worst-case w-throughput of one. Now, using the worst-case w-throughput formula, we estimated the minimum number of active frequency hopping sequences that can be used in a frequency hopping scheme such that a frequency hopping sequence can transmit with positive throughput in the presence of other mutual interfering frequency hopping sequences. This result can be used to determine a lower bound on the maximum size of a network (frequency hopping multiple access system) such that each user has a positive throughput in the presence of other legitimate users. On the other hand, the results of the performance of the frequency hopping schemes in the presence of an adaptive jammer were that the smaller the size of the frequency hopping scheme, the poorer the performance. Given a frequency hopping scheme, we came to the conclusion that to minimise the probability of jamming an active channel it is desirable to have each frequency channel appear the same number of times at a time slot in the frequency hopping sequences.

In Chapter 4 we considered cover-free codes. When we design a frequency hopping scheme from a cover-free code we note that every frequency channel appears the same number of times at a time slot in the frequency hopping sequences. Further, it was observed that by definition a cover-free code provides the minimum number of time slots a frequency hopping sequence can transmit in the presence of group-wise mutual interference. Next we introduced a jammer in a cover-free code. The combinatorial properties of cover-free codes enabled us to determine the minimum number of time slots a (θ_1, θ_2)-adaptive jammer can take to identify an active frequency hopping sequence.

Thus far we have the BRR frequency hopping scheme that achieves worst-case w throughput of one but is not secure. We also have the cover-free code, for which we can determine a lower bound on its worst-case w-throughput, as well as the jamming

resistance, but is also not secure in the presence of an adaptive jammer. In fact the numerous frequency hopping schemes analysed in Chapters 3 and 4 are not secure in the presence of jamming. So, in Chapter 5 we proposed two frequency hopping schemes which use Latin square(s): S-BRR frequency hopping scheme and PR-LS frequency hopping scheme. Both of the proposed frequency hopping schemes achieve a throughput of one in the presence of group-wise mutual interference, as well as being able to withstand jamming until the end of a session. The difference between the two is that the S-BRR frequency hopping scheme uses a pair of orthogonal Latin squares, while the PR-LS frequency hopping scheme uses a single Latin square. The latter is thus both efficient and secure.

6.2 Future work

We now list possible future directions for our work.

- In this thesis we have assumed that users in a frequency hopping scheme can agree on $t = 0$, that is users know at which point in a frequency hopping sequence to start. We have also assumed that all users stay synchronised until the end of the session, where a session is taken as the length of a frequency hopping sequence. However, in practice this is not always the case. The length of the correlation window can sometimes be less than the length of a frequency hopping sequence. It is sometimes necessary to consider partial synchronisation in applications where synchronisation time has to be minimized, or to minimize hardware complexity in a receiver [10, 14, 32, 39, 71]. The question we now ask is how do we define group-wise mutual interference in a partially synchronised setting where the window length is less than the length of a frequency hopping sequence and can change over time depending on channel conditions.

- In Chapter 2 we discussed some of the lower bounds on Hamming correlation that exist in the literature, Lempel-Greenberger and Peng-Fan bounds. These bounds

measure the theoretical performance of frequency hopping schemes and involve some/all of the five parameters: the size of the frequency library, the length of a frequency hopping sequence, the size of a frequency hopping scheme, the maximum Hamming auto-correlation and the maximum Hamming cross-correlation. In Section 3.10.1 we have compared estimations of worst-case w-throughput of frequency hopping schemes. To improve the comparison of the different frequency hopping schemes we suggest determining a lower bound on the Hamming group correlation of frequency hopping schemes. The bound will then be used in the computation of the worst-case w-throughput and give a better comparison of the frequency hopping schemes.

- In some of the FH schemes considered in Chapter 3 and the FH scheme of Chapter 4 we discussed how the information about a channel a jammer eavesdrop on can determine its action on a succeeding time slot. We pointed out that this jamming strategy works when there is only one active FH sequence. In real life applications, we could have more than one active FH sequence. The jammer can exploit its knowledge of the number of active FH sequences as well as the information it obtains from the channels it eavesdrop on, to modify the size of the search space.

