The Hong Kong Polytechnic University

Department of Electronic and Information Engineering

A thesis submitted for the Degree of Master of Philosophy

Enhancements in Chaos-Based Digital Communication Systems

Cheong Kai-Yuen

October 2003

CERTIFICATE OF ORIGINALITY

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it reproduces no material previously published or written nor material which has been accepted for the award of any other degree or diploma, except where due acknowledgement has been made in the text.

(Kai-Yuen Cheong)

Abstract

Use of chaos as a fast and convenient mean to spread the spectrum of a signal has received much attention in communication engineering in the past few years. The advantages of spread-spectrum communications include the robustness against multipath fading, resistance to jamming and high secrecy due to low probability of detection. On the other hand, many problems are there to overcome in chaos communication. They include the synchronization problem for coherent demodulation and the estimation problem due to the random-like property of chaos. Moreover, in a spread-spectrum system, the issue of bandwidth efficiency must be considered. For instance, multiple users should be able to use the same frequency band without interfering with each other.

This thesis studies the modulation-demodulation methods in chaos communications. The study is centered on the previously proposed chaos-shift-keying (CSK) and differential chaos-shift-keying (DCSK) systems. The thesis includes the study of detection methods of CSK and a mul-

tiple access system based on DCSK. Also, an M-ary scheme for chaos communications is proposed.

The performances of the digital communication systems in this thesis are measured by their bit error rates (BER). The channel is assumed to be of additive white Gaussian noise (AWGN). Computer simulations are carried out and analyses are given. Overall evaluations are also presented.

Publications arising from the thesis

1. K.Y. Cheong, F.C.M. Lau and C.K. Tse, "Permutation-based *M*-ary chaotic-sequence spread-spectrum communication systems," *Circuits, Systems and Signal Processing,* to appear.

2. F.C.M. Lau, K.Y. Cheong and C.K. Tse, "Permutation-based DCSK and multiple access DCSK systems," *IEEE Transactions on Circuits and Systems I,* vol. 50, no. 5, pp. 702–707, 2003.

3. K.Y. Cheong, F.C.M. Lau and C.K. Tse, "An M-ary spread-spectrum communication system based on permutated chaotic-sequences," in *Proceedings, ECCTD'03,* vol. 3, Kraków, Poland, Sept. 2003, pp. 237–240.

4. K.Y. Cheong, F.C.M. Lau and C.K. Tse, "An M-ary spread-spectrum communication system based on permutated chaotic-sequences," in *Proceedings, RIUPEEEC'03,* Hong Kong, China, Aug. 2003,

pp. 151–152.

5. F.C.M. Lau, K.Y. Cheong and C.K. Tse, "A permutation-based multiple access DCSK system," in *Proceedings, NOLTA'02,* Xian, China, Oct. 2002, pp. 511–514.

Acknowledgement

Upon the completion of this thesis, I would like to express my gratitude to Dr Francis Lau, my supervisor, for his guidance and support through the ups and downs in these two years. I must also thank my co-supervisor Professor Michael Tse, who has broadened my views on so many things since I was an undergraduate.

Also, I am grateful to all the colleagues and friends in the Hong Kong Polytechnic University, with whom I live the most wonderful years in my life. I am indebted to them for their encouragement and inspiration.

And surely I must thank my parents for making everything here possible. I sincerely dedicate this thesis to them.

Contents

List of Figures

Chapter 1

Introduction

1.1 About the Definition of Chaos

The definition of chaos seems to be the first simple issue for this thesis. Modern chaos theory was rooted in the study of complex dynamical systems by Poincaré more than a century ago. With the aid of the rapid development of computing technology, Lorenz shaped the study of chaos in science [1] with his discovery of chaotic motions in a model of atmospheric convection [2]. The term "chaos" first appear in year 1975 [3], and since then, the study of chaos proliferates in all aspects of science.

Unfortunately, a universally accepted definition of chaos is not yet available [4, 5, 6]. In general, chaos is the term used to describe the random-like behavior of deterministic physical systems. It is commonly agreed that the sensitivity to initial condition is necessary for a system's

state, as a discrete or continuous function of time, to be chaotic. That is, any two different orbits initially close together diverge over time. For example, orbits of the map

$$x_{k+1} = 4x_k(1 - x_k) \tag{1.1}$$

have this property. As discussed in [4], it is not clearly defined what can be called a chaos or not, but all candidates are trajectories of deterministic mechanisms. This is the fundamental difference between a random variable and a chaotic trajectory. The random-like behavior of a chaotic signal is limited to its unpredictability, which occurs only because it is not possible to determine the initial condition exactly. The uncertain part of the initial condition becomes a random variable, causing eventually a deterministic system to become unpredictable. In practice chaos is recognized to be partly random and partly deterministic. In some engineering situations, chaotic signals might have advantages over random signals, and this thesis studies the advantages of using chaotic signals in digital communication systems.

In this thesis, the mathematical definition of a chaotic map given by [7] is sufficient for our purpose. All chaotic signals considered in this thesis are generated by chaotic maps under this definition. Omitting the details and explanations of terms used, it can be expressed as follows. Let $\boldsymbol{V}$ be a set. The function $f : \boldsymbol{V} \to \boldsymbol{V}$ is said to be chaotic on $\boldsymbol{V}$ if

1. f has sensitive dependence on initial conditions;

2. f is topologically transitive; and

3. periodic points are dense in $\boldsymbol{V}$.

1.2 Spread-Spectrum Communications

Spread-spectrum modulation is a technique widely used in communication systems. It produces a signal of much higher bandwidth than the input data signal [8, 9] and transmits it to the channel. This technique sacrifices bandwidth efficiency in order to gain other advantages of a spread-spectrum signal.

Channel defects such as multipath fading can be coped with by using spread-spectrum modulation. While the unintended paths are harmful to narrowband signals, a spread-spectrum signal remains robust in such channels. Also, security needs often justify the use of spread-spectrum systems. In situations where low detectability of signal by unintended receivers and high anti-jamming robustness are needed, the energy of the transmitted signal must be spread over a wide bandwidth, and a spread-spectrum system becomes the basic requirement.

Currently, the direct-sequence and frequency-hopping spread spectrum techniques are usually used in practical communication systems [8]. Some variations are also found, but basically most techniques involve a

pseudorandom process [9]. This process produces a random-like but reproducible signal. The random-like property is used to spread the spectrum of the data signal and enhance the security of the communication system.

1.3 Motivations for the Study of Chaos Communications

As discussed in the last section, a pseudorandom process is useful in many areas in spread-spectrum communications. Unlike other currently available pseudorandom signals, chaotic signals are not periodic, and are unpredictable in the long term. Also, it can be found in continuous form instead of only binary sequences. Moreover, the generation of chaos is relatively easy.

But there are some questions to be answered first. Chaotic signals are reproducible only under certain conditions. The design of a communication system based on chaos has to take the issue of chaos synchronization into account. Also, communications based only on chaos may not be very secure, due to the presence of nonlinear time-series recovery techniques. Spectral properties of chaos is another concern for spread-spectrum communications which involves the study of dynamical systems.

In spite of the difficulties, research in this area is getting more and

more mature in recent years [10, 11, 12]. Chaos communication is expected to be a new choice for practical spread-spectrum communication systems.

1.4 Methodology and Layout of Thesis

This thesis is entitled "Enhancements in Chaos-Based Digital Communication Systems." Analog communications is also discussed briefly in the next chapter, where recent research results of the field relevant to this thesis are reviewed. The three chapters after that are my studies and proposals of new chaotic communication systems based on existing research results. Chapter 3 is a discussion on methods that identify a chaotic system by extracting parameters from the signals it generates. Applications to communication systems are illustrated. Chapter 4 discusses a multiple access communication system. As each user of a spread-spectrum communication system occupies a much larger bandwidth than the data bandwidth, multiple access becomes a necessary feature of any such system in practical use. Chapter 5 presents a chaos-based communication system with M-ary enhancement to improve the system performance over binary systems.

In all the communication schemes proposed, modulation and demodulation are explained in terms of system architecture and the processing

of signals. Rationales and analyses are given, while computer simulations by Matlab and Mathematica programs are carried out to give the actual system performances.

The performance of a digital communication system is measured by plotting the bit error probability or bit error rate (BER) against E_b/N_0, the average-bit-energy to noise-power-spectral-density ratio. Average bit energy is calculated by multiplying the average bit duration by the average signal power. For an M-ary system, the average bit duration is obtained by dividing the symbol duration by the number of bits N carried by each symbol, which is given by $N = \log_2 M$. Also, by converting M-ary symbols to and from binary bits at the receiver and sender, bit error rate can be obtained for M-ary systems.

In this thesis, one-dimensional discrete chaotic signals are generated by second or third order Chebyshev polynomials unless specified otherwise. That is, with a randomly chosen initial condition $x_0 \in [-1, +1]$, we generate x_k by

$$x_k = T_n(x_{k-1}) = \cos(n \cos^{-1}(x_{k-1})) \tag{1.2}$$

where n equals 2 or 3. The maps can also be conveniently expressed as

$$\begin{aligned} T_2(x) &= 2x^2 - 1 \\ T_3(x) &= 4x^3 - 3x. \end{aligned} \tag{1.3}$$

In this thesis all signals studied are discrete. The discrete system is

used as an equivalent model of a general continuous-time bandpass system. Following the derivations in [11], the E_b/N_0 ratio of the continuous-time system equals $(\beta\sigma_s^2)/(2\sigma_n^2)$ in the discrete-time model. Here σ_s^2 and σ_n^2 are the variances of the discrete-time signal and noise samples, respectively, while β, also called the spreading factor, is the number of signal chips used to represent one bit. Moreover, since the bandwidth of the continuous-time system equals to half of the chip frequency in the discrete-time model according to the sampling theorem, the bandwidth-duration product WT_b in the continuous-time system [8] can be shown to be

$$\begin{aligned} WT_b &= \frac{2T_b}{T_c} \\ &= 2\beta \end{aligned} \tag{1.4}$$

where T_b and T_c are the bit duration and the sampling period, respectively.