  Consider an FH scheme, with $w+1$, $w+1 \geq 1$, active sequences being used in the presence of an adaptive jammer. We consider the information that an adaptive jammer has, after eavesdropping on t time slots. The jammer uses the information it learns from eavesdropping to restrict its search space.

  At each time slot $t \geq 0$, a jammer knows that the channel it was eavesdropping on is either active or inactive. Further, the jammer has a partial sequence of channels it has eavesdropped on thus far up to time slot $t-1$.

  Suppose on the current time slot t the jammer eavesdrop on an active channel. The jammer creates all $(w+1)$-subsets from the current search space that are ca-

pable of producing the partial sequence (including the current frequency channel): we call these subsets the parent sets.

On the other hand, suppose on time slot t the channel is inactive. Then the jammer discard from the search space all the FH sequences with the inactive channel appearing on that time slot. This allows the jammer to restrict the search space even further. The jammer again creates $(w+1)$-subsets, parent sets, from the now smaller search space.

The jammer has identified at least one active FH sequence if the intersection of all parent sets is non-empty. If the intersection is empty, then the jammer repeats this algorithm again on time slot $t+1$. It stops when an active FH sequence has been identified or the session has ended.

So, we would like an FH scheme to have the property that the intersection of all the parent sets is empty for as large a t as possible.

Note that if an FH scheme is a $(w+1)$-IPP code [11, 38, 95] then a jammer that eavesdrops on an active channel in all v time slots can identify at least one active FH sequence. However, the identifiable parent property does not indicate whether it is possible to identify an active FH sequence in fewer time slots. In addition, in the case of a mixed-fate jammer, the jammer would want to identify an active sequence from a partial (eavesdropped) sequence. Modelling this jammer may lead to interesting correspondence between FH schemes with anti-jamming properties and IPP codes as well as other fingerprinting codes.

- In Chapter 5 we have mentioned that theoretically there is a trade-off between the security and computation costs for the S-BRR and PR-LS frequency hopping schemes. In both the S-BRR and PR-LS frequency hopping schemes we have more computations than in the BRR frequency hopping scheme, however we have the advantage of jamming resistance for an entire session. So, there is a need for the construction of frequency hopping schemes whose computational complexity

is reduced but at the same time is secure and has a worst-case w-throughput of one.

- Last but not least, in this thesis we have not determined the minimum number of time slots a jammer can take to identify an active frequency hopping sequence in most of the frequency hopping schemes. Since the frequency hopping schemes are diverse, in terms of the size of the frequency library, the length of the frequency hopping sequences, the size of the frequency hopping scheme, a jamming resistance comparison could be made through practical simulations. It is possible to reasonably model and simulate a frequency hopping anti-jam system, using for example SIMULINK.

Bibliography

[1] 802.11b Wireless LANs. Available online: http://web.stanford.edu/group/networking/NetConsult/wireless/wlan.html. Accessed: 17 July 2016. 9, 16

[2] Frequency Hopping Spread Spectrum (FHSS). Available online: http://ecomputernotes.com/digital-electronics/digital/frequency-hopping-spread-spectrum. Accessed: 26 July 2016. 9, 18

[3] Spread spectrum communication systems. Available online: http://www.ni.com/white-paper/14874/en/, 07 May 2014. Accessed: 17 July 2016. 9, 14

[4] Specification of the Bluetooth system version 4.0 B. *The Bluetooth Special Interest Group*, 2010. 24

[5] IEEE standard for information technology–Telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pages 1–2793, March 2012. 16, 18, 21, 128, 135, 154

[6] Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE 802.11 Wireless LANs, 2012. 53

[7] I. Anderson. *Combinatorial designs: Construction methods*. Ellis Horwood, 1990. 82

[8] I. Anderson. Some cyclic and 1-rotational designs. In J. W. P. Hirschfeld, editor, *Surveys in Combinatorics*, pages 47–73. Cambridge University Press, 2001. 130