Chapter 2

Existing Research Results

2.1 Issues of Concern

Given the possible advantages of chaos communications, various modulation and demodulation schemes were proposed in the past few years. From the information theory point of view, it has been shown that it is possible for the noise performance of a chaos communication system to be as good as traditional communication systems [13]. Unfortunately, the performance of a practical chaos communication scheme currently available is still far worse than traditional systems such as the binary phase-shift-keying (BPSK) system.

In communication engineering, there are three levels where chaos may be injected. They are, from bottom to top, the hardware level, the signal level and the coding level. At each level chaos offers different possibil-

ities [10], and they may be divided into two categories, coherent and noncoherent detections. Coherent detections assume that the receiver has a copy of the set of all possible signals that could be transmitted by the other side, before the signal is received. Noncoherent detections do not have this assumption.

In chaos communications, coherent detection unavoidably implies a chaos synchronization process, which is possible but difficult [14, 15]. For analog communication schemes, those based on chaos masking [16] generally require the synchronization process, while those with direct chaotic modulation [17] do not necessarily require it. For digital modulation schemes, both coherent and noncoherent ones are readily found. For instance, in [18], the simple chaotic on-off keying (COOK) modulation is basically noncoherent. The chaos-shift-keying (CSK) system and the differential chaos-shift-keying (DCSK) system can be coherent or not, depending on the system design. The performance of coherent detection is always better than noncoherent detection in an additive white Gaussian noise (AWGN) channel when synchronization is possible [8].

Other concerned issues in chaos communications include system security [19] and multiple access. In the following sections of this chapter, some of these topics are discussed in more detail.

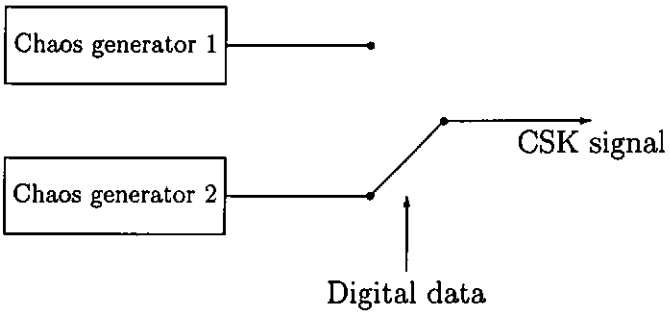

Figure 2.1: Block diagram of the transmitter of a general CSK system.

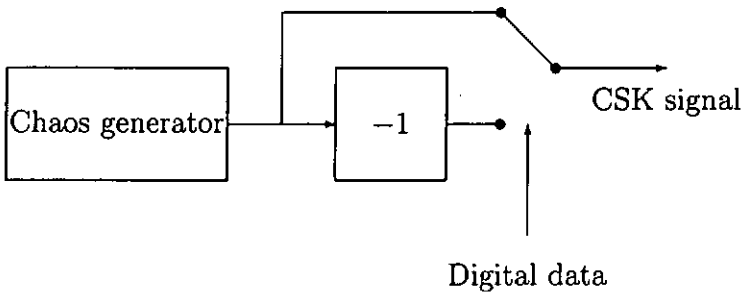

Figure 2.2: Block diagram of the transmitter of an antipodal CSK system.

2.2 CSK System

The CSK is, among the many schemes proposed so far, the simplest and most direct method of chaos communication at the signal level. The transmitter of CSK, as shown in Figure 2.1, basically consists of two chaos generators representing two digital symbols, and a switch which is set according to the binary data. The transmitter of one special type of CSK, the antipodal CSK, is shown in Figure 2.2. Under certain conditions,

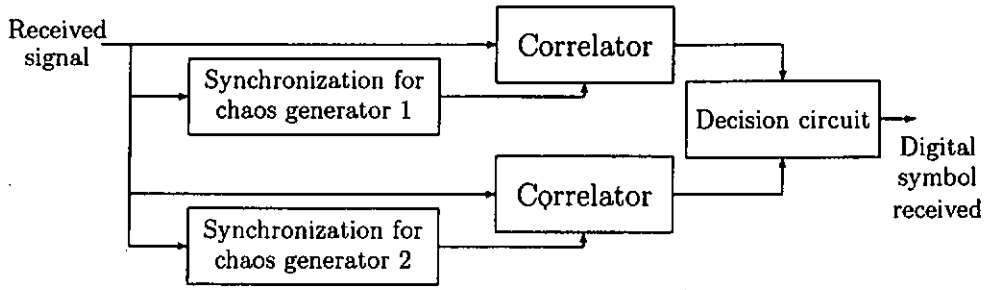

Figure 2.3: Block diagram of the coherent detector of a general CSK system.

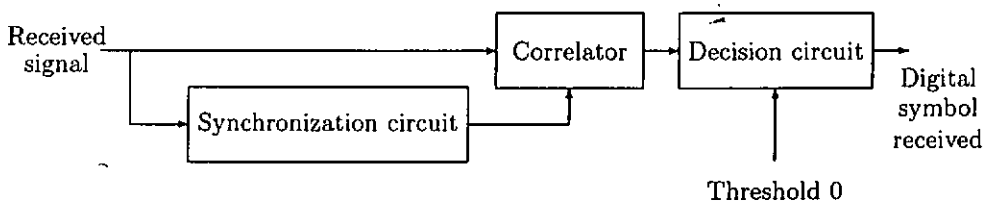

Figure 2.4: Block diagram of the coherent detector of an antipodal CSK system.

antipodal CSK offers the best performance over all CSK systems [20].

Architecture of the receiver is found in different versions, coherent and noncoherent. Figure 2.3 and 2.4 show the coherent detectors for the general CSK and the antipodal CSK systems, respectively. In the coherent schemes, detections are basically done by a matched filter or an equivalent correlator [8], which offers optimal detection.

In chaos communication, if the same set of signals is to be repeatedly used in every symbol duration, coherent detection can be achieved easily as the sender and receiver can make an agreement about the set of signals to be used. In that case, the system is close to some form of a direct-sequence spread-spectrum communication system. Normally, in CSK systems, we assume that a new signal is used for each symbol duration, and the signals produced by the chaos generators will not repeat. If coherent detection is to be used, synchronization of chaotic signals between the sender and receiver must be achieved. As discussed before, such a synchronization is possible theoretically, but practical difficulties might make noncoherent detections more feasible.

When coherent detection cannot be achieved, noncoherent methods will be used. Figure 2.5 shows the detector when the digital symbol received can be determined by extracting one parameter from the received signal. Figure 2.6 shows another noncoherent detector where two separate devices are used to detect the two possible symbols, and the

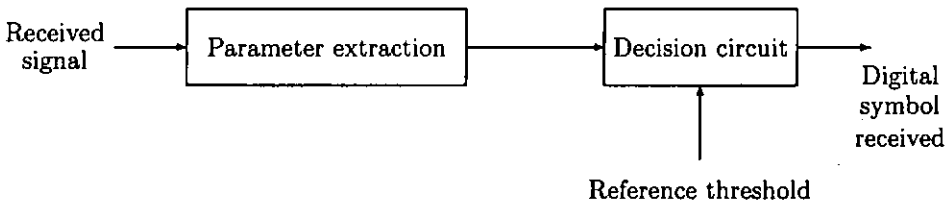

Figure 2.5: Block diagram of the noncoherent CSK detector using one parameter for detection.

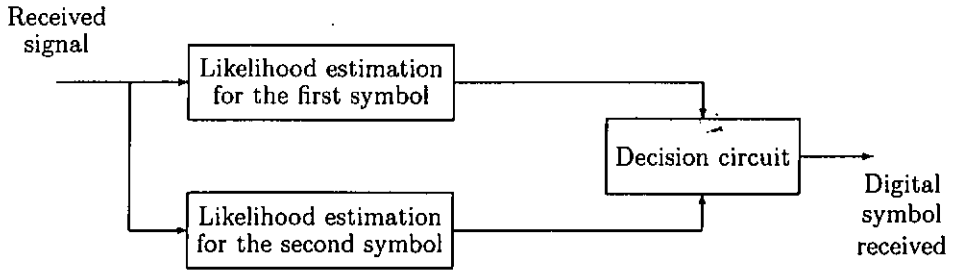

Figure 2.6: Block diagram of the noncoherent CSK detector with two separate detection blocks for the two symbols.

likelihood functions of the symbols are estimated and compared.

In a CSK system, noncoherent demodulation is not easy. The receiver has to decide which symbol is transmitted at the sender's side, only by looking at a signal of finite length corrupted by noise. In the following, we review some of the existing methods that is used to identify chaotic attractors and decode digital data in CSK. Some other methods are proposed and discussed in Chapter 3 of this thesis.

In the noncoherent CSK system proposed in [18], the signal variance is the key parameter for demodulation. In other words, the average power of signals produced by the two chaos generators at the modulation side are used to distinguish the two digital symbols. One extreme case is the COOK system, where chaotic signal is only present when symbol "1" is sent, and transmission is turned off when symbol "0" is sent.

As discussed in [18], the main drawback of such schemes is that the receiver's symbol decision threshold depends on the noise level. Another obvious problem is that the system has no security, any unintended receiver can decode the data easily.

In [21] another suggestion was made. If the probability density functions of the two chaotic attractors used by the sender are known, the receiver can estimate the likelihood that a particular symbol is being sent by comparing the received signal with the probability density functions. For instance, by [22] it is known that a random sample drawn from

an orbit produced by the Chebyshev polynomials follows the probability density function

$$\rho(x) = \frac{1}{\pi\sqrt{1-x^2}} \tag{2.1}$$

with $-1 < x < 1$.