[9] S. Bag, S. Ruj, and B. Roy. Jamming resistant schemes for wireless communication: A combinatorial approach. In *Springer Lecture Notes in Computer Science - Information Systems Security*, volume 8303, pages 43–62. 2013. 26, 27, 119, 122

[10] J. Bao and L. Ji. Frequency hopping sequences with optimal partial hamming correlation. Available online: http://arxiv.org/abs/1511.02924, 2015. Accessed: 20 March 2016. 169

[11] A. Barg and G. A. Kabatiansky. A class of i.p.p codes with efficient identification. *Journal of complexity*, 20(2):137–147, 2004. 171

[12] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*. Cambridge University Press, 2nd edition, 1986. 82

[13] M. Bishop. *Introduction to computer security*. Addison-Wesley, 2005. 50

[14] H. Cai, Z. Zhou, Y. Yang, and X. Tang. A new construction of frequency hopping sequences with optimal partial hamming correlation. *IEEE Transactions on Information Theory*, 60(9):5782–5790, 2014. 169

[15] P. J. Cameron. Strongly regular graphs. pages 203–221. L.W. Beineke, R.J. Wilson (Eds), Cambridge Univ. Press, 2004. 68, 75

[16] P. J. Cameron and J. H. van Lint. *Graph theory, coding theory and block designs (London Mathematical Society Lecture Notes Series)*. Cambridge University Press, 1975. 61

[17] Y. M. Chee, A. C. H. Ling, and J. Yin. Optimal partitioned cyclic difference packings for frequency hopping and code synchronization. *IEEE Transactions on Information Theory*, 56(11):5738–5746, 2010. 46

[18] P. Chiu. Cubic ramanujan graphs. *Combinatorica*, 12(3):275–285, 1992. 66

[19] W. Chu and C. J. Colbourn. Optimal frequency hopping sequences via cyclotomy. *IEEE Transactions on Information Theory*, 51(3):1139–1141, 2005. 23, 100, 103, 104, 106

[20] J. H. Chung, G. Gong, and K. Yang. New families of optimal frequency hopping sequences of composite lengths. *IEEE Transactions on Information Theory*, 60(6):3688–3697, June 2014. 129

[21] J. H. Chung, Y. K. Han, and K. Yang. New classes of optimal frequency hopping sequences by interleaving techniques. *IEEE Transactions on Information Theory*, 55(12):5783–5791, 2009. 24, 100, 129

[22] J.-H. Chung and K. Yang. Optimal frequency hopping sequences with new parameters. *IEEE Transactions on Information Theory*, 56(4):1685–1693, 2010. 100

[23] J.-H. Chung and K. Yang. k -fold cyclotomy and its application to frequency hopping sequences. *IEEE Transactions on Information Theory*, 57(4):2306–2317, April 2011. 46

[24] R. K. F. Chung. Spectral graph theory. *CBNS American Mathematical Society*, 1997. 65

[25] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs, Second Edition (Discrete Mathematics and Its Applications)*. CRC Press, 2006. 68, 77, 82

[26] G. Davidoff, P. Sarnak, and A. Valette. *Elementary Number Theory, Group Theory and Ramanujan Graphs*. Cambridge University Press, 2003. 65

[27] C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo, and M. Mishima. Sets of frequency hopping sequences: Bounds and optimal constructions. *IEEE Transactions on Information Theory*, 55(7):3297–3304, 2009. 24, 46, 107, 113, 114, 129, 130

[28] C. Ding, M. J. Moisio, and J. Yuan. Algebraic constructions of optimal frequency hopping sequences. *IEEE Transactions on Information Theory*, 53(7):2606–2610, 2007. 107

[29] C. Ding and J. Yin. Sets of optimal frequency hopping sequences. *IEEE Transactions on Information Theory*, 54(8):3741–3745, 2008. 100

[30] A. D'yachkov, V. Lebedev, P. Vilenkin, and S. Yekhanin. Cover-free families and superimposed codes: Constructions, bounds, and applications to cryptography and group testing, 2001. 148