Another approach to identify a chaotic attractor is to inspect the dynamics of its trajectory. With a chaotic signal contaminated by noise, we can determine how likely that the signal is generated by a particular system by comparing the signal with all possible trajectories produced by the system. For instance, denote the received signal by $\boldsymbol{r} = (r_1, r_2, \cdots, r_n)$. Assuming that the signal is corrupted by AWGN with a probability density function

$$p_\eta(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-(x^2/2\sigma^2)} \tag{2.2}$$

where σ^2 denotes the noise power, then the likelihood that the original signal transmitted by the sender is $\boldsymbol{s} = (s_1, s_2, \cdots, s_n)$ can be estimated by the probability density function

$$p(\boldsymbol{r}|\boldsymbol{s}) = \prod_{i=1}^{n} p_\eta(r_i - s_i). \tag{2.3}$$

So the overall likelihood that a particular map $x_{i+1} = f_\alpha(x_i)$ is being used by the sender can be represented by the probability density function

$$p(\boldsymbol{r}|\alpha) = \int_{-\infty}^{\infty} p_s(s_1) \prod_{i=1}^{n} p_\eta(r_i - f_\alpha^{(i-1)}(s_1)) ds_1. \tag{2.4}$$

Here $p_s(x)$ is the probability density function of a sample value taken from the chaotic attractor represented by $f_\alpha(x)$, and $f_\alpha^{(k)}(x)$ is the iteration of $f_\alpha(x)$ for k times.

This method of inspecting the whole trajectory at once is found in variations in noise reduction techniques [23] and CSK communication systems [24]. In the noncoherent CSK system using two chaotic dynamical systems known by both sides, the receiver first computes the likelihood values for the received signal to be produced by the two dynamical systems, and then compare the two values to decode the symbol transmitted. Theoretically this maximum likelihood approach gives the optimum receiver for noncoherent CSK. However, in practical systems, numerical approximations unavoidably degrades the system performance. The return map approach provides an alternative that gives acceptable performance with lower computational requirements.

In the return map approach of CSK using one-dimensional maps, the pairwise relation of consecutive points on the received trajectory is inspected in order to construct the return map. The chaotic attractor used, and so the digital data transmitted, can be estimated by either the probability approach or the simple regression approach [25]. As the name implies, performance of the return map approach is sensitive to the maps used [26]. The major drawback is that the results obtained from one particular set of maps may not be applied to another set.

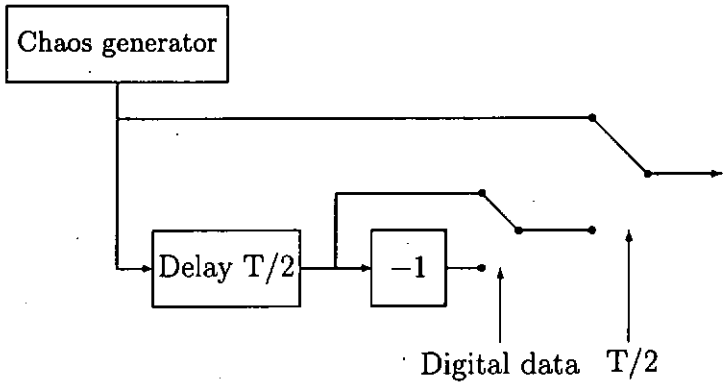

Figure 2.7: Block diagram of the transmitter of a DCSK system.

2.3 DCSK System

The modulator of a DCSK system is shown in Figure 2.7. In the first and second half of each bit duration, a reference chaotic signal and a data signal are sent respectively. If bit "+1" is to be sent in this bit duration, the data signal is the same as the reference signal. If bit "−1" is to be sent, the data signal is the inverted version of the reference signal. Basically, demodulation is done by finding the correlation between the reference signal and the data signal. The block diagram of a DCSK demodulator is shown in Figure 2.8. Note that the correlator in Figure 2.8 operates only in the second half of every bit duration. If the correlation is positive, "+1" is decoded as the symbol sent, otherwise "−1" is decoded.

A variation of DCSK is the frequency modulated DCSK (FM-DCSK) scheme, which basically inserts a frequency modulator at the output

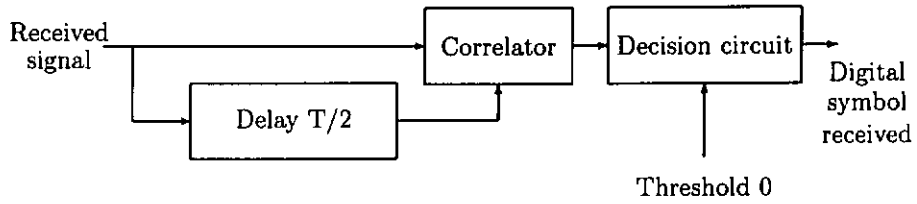

Figure 2.8: Block diagram of the receiver of a DCSK system.

point of the chaos generator in the DCSK modulator. The main advantage of FM-DCSK is that the bit energy is constant for every bit, which eliminates the estimation problem in the DCSK system. It has been shown that the FM-DCSK has a good potential to be applied in practical communication systems [27, 28, 29].

2.4 Chaotic-Sequence Communications

The basic motivation for chaos communications is to take advantage of the inherently wideband chaotic signals. The CSK and DCSK systems are two such examples. Another option is to use chaos in the coding level of communications. For example, a direct application of chaos to the existing direct-sequence spread-spectrum system is to replace the binary sequences for spreading binary symbols by aperiodic chaotic sequences [30]. The use of chaotic sequences may enhance the system security, compared with conventional systems using periodic sequences, due to the increased

difficulty in detecting the chip frequency. Another example is the application of chaotic-sequences in frequency-hopping communication systems [31]. Moreover, binary sequences for the use of spread-spectrum systems may also be generated by chaotic dynamics [32].

The first issue of concern in communications using chaotic-sequences is the correlation properties of the sequences [33], especially when multiple access is required. Chaotic-sequences are basically uncorrelated in the long term, but extra processing is required if orthogonality is needed for short sequences. Most proposed systems using chaotic-sequences do not ensure their orthogonality, but the performances are still acceptable.

2.5 Multiple Access in Chaos-Based Communications

A spread-spectrum communication system generally allows multiple access in order to achieve reasonable bandwidth efficiency. Also, multiple access using spread-spectrum techniques is advantageous over the traditional time-division multiple-access (TDMA) and frequency-division multiple-access (FDMA) in several aspects [9, 11].

In chaos communications, while code-division multiple-access (CDMA) systems using chaotic-sequences [33, 34, 35] are being investigated by the mainstream, a few multiple-access systems based on CSK and DCSK are

also available [20, 36, 37]. Other chaos communication schemes proposed so far are mostly single-user systems.

In the multiple-access CSK scheme, each user simply injects the CSK signals into the channel independently, as in a single-user system. The signal obtained by each receiver is the sum of the signals of all users, with distortions caused by the channel. Demodulation is achieved by correlating the received signal with the synchronized chaotic signal in each sender-receiver pair.

For noncoherent detections, the multiple-access DCSK system proposed in [36] uses a time-delay approach to reduce the interference between the users. The essential feature of this scheme is that the frame structure of reference and data signal is different for each user. For instance, the jth transmitter sends j reference blocks in a row before the data blocks are sent. In this way the total number of bits sent will always be a multiple of j. Figure 2.9 shows the frame structure for the first three users. Demodulation is accomplished by correlating the reference signal with the corresponding data signal. It can be shown that, for every bit sent by each user, no other user uses the same two time slots to send the reference and data signal for another bit. Thus, excessive interference is avoided and the users can share the channel.

The multiple-access FM-DCSK scheme in [20] also uses different frame structures for different users. Walsh functions are used to produce orthog-

User 1 (Conventional DCSK)

$R_{1,1}$	$D_{1,1}$	$R_{1,2}$	$D_{1,2}$	$R_{1,3}$	$D_{1,3}$	$R_{1,4}$	$D_{1,4}$	$R_{1,5}$	$D_{1,5}$	$R_{1,6}$	$D_{1,6}$

User 2

$R_{2,1}$	$R_{2,2}$	$D_{2,1}$	$D_{2,2}$	$R_{2,3}$	$R_{2,4}$	$D_{2,3}$	$D_{2,4}$	$R_{2,5}$	$R_{2,6}$	$D_{2,5}$	$D_{2,6}$

User 3

$R_{3,1}$	$R_{3,2}$	$R_{3,3}$	$D_{3,1}$	$D_{3,2}$	$D_{3,3}$	$R_{3,4}$	$R_{3,5}$	$R_{3,6}$	$D_{3,4}$	$D_{3,5}$	$D_{3,6}$

Figure 2.9: Frame structure of a 3-user multiple-access DCSK system for 6 bits. $\boldsymbol{R}_{i,j}$ is the reference signal of the jth bit of the ith user, and $\boldsymbol{D}_{i,j}$ is the corresponding data signal.

onal signals and zero inter-user interference is ensured. In Figure 2.10, the essential frame structure of a simplified four-user system is shown. For each user, the same block of chaotic signal or its inverted version is sent repeatedly for a number of times. For each receiver, the Walsh function corresponding to the user is used again to remove the signals of others. Demodulation can then be accomplished without difficulty. Note that the frame structure also improves noise performances. As the same block of chaotic signal is sent a number of times, the effect of noise can be lowered by averaging.

In Chapter 4 of this thesis, another multiple-access DCSK system based on permutation techniques is proposed.

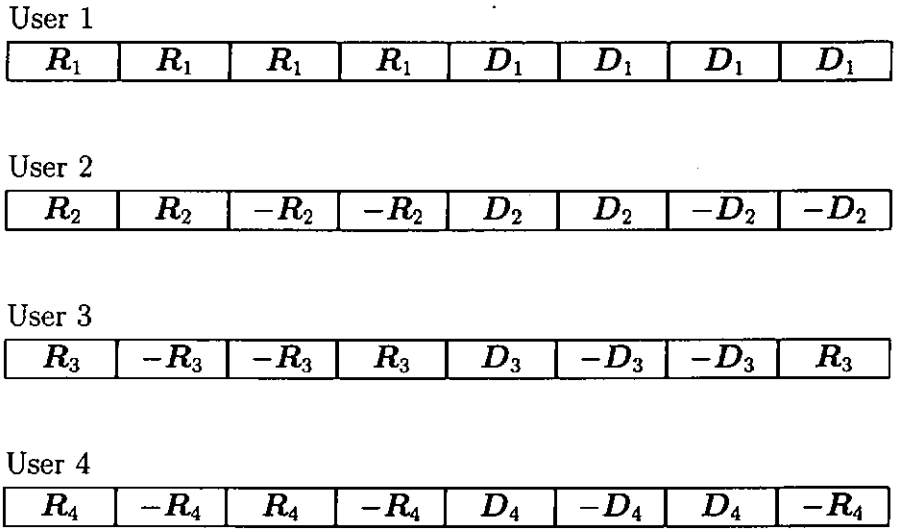

Figure 2.10: Frame structure of a 4-user multiple-access FM-DCSK system for one bit duration. $\boldsymbol{R}_i$ is the reference signal of the ith user and $\boldsymbol{D}_i = \alpha_i \boldsymbol{R}_i$ where $\alpha_i \in \{-1, +1\}$ is the digital data of the ith user.

2.6 M-ary Transmissions in Chaos-Based Communications

In chaos-based digital communication systems, digital symbols to be transmitted are mapped to chaotic signals. Depending on the demodulation techniques, the signals used must be long enough to carry certain characteristics for the receiver to detect. To eliminate the effect of the random-like behavior of chaotic signals, the symbol duration of a chaos-based digital communication system is usually much longer than that of conventional communication systems. Also, chaotic signals occupy a much larger bandwidth. To reasonably utilize the channel and increase the data rate, multiple access should be allowed, or an M-ary transmission scheme should be used.

For each symbol duration in an M-ary system, a symbol out of $M > 2$ possible symbols is transmitted. The advantage of having M symbols instead of just two is that each symbol now carries more information and the data rate is increased using the same channel.

Several M-ary schemes based on DCSK can be found in [38]. One approach is to scale the signal magnitude to several levels according to the symbols transmitted. Correlation between the reference and data part can also be scaled by introducing some extra delay in the modulator.

Sometimes, techniques for multiple-access can be applied to M-ary

systems. For instance, in the demonstration shown in Figure 2.10, a user can simultaneously use several modulators and transmit more than one bit within one symbol duration. As long as the signals produced by the modulators are orthogonal, they will not interfere with each other in both the multiple-access system and the M-ary system.

In this thesis, another M-ary chaos communication scheme is proposed. In the proposed system, the number of symbols M is much larger than that of the existing schemes. It will be introduced in Chapter 5.

Chapter 3

Identification of Chaotic Attractors

3.1 Fractal Dimension

Fractals are self-similar complex objects found in nature [39]. Some fractals such as the Koch curve have simple mathematical definitions, while others may be produced by some chaotic processes [40]. The concept of dimension in geometry can be extended to fractal objects, of which the dimension is not an integer. For instance, given a fractal object in the Cartesian space, we can find its box-counting dimension [40] by covering the space with a grid of edge length ϵ and calculate

$$D_b = \lim_{\epsilon \to 0} \frac{\log(N(\epsilon))}{\log(\frac{1}{\epsilon})} \tag{3.1}$$

where $N(\epsilon)$ is the box-count of the object occupying the space in the grid.

While D_b gives a geometrical approach to calculate fractal dimension, a similar quantity named correlation dimension [41] is more convenient and practical to use when the object is represented by a set of data points in the space. With the set of data points $\{z_1, z_2, \cdots z_K\}$ in Cartesian space, the correlation integral is defined as

$$C(\epsilon) = \lim_{K\to\infty} \frac{1}{K^2} \sum_{i,j}^{K} U(\epsilon - \|z_i - z_j\|) \tag{3.2}$$

where $U(x)$ is the unit step function, giving 1 or 0 as a counter upon whether its argument x is positive or not. The correlation dimension D_c is then

$$D_c = \lim_{\epsilon\to 0} \frac{\log C(\epsilon)}{\log(\epsilon)}. \tag{3.3}$$

While D_b and D_c are just two approaches to calculate dimension, in practice the two quantities calculated for a general finite set of data points can differ slightly.

The following experiment illustrates the possibility to use the concept of dimension in a communication system. Suppose we are to build a CSK system with two chaos generators. The sender uses two chaotic signals known to have different fractal dimensions, and the receiver decodes by using an algorithm which calculates correlation dimensions according to (3.2) and (3.3). The algorithm first collects the K data points from the

received signal and uses a few chosen values of ϵ to plot $\log C(\epsilon)$ against $\log(\epsilon)$. A value of D_c is then obtained from the slope of the line plotted.

In the simulation the first map chosen by the sender is the Chebyshev map of the second order, as shown in (1.3), which is sometimes called the logistic map. The other map is the two-dimensional Hénon map [40], which is simplified here as

$$x_k = 1.4 - x_{k-1}^2 + 0.3x_{k-2} \tag{3.4}$$

for our purpose. It can be shown that no information is lost when the two-dimensional orbit of the Hénon map is changed to this one-dimension form for the purpose of signal transmission.

The signal that the receiver receives are corrupted by noise, so we have

$$r_k = s_k + \xi_k \tag{3.5}$$

where s_k represents the Hénon map or logistic map sample sent by the sender, ξ_k is the noise sample and r_k denotes the received sample. The receiver constructs a three-dimensional signal by assigning $z_k = (r_k \;\; r_{k-1} \;\; r_{k-2})$, for the use of computations based on (3.2). When the noise level is low and the number of data points is high, the data points z_k collectively reveal the true correlation dimension of the chaotic attractor behind. The three-dimensional signal construction can be replaced by other such constructions of higher dimension. It is chosen only

because we already know that the correlation dimensions of our attractors are lower than three.

Finally, the receiver performs the numerical computations to extract the correlation dimension of signal. Figure 3.1 and Figure 3.2 shows two independent trials of the extraction of correlation dimensions from the chaotic signals. In both trials, the number of chaotic samples sent to represent a symbol is set to 1000, which is necessary for computing the dimension. For both the logistic map and Hénon map signals, we plot the correlation dimensions extracted against the E_b/N_0 ratio, where E_b denotes the total energy of the signal representing one symbol, and N_0 the noise power spectral density.

It can be observed that the algorithm become unreliable when E_b/N_0 is lower than 60 dB. When E_b/N_0 decreases, i.e., noise level increases, the correlation dimension first rises and then drops. But for both cases we can no longer distinguish the logistic or Hénon attractors from each other. The rise can be explained by the fact that noise samples are uncorrelated, and they just randomly fill up the space concerned. Thus, they tend to increase the calculated correlation dimension of the received samples. The cause of the drop when the noise power is even higher is that the algorithm recognizes the samples as zero-dimensional separate points as they are scattered in a large space. In other words, since the number of samples K in (3.2) is finite in a practical experiment, it may

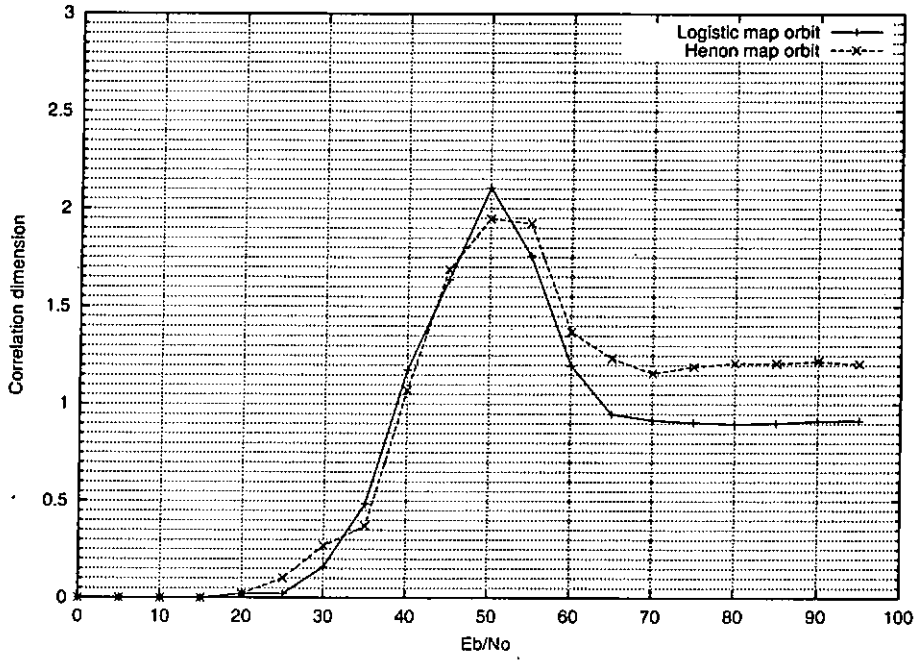

Figure 3.1: First trial of correlation dimension extraction from orbits of different chaotic attractors in a noncoherent CSK system.

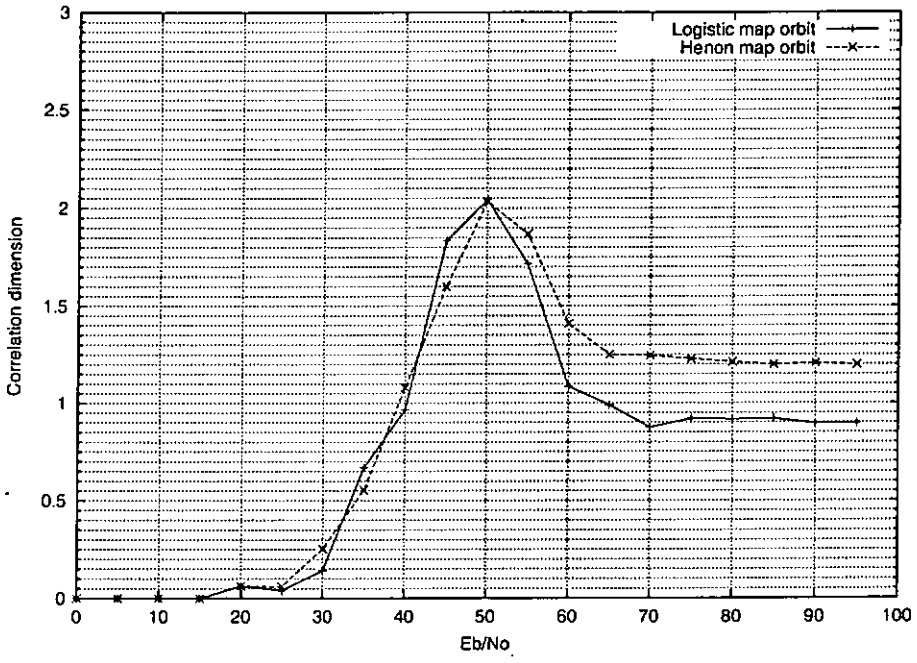

Figure 3.2: Second trial of correlation dimension extraction from orbits of different chaotic attractors in a noncoherent CSK system.

not be large enough for the samples to fill up the space as they should, and it is more obvious when noise level is higher because the space to fill is larger in that case.