[31] Y. Emek and R. Wattenhofer. Frequency hopping against a powerful adversary. In Y. Afek, editor, *Distributed Computing*, volume 8205 of *Lecture Notes in Computer Science*, pages 329–343. Springer Berlin Heidelberg, 2013. 25, 61, 62, 65, 67

[32] Y.-C. Eun, S.-Y. Jin, Y.-P. Hong, and H.-Y. Song. Frequency hopping sequences with optimal partial autocorrelation properties. *IEEE Transactions on Information Theory*, 50(10):2438–2442, Oct 2004. 169

[33] P. Fan and M. Darnell. *Sequence design for communications application*. Research Studies Press Ltd, 1996. 18

[34] A. Fiat and T. Tassa. Dynamic traitor tracing. *LNCS Advances in Cryptology -Crypto '99*, 1666:354–371, 1999.

[35] R. Fuji-Hara, Y. Miao, and M. Mishima. Optimal frequency hopping sequences: A combinatorial approach. *IEEE Transactions on Information Theory*, 50(10):2408–2420, 2004. 23, 24, 46, 80, 81, 82, 85, 129

[36] G. Ge, R. Fuji-Hara, and Y. Miao. Further combinatorial constructions for optimal frequency hopping sequences. *Journal of Combinatorial Theory, Series A*, 113(8):1699 – 1718, 2006. Special Issue in Honor of Jacobus H. van Lint. 46

[37] G. Ge, Y. Miao, and Z. Yao. Optimal frequency hopping sequences: Auto- and cross-correlation properties. *IEEE Transactions on Information Theory*, 55(2):867–879, 2009. 23, 107, 108, 109, 110

[38] J.-P. L. H. D. L. Hollmann, J. H. Van Lint and L. M. G. M. Tolhuizen. On codes with the identifiable parent property. *Journal of Combinatorial Theory*, Series A, 82:121–133, 1998. 171

[39] H. Han and D. Peng. Set of optimal frequency hopping sequences based on polynomial theory. *Electronics Letters*, 50(3):214–216, January 2014. 46, 169

[40] Y. K. Han and K. Yang. On the Sidel'nikov sequences as frequency hopping sequences. *IEEE Transactions on Information Theory*, 55(9):4279–4285, 2009. 100

[41] N. B. A. Handrizal and N. A. A. Ahmed. Spread spectrum process using direct sequence spread spectrum and frequency hopping spread spectrum. *National conference on postgraduate research*, 2009. 18

[42] F. Harary. *Graph Theory*. Addison-Wesley, 1969. 61

[43] A. S. Hedayat, N. J. A. Sloane, and J. Stufken. *Orthogonal arrays: Theory and applications.* Springer, June 22, 1999. 121, 152

[44] S. Hong, S. Kapralov, H. K. Kim, and D. Y. Oh. Uniqueness of some optimal superimposed codes. *Problems of Information Transmission*, 43(2):113–123, 2007. 148

[45] S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their applications. *BULL. AMER. MATH. SOC.*, 43(4):439–561, 2006. 65

[46] H. Jin and M. Blaum. Combinatorial properties for traceability codes using error correcting codes. *IEEE Transactions on Information Theory*, 53(2):804–808, Feb 2007. 47, 149

[47] T. Jin, G. Noubir, and B. Thapa. Zero pre-shared secret key establishment in the presence of jammers. In *Proceedings of the Tenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '09, pages 219–228, New York, NY, USA, 2009. ACM. 50

[48] B. W. Jordan and R. Livné. Ramanujan local systems on graphs. *Topology*, 36(5):1007–1024, 1997. 66

[49] D. Jungnickel. On difference matrices, resolvable transversal designs and generalized hadamard matrices. *Mathematische Zeitschrift*, 167(1):49–60, 1979. 129

[50] A. Kagan. *How Things Work: WLA Technologies and Security Mechanisms*. The SANS Institute, 7 November 2003. 16

[51] J. J. Komo and S. C. Liu. Maximal length sequences for frequency hopping. *IEEE Journal on Selected Areas in Communications*, 8(5):819–822, 1990. 46