As we can see, fractal dimension can be readily obtained from a chaotic orbit when the noise level is low. Unfortunately, due to the use of ϵ, which is a very small quantity, the algorithm implemented is sensitive to the noise level. Also, the computational requirement of the algorithm is high, due to the large number of data points needed. As a conclusion, chaos communications based on the extraction of correlation dimension may not be very feasible.

3.2 Lyapunov Exponent

The main feature of chaos is the sensitivity to initial conditions. The Lyapunov exponent is a parameter which accounts for this sensitivity [40]. It gives the average exponential rate of divergence of nearby orbits.

Mathematically, given an orbit $\{x_1, x_2, \cdots\}$, which is generated by a map $x_{i+1} = f(x_i)$, the Lyapunov exponent $L(x_1)$ for the one-dimensional map is defined as

$$L(x_1) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \ln |f'(x_i)|. \tag{3.6}$$

The extraction of Lyapunov exponent can be very accurate when there is no noise and the given orbital data set is long enough. When the

map $f(x)$ is not available, we can extract the Lyapunov exponent of an orbit by finding pairs of segments in it which are close to each other at the beginning and diverge later on. In other words, in (3.6), we attempt to estimate $f'(x)$ by $(f(x) - f(y))/(x - y)$ where y, found by searching the orbit, is a value close to x. This method is applicable to CSK systems in which the map being used is exactly what the receiver needs to guess.

The following simulation experiment is conducted to obtain the actual performance of this method. In this experiment, a noncoherent CSK system using two chaotic maps is simulated. The first map is the Chebyshev map of the second order. The second map is the Chebyshev map of the fourth order. That is, we use the two maps

$$T_2(x) = \cos(2\cos^{-1} x) \tag{3.7}$$

$$\begin{aligned} T_4(x) &= \cos(4\cos^{-1} x) \\ &= \cos(2\cos^{-1}\cos(2\cos^{-1} x)) \\ &= T_2(T_2(x)) \end{aligned} \tag{3.8}$$

in the hope that the rate of divergence of the second map is exactly double of the first one. As the map $T_2(x)$ is topologically conjugate to the tent map, their orbits have the same Lyapunov exponents [22]. The magnitude of slope is 2 for every point on the tent map, so the theoretical Lyapunov exponent of a tent map orbit is $\ln 2$. The corresponding Lyapunov exponents are thus $\ln 2$ and $\ln 4$ for the maps $T_2(x)$ and $T_4(x)$.

In the simulated CSK system, signal corrupted by noise is received by the receiver, that is

$$r_k = s_k + \xi_k \tag{3.9}$$

where s_k represents the sample sent by the sender, ξ_k is the noise sample and r_k denotes the received sample. The receiver then compute the Lyapunov exponent from the received signal. Figures 3.3 and 3.4 show two independent simulations. The approach is similar to the experiments in the previous section. The number of chaotic samples sent to represent a symbol is set to 1000. From the figures, we see that when E_b/N_0 is over 60 dB the correct Lyapunov exponents can be found and thus the two digital symbols of the CSK system can be readily distinguished. When the noise level is higher, the two digital symbols can still be distinguished, but the threshold for decision has to be changed. When the noise level is even higher, this method fails completely as it is impossible to identify points that are close together in the original orbit. In that case the $f'(x_i)$ evaluated for (3.6) is a essentially the difference of two Guassian random numbers. Therefore, the calculated Lyapunov exponent increases linearly with the noise power (in dB) in this range.

As we can see, the noise performance of this method is not good. Moreover, it requires a long signal length. Although it seems to be better than the fractal dimension approach, we conclude that the direct extrac-

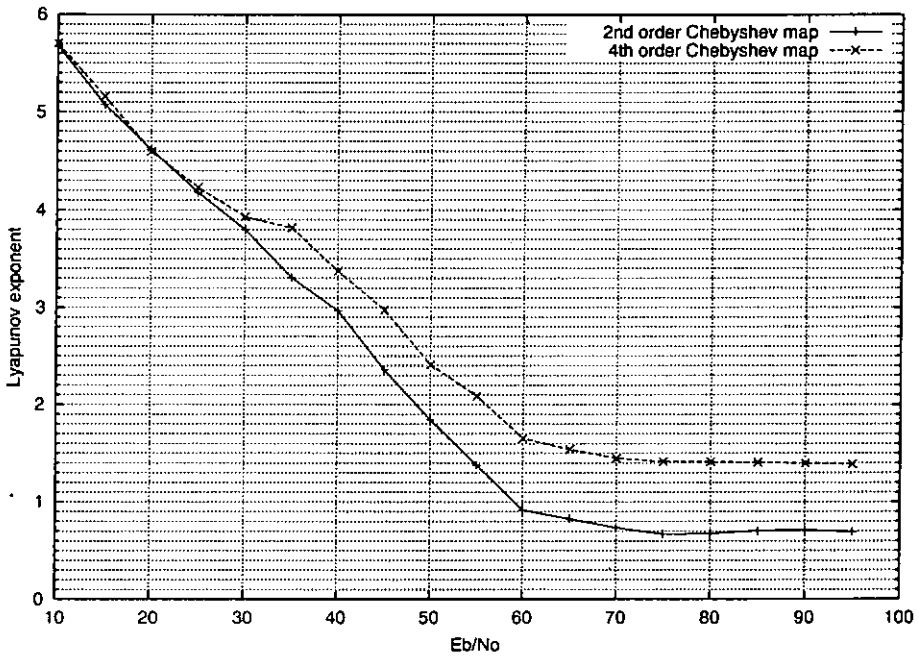

Figure 3.3: First trial of Lyapunov exponent extraction from orbits of different chaotic attractors in a noncoherent CSK system.

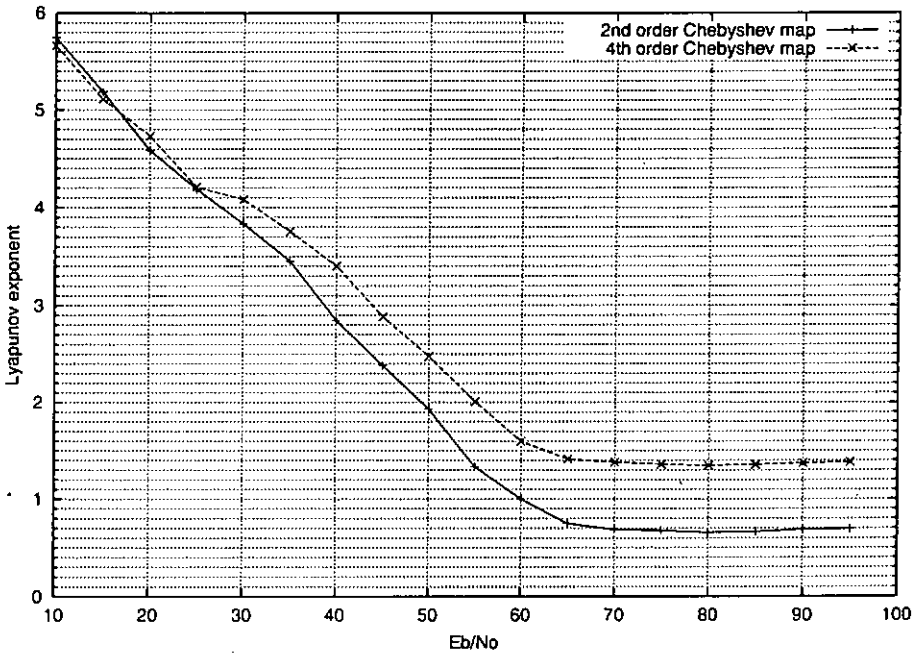

Figure 3.4: Second trial of Lyapunov exponent extraction from orbits of different chaotic attractors in a noncoherent CSK system.

tion of Lyapunov exponent from a signal, as a demodulation method in noncoherent CSK systems, is not practical.

While both the fractal dimension and the Lyapunov exponent methods do not perform well, the concept of extracting certain parameters from chaotic signals remains a possibility when we consider the detection methods of noncoherent CSK systems. In the rest of this thesis, we shift our focus to the possible improvements of some other existing chaos communication systems.

Chapter 4

A Multiple Access System Based on DCSK

4.1 DCSK System Model

In this chapter a multiple-access DCSK system using permutation techniques is presented [42]. The proposed permutation-based DCSK (P-DCSK) system is basically a DCSK system with an additional layer of signal transformation. The resulting DCSK system has enhanced security and provides multiple access capability.

Before going into the details of the P-DCSK system, the conventional DCSK model is introduced here, in terms of its discrete signals. In the DCSK system, each bit duration is divided into two equal time slots in which two sets of chaotic signal samples are sent respectively. The first

sample set is called the reference sample set while the second one, which carries the data, is called the data sample set. If a "+1" is transmitted, the data sample set is identical to the reference sample set, and if a "–1" is transmitted, an inverted version of the reference sample set is used as the data sample set.

Let 2β be the spreading factor, the number of chaotic samples sent for each binary symbol, where β is an integer. Denote the transmitted symbol by $\alpha \in \{-1, +1\}$. Within one bit duration, we denote the time by k, ranging from 1 to 2β. Then the output s_k of the DCSK transmitter is

$$s_k = \begin{cases} x_k & \text{for } k = 1, 2, \ldots, \beta \\ \alpha x_{k-\beta} & \text{for } k = \beta+1, \beta+2, \ldots, 2\beta \end{cases} \tag{4.1}$$

where $\{x_k\}$ are the chaotic samples. The transmitted signal passes through an additive white Gaussian noise channel and reaches the receiver. At time k, the received signal r_k is

$$r_k = s_k + \xi_k \tag{4.2}$$

where ξ_k denotes additive white Gaussian noise with zero mean and variance $N_0/2$. At the receiving end, the reference sample set and the corresponding data sample set are correlated. The output of the correlator is given by

$$y = \sum_{k=1}^{\beta} r_k r_{k+\beta}. \tag{4.3}$$

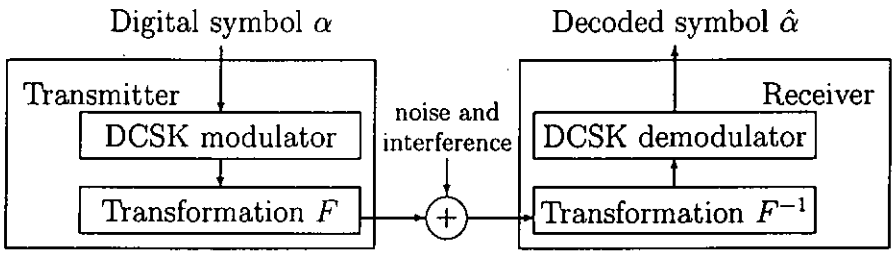

Figure 4.1: Block diagram of the P-DCSK system.

Depending on whether the output y is larger or smaller than zero, a "+1" or "−1" is decoded.

4.2 P-DCSK System Architecture

The structure of the P-DCSK communication system is shown in Figure 4:1. A layer of transformation F and its inverse are added to the transmitter and receiver, respectively. In the proposed system, the transformation is a simple permutation. For a multiple access system, each user uses a different permutation, which will be discussed later in this section.

Suppose there are N users using the same channel. Each user operates a P-DCSK system with an independent chaos generator and all users use the same spreading factor. Consider the signals within one symbol duration. For simpler notations we denote, for the ith user, the output signal of the DCSK modulator by

$$s^{(i)} = (s_1^{(i)} \quad s_2^{(i)} \quad \cdots \quad s_{2\beta}^{(i)}) \tag{4.4}$$

where $s_k^{(i)}$ equals $x_k^{(i)}$ or $\alpha^{(i)}x_{k-\beta}^{(i)}$ according to (4.1). Here $\alpha^{(i)}$ denotes the symbol transmitted by the ith user. The transformation F_i, a permutation, is then applied to the signal $\boldsymbol{s}^{(i)}$. The signal sent to the channel is

$$\begin{aligned} \boldsymbol{u}^{(i)} &= F_i(\boldsymbol{s}^{(i)}) \\ &= \boldsymbol{s}^{(i)}\boldsymbol{P}_{2\beta}^{(i)} \end{aligned} \tag{4.5}$$

where $\boldsymbol{P}_{2\beta}^{(i)}$ is a $2\beta \times 2\beta$ permutation matrix [43] used by the ith user. The overall signal block sent to the channel in this bit duration, denoted by $\boldsymbol{u}$, is the sum of the signals of all users, that is,

$$\boldsymbol{u} = \sum_{i=1}^{N} \boldsymbol{u}^{(i)} = \sum_{i=1}^{N} \boldsymbol{s}^{(i)}\boldsymbol{P}_{2\beta}^{(i)}. \tag{4.6}$$

All receivers in the system receive the same signal block, which is

$$\boldsymbol{v} = \boldsymbol{u} + (\boldsymbol{\Psi}_0 \;\; \boldsymbol{\Psi}_1) \tag{4.7}$$

where $\boldsymbol{\Psi}_0$ and $\boldsymbol{\Psi}_0$ are the noise vectors, defined as

$$\begin{aligned} \boldsymbol{\Psi}_0 &= (\xi_1 \;\; \xi_2 \;\; \cdots \;\; \xi_\beta) \\ \boldsymbol{\Psi}_1 &= (\xi_{\beta+1} \;\; \xi_{\beta+2} \;\; \cdots \;\; \xi_{2\beta}). \end{aligned} \tag{4.8}$$

At the jth receiver, the incoming block first undergoes an inverse transformation F_j^{-1} to retrieve an output block $\boldsymbol{r}^{(j)}$ where

$$\begin{aligned} \boldsymbol{r}^{(j)} &= F_j^{-1}(\boldsymbol{v}) \\ &= (\boldsymbol{u} + (\boldsymbol{\Psi}_0 \;\; \boldsymbol{\Psi}_1))(\boldsymbol{P}_{2\beta}^{(j)})^{-1} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{N} \boldsymbol{s}^{(i)} \boldsymbol{P}_{2\beta}^{(i)} (\boldsymbol{P}_{2\beta}^{(j)})^{-1} + (\boldsymbol{\Psi}_0 \;\; \boldsymbol{\Psi}_1)(\boldsymbol{P}_{2\beta}^{(j)})^{-1} \\
&= \boldsymbol{s}^{(j)} + \sum_{\substack{i=1 \\ i \neq j}}^{N} \boldsymbol{s}^{(i)} \boldsymbol{P}_{2\beta}^{(i,j)} + (\boldsymbol{\Psi}_0 \;\; \boldsymbol{\Psi}_1)(\boldsymbol{P}_{2\beta}^{(j)})^{-1} \qquad (4.9)
\end{aligned}
$$

where

$$
\boldsymbol{P}_{2\beta}^{(i,j)} = \boldsymbol{P}_{2\beta}^{(i)} (\boldsymbol{P}_{2\beta}^{(j)})^{-1}. \qquad (4.10)
$$

The matrix $\boldsymbol{P}_{2\beta}^{(i,j)}$, being the product of two permutation matrices, is also a permutation matrix. The output block $\boldsymbol{r}^{(j)}$ is then passed to a conventional DCSK demodulator for decoding. In the last line of (4.9), the first term $\boldsymbol{s}^{(j)}$ is the desired DCSK signal for User j, while all the other terms are either noise or interference generated by other users. While the expected effect of white noise is independent of any permutation applied on the noise samples, the co-channel interference can be minimized by the choice of permutations.

To ensure that the co-channel interference is kept to a low level, the $(\lambda + \beta)$th $(\lambda = 1, 2, \ldots, \beta)$ element in $\boldsymbol{s}^{(i)} \boldsymbol{P}_{2\beta}^{(i,j)}$ $(i \neq j)$ should not be equal to the λth element or its negation. To achieve this, we first define $\boldsymbol{R}_\beta$ as a random permutation matrix of size $\beta \times \beta$ and $\boldsymbol{A}_\beta$ as the "shifting"

matrix of size $\beta \times \beta$ where

$$\boldsymbol{A}_\beta = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \ddots & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}. \tag{4.11}$$

Note that the consequence of multiplying $\boldsymbol{A}_\beta$ to an array $(x_1 \ x_2 \ \ldots \ x_\beta)$ is equivalent to shifting the elements in the array to the right by one place with the overflown element being re-inserted from the left. In other words,

$$(x_1 \ x_2 \ \ldots \ x_\beta)\boldsymbol{A}_\beta = (x_\beta \ x_1 \ x_2 \ \ldots \ x_{\beta-1}). \tag{4.12}$$

Next we define

$$\boldsymbol{Q}_\beta^{(i)} = \boldsymbol{R}_\beta \boldsymbol{A}_\beta^i \tag{4.13}$$

and the permutation matrix for User i can be chosen as

$$\begin{aligned} \boldsymbol{P}_{2\beta}^{(i)} &= \begin{pmatrix} \boldsymbol{I}_\beta & \boldsymbol{0}_\beta \\ \boldsymbol{0}_\beta & \boldsymbol{Q}_\beta^{(i)} \end{pmatrix} \\ &= \begin{pmatrix} \boldsymbol{I}_\beta & \boldsymbol{0}_\beta \\ \boldsymbol{0}_\beta & \boldsymbol{R}_\beta \boldsymbol{A}_\beta^i \end{pmatrix} \end{aligned} \tag{4.14}$$

where $\boldsymbol{I}_\beta$ and $\boldsymbol{0}_\beta$ are the identity matrix and zero matrix, respectively, of size $\beta \times \beta$. The permutation matrix $\boldsymbol{P}_{2\beta}^{(i,j)}$ in (4.10) can now be re-written

as

$$\boldsymbol{P}_{2\beta}^{(i,j)} = \begin{pmatrix} \boldsymbol{I}_\beta & \boldsymbol{0}_\beta \\ \boldsymbol{0}_\beta & \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{i-j} \boldsymbol{R}_\beta^{-1} \end{pmatrix}. \tag{4.15}$$

It can be readily shown that the diagonal elements of $\boldsymbol{R}_\beta \boldsymbol{A}_\beta^{i-j} \boldsymbol{R}_\beta^{-1}$ are all zeros when $i \neq j$. Thus, the non-zero elements in the λth ($\lambda = 1, 2, \ldots, \beta$) and $(\lambda + \beta)$th rows in $\boldsymbol{P}_{2\beta}^{(i,j)}$ will not differ by β columns, and a low co-channel interference is achieved.

4.3 Security in Frequency Spectrum

In this section, we try to analyse the frequency spectra of a 10-bit signal sample for both the DCSK and the P-DCSK systems. Figure 4.2 plots the magnitude of the spectrum of DCSK signal. It can be seen that no useful information can be retrieved. Next, we square the DCSK signal sample and plot the magnitude spectrum again. From Figure 4.3, it can be observed that the spectral value goes to zero at odd multiple frequencies of the bit rate. When the DCSK signal sample is squared, the resultant signals in the information-bearing slots become identical to their corresponding reference slots. Thus, no frequency component at odd multiples of the bit rate exists. This phenomenon is not desirable because any unintended receiver can retrieve the bit rate of the system.