[52] R. Kumar, S. Rajagopalan, and A. Sahai. Coding constructions for blacklisting problems without computational assumptions. In M. Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, volume 1666, pages 609–623. Springer Berlin Heidelberg, 1999. 149

[53] J. Lansford, A. Stephens, and R. Nevo. Wi-Fi (802.11b) and Bluetooth: Enabling coexistence. *IEEE Network*, 15(5):20–27, Sep 2001. 18

[54] V. S. Lebedev. A note on the uniqueness of (w, r) cover-free codes. *Problems of Information Transmission*, 41(3):199–203, 2005. 148

[55] A. Lempel and H. Greenberger. Families of sequences with optimal Hamming-correlation properties. *IEEE Transactions on Information Theory*, 20(1):90–94, 1974. 22, 23, 29, 32, 34, 35, 37, 46, 88, 94

[56] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1994. 108

[57] F. Liu, D. Peng, Z. Zhou, and X. Tang. A new frequency hopping sequence set based upon generalized cyclotomy. *Designs, Codes and Cryptography*, 69(2):247–259, 2013. 100

[58] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming resistant wireless broadcast communication. In *Proceedings of IEEE INFOCOM '10*, pages 1–9, March 2010. 50

[59] L. Lovász. Random walks on graphs: A survey. *Combinatorics, Paul Erdős is Eighty*, pages 353–397, 1993. 61

[60] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988. 65, 66

[61] M. M. M. Genma and M. Jimbo. Cyclic resolvability of cyclic steiner 2-designs. *Journal of Combinatorial Designs*, 5:177–187, 1997. 84

[62] W. Ma and S. Sun. New class of optimal frequency hopping sequences by polynomial residue class rings. *CoRR*, abs/1010.5291, 2010. 46

[63] A. Marcus, D. Spielman, and N. Srivastava. Interlacing families i: Bipartite ramanujan graphs of all degrees. *2013 IEEE 54th Annual Symposium on Foundations of computer science*, 2013. 66

[64] A. Marcus, D. Spielman, and N. Srivastava. Interlacing families iv: Bipartite ramanujan graphs of all sizes. *2015 IEEE 56th Annual Symposium on Foundations of computer science*, 2013. 66

[65] G. A. Margulis. Explicit group theoretical constructions of combinatorial schemes and their applications to the design of the expanders ad concentrators. *Problems of information Transmission*, 24(1):39–46, 1988. 66

[66] S. V. Maric and E. L. Titlebaum. A class of frequency hop codes with nearly ideal characteristics for use in multiple access spread spectrum communications and radar and sonar systems. *IEEE Transactions on Communications*, 40(9):1442–1447, Sep 1992. 22

[67] M. Mishima and M. Jimbo. Some types of cyclically resolvable cyclic Steiner 2-designs. *Congressus Numerantium*, 123:193–203, 1997. 85

[68] M. Morgenstern. Existence and explicit constructions of $q+1$-regular ramanujan graphs for every prime power q. *Journal of Combinatorial Theory, Series B*, 62:44–62, 1994. 66

[69] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou. A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys & Tutorials*, 11(4):42–56, 2009. 51

[70] S.-L. Ng and M. B. Paterson. Disjoint difference families and their applications. *Designs, Codes and Cryptography*, 78(1):103–127, 2016. 80

[71] X. Niu, D. Peng, and F. Liu. Lower bounds on the periodic partial correlations of frequency hopping sequences with partial low hit zone. In *2009 Fourth International Workshop on Signal Design and its Applications in Communications*, pages 84–87, Oct 2009. 169

[72] X. Niu, D. Peng, and Z. Zhou. New classes of optimal frequency hopping sequences with low hit zone with new parameters. In *Proceedings of the 5th International Workshop on Signal Design and its Applications in Communications*, pages 111 –114. 2011. 46

[73] M. M. Nyirenda, S.-L. Ng, and K. M. Martin. A combinatorial framework for frequency hopping multiple access. In *Proceedings of the Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory*, 2014. 27, 28, 46