The frequency spectra of the P-DCSK signal sample and the square

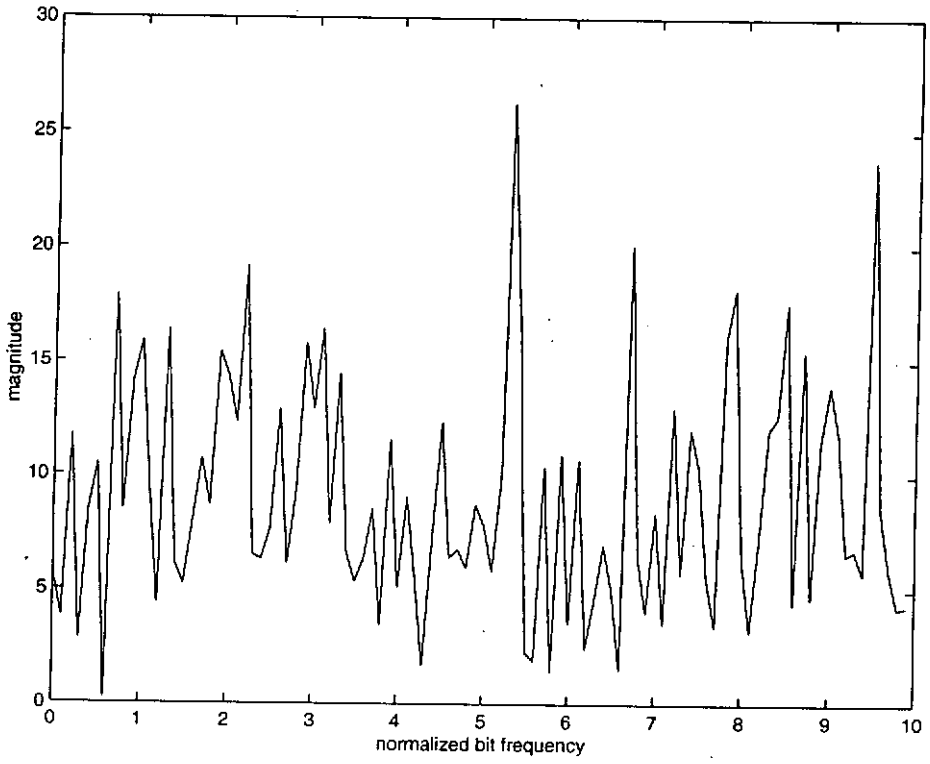

Figure 4.2: Magnitude of frequency components versus normalized bit frequency for a conventional DCSK signal sample.

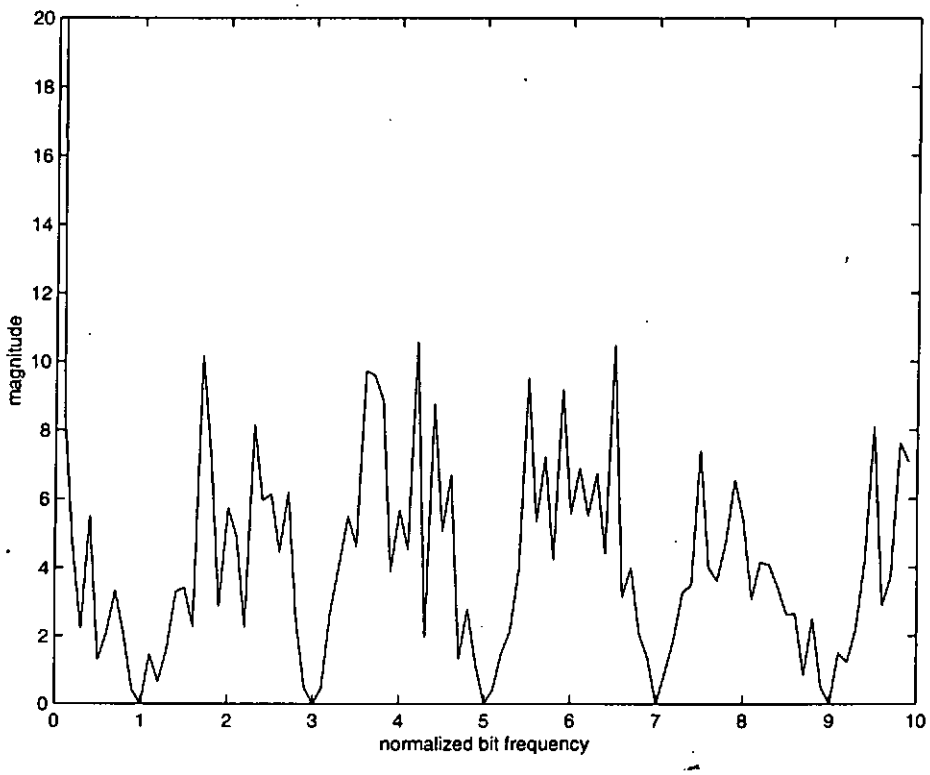

Figure 4.3: Magnitude of frequency components versus normalized bit frequency for the square of a conventional DCSK signal sample.

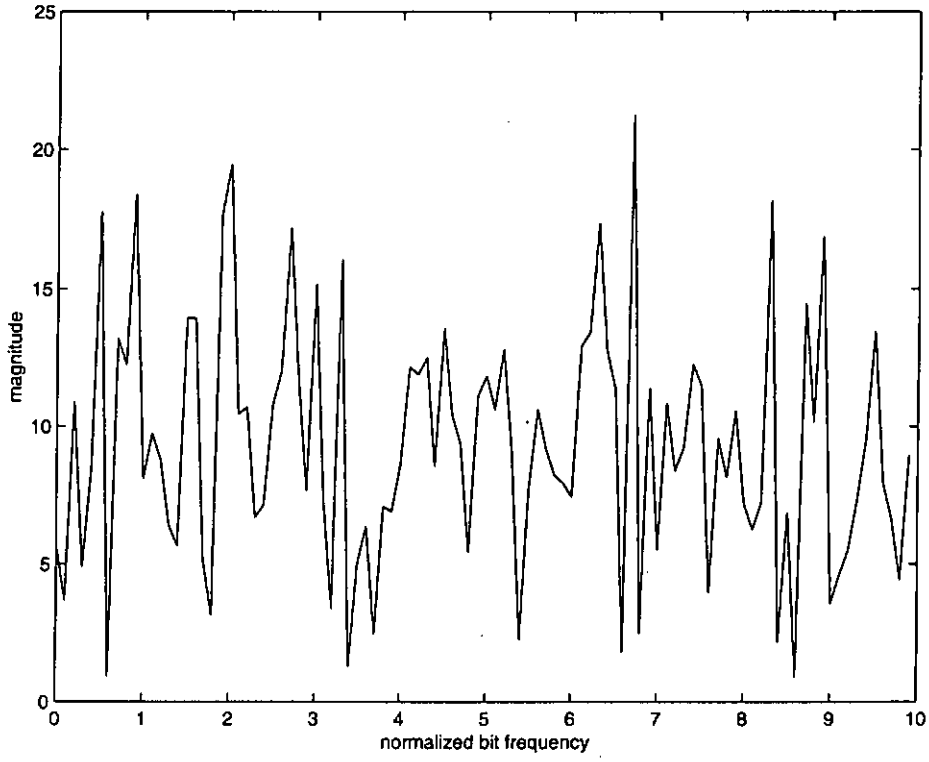

Figure 4.4: Magnitude of frequency components versus normalized bit frequency for a permutation-based DCSK signal sample.

of the sample are plotted in Figure 4.4 and Figure 4.5, respectively. It can be seen that in both cases no bit rate information can be retrieved from the spectrum.

For the intended receiver, with complete knowledge of the permutation matrix, demodulation can be accomplished easily as in DCSK systems. Hence we conclude that, when the DCSK system is replaced by the P-DCSK system, data security is enhanced, while the system performance is not affected.

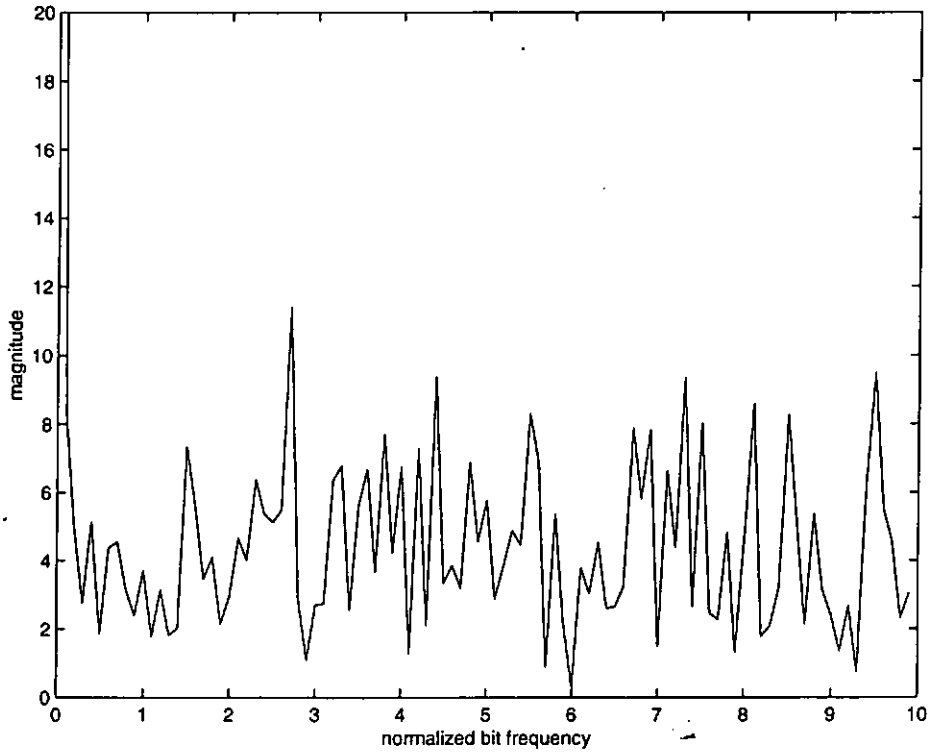

Figure 4.5: Magnitude of frequency components versus normalized bit frequency for the square of a permutation-based DCSK signal sample.