[74] M. M. Nyirenda, S.-L. Ng, and K. M. Martin. A combinatorial model of interference in frequency hopping schemes. Available online: http://arxiv.org/abs/1508.02570, 2015. 98

[75] B. O'Hara and A. Petrick. *IEEE 802.11 Handbook: A Designer's Companion*. IEEE standards wireless networks series. Wiley, 2005. 22

[76] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy. Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications Surveys & Tutorials*, 13(2):245–257, 2011. 51

[77] D. Peng and P. Fan. Lower bounds on the Hamming auto- and cross-correlations of frequency hopping sequences. *IEEE Transactions on Information Theory*, 50(9):2149–2154, 2004. 22, 29, 32, 34, 37, 38, 39, 42, 44

[78] R. Peterson, R. Ziemer, and D. Borth. *Introduction to Spread Spectrum Communications*. Englewood Cliffs, N.J.: Prentice Hall, 1995. 50

[79] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein. Theory of spread-spectrum communications–a tutorial. *IEEE Transactions on Communications*, 30(5):855–884, 1982. 15

[80] A. K. Pizer. Ramanujan graphs and hecke operators. *Bulletin of the AMS*, 23(1), 1990. 66

[81] R. Poisel. *Modern communications jamming: Principles and techniques*. Artech House, illustrated edition, 2004. 15, 50, 55

[82] C. Pöpper, M. Strasser, and S. Čapkun. Jamming-resistant broadcast communication without shared keys. In *Proceedings of the 18th Conference on USENIX Se-*

curity Symposium, SSYM'09, pages 231–248, Berkeley, CA, USA, 2009. USENIX Association. 50

[83] J. Proakis. *Digital communications*. McGraw-Hill, 1995. 19

[84] J. Proakis. Interference suppression in spread spectrum systems. In *Proceedings of IEEE 4th International Symposium on Spread Spectrum Techniques and Applications*, volume 1, pages 259–266 vol.1, 1996. 50

[85] J. S. B. Raju and D. P. Harini. Novel techniques for transmissions to communication jamming denial-of-service attacks. *International Journal of Advanced Trends in Computer Science and Engineering*, 3(5):342–346, 2014. 55

[86] I. S. Reed. k^{th} order near orthogonal codes. *IEEE Transactions on information theory*, pages 116–117, 1971. 114, 115

[87] W. Ren, F. W. Fu, and Z. Zhou. New sets of frequency hopping sequences with optimal Hamming correlation. *Designs, Codes and Cryptography*, 72(2):423–434, 2014. 100

[88] M. D. Renzo and M. Debbah. Wireless physical-layer security: The challenges ahead. *International Conference on Advanced Technologies for Communications*, pages 313–316, 2009. 50

[89] R. Safavi-Naini and Y. Wang. Sequential traitor tracing. *IEEE Transactions on Information Theory*, 49(5):1319–1326, 2003.

[90] D. V. Sarwate. Reed-solomon codes and the design of sequences for spread-spectrum multiple access communications. In S. B. Wicker and V. K. Bhargava, editors, *Reed-Solomon Codes and their Applications*. IEEE Press, 1994. 18

[91] D. V. Sarwate. Optimum PN sequences for CDMA systems. In *Code Division Multiple Access Communications*, pages 53–78. Springer US, 1995. 23, 46, 113, 114

[92] R. A. Scholtz. The spread spectrum concept. *IEEE Transactions on Communications*, 25(8):748–755, 1977. 20

[93] S. M. Schwartz. Frequency hopping spread spectrum vs direct sequence spread spectrum in broadband wireless access and wireless LAN (white paper). http://sorin-schwartz.com/white\textunderscorepapers/fhvsds.pdf. Accessed: 2013-09-31. 20

[94] H. Song and S. Golomb. On the nonperiodic cyclic equivalence classes of reed-solomon codes. *IEEE Transactions on Information Theory*, 39(4):1431–1434, 1993. 113, 114

[95] J. N. Staddon, D. R. Stinson, and R. Wei. Combinatorial properties of frameproof and traceability codes. *IEEE Transactions on Information Theory*, 47(3):1042–1049, 2001. 148, 149, 150, 171

[96] W. Stallings. *Wireless communications and networks*. Prentice-Hall, Inc., 2002. 14

[97] D. R. Stinson. *Combinatorial Designs: Constructions and analysis*. Springer Theoretical Computer Science, 2004. 82, 121

[98] D. R. Stinson. *Cryptography: Theory and practice, third edition*. Chapman & Hall/CRC, 2006. 50

[99] D. R. Stinson and R. Wei. Generalized cover-free families. *Discrete Mathematics*, 279(1 - 3):463 – 477, 2004. 148

[100] T. Storer. *Cyclotomy and difference sets*. Chicago, IL: Markham, 1967. 101

[101] M. Strasser. *Novel techniques for thwarting communication jamming in wireless networks*. PhD thesis, ETH Zurich, February 2010. PhD thesis. 50, 55

[102] M. Strasser, C. Pöpper, and S. Čapkun. Efficient uncoordinated FHSS anti-jamming communication. In *Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing*, MobiHoc '09, pages 207–218, New York, NY, USA, 2009. ACM. 27

[103] N. Thakur and A. Sankaralingam. Introduction to jamming attacks and prevention techniques using honeypots in wireless networks. *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, 3(2):202–207, 2013. 50

[104] D. Torrieri. *Principles of spread spectrum communication systems*. Springer Science and Business Media, Inc, 2005. 15

[105] D. Torrieri. Code division multiple access. In *Principles of spread spectrum communication systems*, pages 365–463. Springer New York, 2011. 20, 21

[106] P. Udaya and M. U. Siddiqi. Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings. *IEEE Transactions on Information Theory*, 44(4):1492–1503, 1998. 46

[107] S. Čapkun, M. Čagalj, G. Karame, and N. Tippenhauer. Integrity regions: Authentication through presence in wireless networks. *IEEE Transactions on Mobile Computing*, 9(11):1608–1621, Nov 2010. 50

[108] H. Wang and P. Huang. Construction of a one coincidence frequency hopping sequence set with optimal performance. In W. Wang, editor, *Proceedings of the Second International Conference on Mechatronics and Automatic Control*, volume 334 of *Lecture Notes in Electrical Engineering*, pages 915–923. Springer International Publishing, 2015. 46

[109] Q. Wang. The linear span of the frequency hopping sequences in optimal sets. *Designs, Codes and Cryptography*, 61(3):331–344, 2011. 107

[110] Q. Wang and V. K. Bhargava. Spread spectrum and coding for multiple access communications. *Canadian Journal of Electrical and Computer Engineering*, 17(4):167–174, 1992. 28, 46

[111] G. H. Weiss. Random walks and their applications. *American Scientist*, 71(1):65–71, 1983. 61

[112] W. Xu, K. Ma, W. Trappe, and Y. Zhang. Jamming sensor networks: Attack and defense strategies. *IEEE Network*, 20(3):41–47, 2006. 51

[113] L.-L. Yang. *Multicarrier communications*. Wiley-Blackwell, 2009. 14

[114] Y. Yang, X. Tang, U. Parampalli, and D. Peng. New bound on frequency hopping sequence sets and its optimal constructions. *IEEE Transactions on Information Theory*, 57(11):7605–7613, 2011. 113, 115

[115] X. Zeng, H. Cai, X. Tang, and Y. Yang. A class of optimal frequency hopping sequences with new parameters. *IEEE Transactions on Information Theory*, 58(7):4899–4907, 2012. 100, 129

[116] X. Zeng, H. Cai, X. Tang, and Y. Yang. Optimal frequency hopping sequences of odd length. *IEEE Transactions on Information Theory*, 59(5):3237–3248, 2013. 100

[117] Y. Zhang, P. H. Ke, and S. Y. Zhang. Optimal frequency hopping sequences based on cyclotomy. *First International Workshop on Education Technology and Computer Science*, 1:1122–1126, 2009. 100