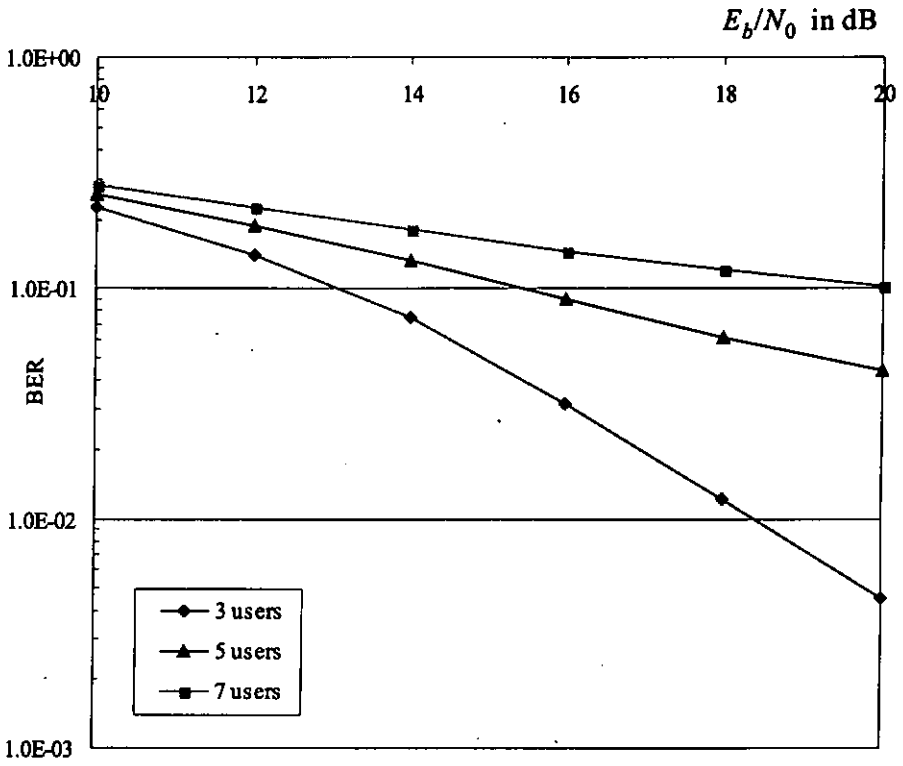

Figure 4.6: Simulated BERs versus E_b/N_0 for the P-DCSK system. Spreading factor $2\beta = 200$. Number of users $N = 3$, 5 and 7.

4.4 System Performance

In this section, the performance of the proposed permutation-based multiple-access DCSK digital communication system is studied by computer simulations. We assume that the map $T_3(x)$ in (1.3), also called the cubic map, is used by all users to generate the chaotic sequences, each with a different initial condition. The system performance of the P-DCSK system is illustrated in Figure 4.6 and Figure 4.7.

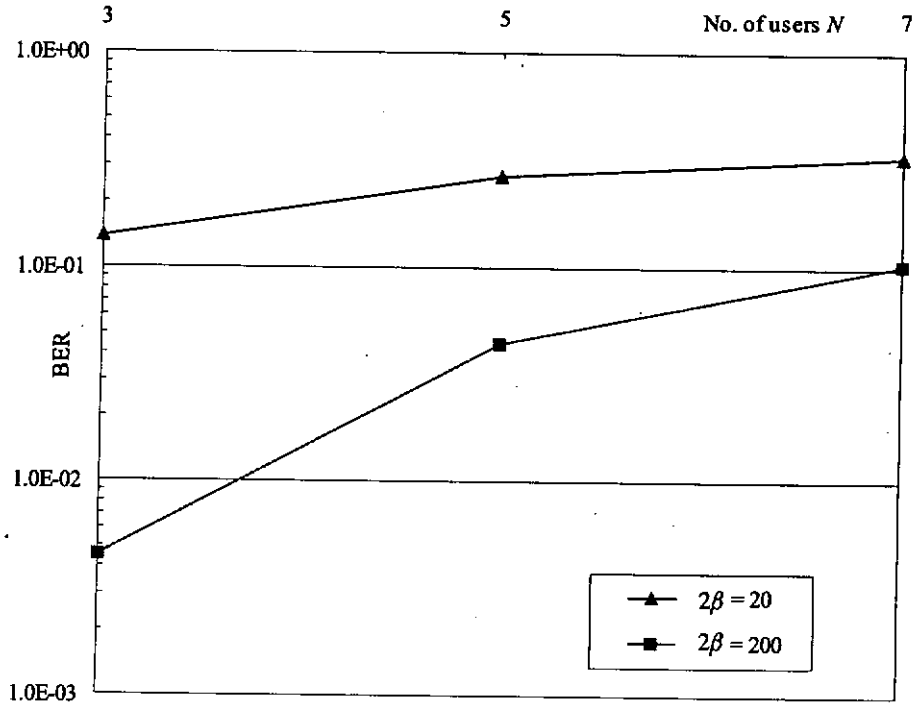

Figure 4.7: Simulated BERs versus number of users N for the P-DCSK system. $E_b/N_0 = 20$ dB. Spreading factor $2\beta = 20$ and 200.

4.5 Derivation of Bit Error Rate with Gaussian Approximation

In this section, we derive the analytical bit error rate of the proposed permutation-based multiple-access DCSK system. First of all, it can be shown that the inverse of a permutation matrix is equal to its transpose. Let us consider, for one bit duration, the received signal block of the jth user. When this block undergoes the inverse transformation, the output block is obtained by expanding (4.9), i.e.,

$$\begin{aligned} \boldsymbol{r}^{(j)} &= (\boldsymbol{x}^{(j)} \quad \alpha^{(j)}\boldsymbol{x}^{(j)}) \\ &+ \left(\sum_{\substack{i=1 \\ i\neq j}}^{N} \boldsymbol{x}^{(i)} \quad \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)}\boldsymbol{x}^{(i)}\boldsymbol{R}_\beta \boldsymbol{A}_\beta^{i-j}\boldsymbol{R}_\beta^T\right) \\ &+ (\boldsymbol{\Psi}_0 \quad \boldsymbol{\Psi}_1\boldsymbol{A}_\beta^{-j}\boldsymbol{R}_\beta^T). \end{aligned} \tag{4.16}$$

When $\boldsymbol{r}^{(j)}$ is sent to the conventional DCSK demodulator of the jth user, the output of the correlator at the end of the bit duration, denoted by $y^{(j)}$, can be computed by correlating the first half, the reference part, and the second half, the data part, of the incoming signal. So $y^{(j)}$, the input to the threshold detector at the end of this symbol duration, is given by

$$\begin{aligned} y^{(j)} &= \alpha^{(j)}\boldsymbol{x}^{(j)}(\boldsymbol{x}^{(j)})^T + \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)}\boldsymbol{x}^{(j)}\boldsymbol{R}_\beta\boldsymbol{A}_\beta^{j-i}\boldsymbol{R}_\beta^T(\boldsymbol{x}^{(i)})^T \\ &+ \alpha^{(j)}\sum_{\substack{i=1 \\ i\neq j}}^{N} \boldsymbol{x}^{(i)}(\boldsymbol{x}^{(j)})^T + \sum_{\substack{n=1 \\ n\neq j}}^{N}\sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)}\boldsymbol{x}^{(n)}\boldsymbol{R}_\beta\boldsymbol{A}_\beta^{j-i}\boldsymbol{R}_\beta^T(\boldsymbol{x}^{(i)})^T \\ &+ \sum_{i=1}^{N} \boldsymbol{x}^{(i)}\boldsymbol{R}_\beta\boldsymbol{A}_\beta^{j}\boldsymbol{\Psi}_1^T + \sum_{i=1}^{N} \alpha^{(i)}\boldsymbol{\Psi}_0\boldsymbol{R}_\beta\boldsymbol{A}_\beta^{j-i}\boldsymbol{R}_\beta^T(\boldsymbol{x}^{(i)})^T \end{aligned}$$

$$
\begin{aligned}
&+ \ \boldsymbol{\Psi}_0 \boldsymbol{R}_\beta \boldsymbol{A}_\beta^j \boldsymbol{\Psi}_1^T \\
= \ & \alpha^{(j)} \boldsymbol{x}^{(j)} (\boldsymbol{x}^{(j)})^T + \sum_{\substack{i=1 \\ i \neq j}}^{N} \alpha^{(i)} \boldsymbol{x}^{(j)} (\boldsymbol{z}^{(i,j)})^T \\
&+ \alpha^{(j)} \sum_{\substack{i=1 \\ i \neq j}}^{N} \boldsymbol{x}^{(i)} (\boldsymbol{x}^{(j)})^T + \sum_{\substack{n=1 \\ n \neq j}}^{N} \sum_{\substack{i=1 \\ i \neq j}}^{N} \alpha^{(i)} \boldsymbol{x}^{(n)} (\boldsymbol{z}^{(i,j)})^T \\
&+ \sum_{i=1}^{N} \boldsymbol{x}^{(i)} (\boldsymbol{\Phi}^{(j)})^T + \sum_{i=1}^{N} \alpha^{(i)} \boldsymbol{\Psi}_0 (\boldsymbol{z}^{(i,j)})^T \\
&+ \boldsymbol{\Psi}_0 (\boldsymbol{\Phi}^{(j)})^T
\end{aligned} \tag{4.17}
$$

where

$$
\boldsymbol{z}^{(i,j)} = (z_1^{(i,j)} \ z_2^{(i,j)} \ \cdots \ z_\beta^{(i,j)}) = \boldsymbol{x}^{(i)} \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{i-j} \boldsymbol{R}_\beta^T \tag{4.18}
$$

$$
\boldsymbol{\Phi}^{(j)} = (\phi_1^{(j)} \ \phi_2^{(j)} \ \cdots \ \phi_\beta^{(j)}) = \boldsymbol{\Psi}_1 \boldsymbol{A}_\beta^{-j} \boldsymbol{R}_\beta^T. \tag{4.19}
$$

Note that the elements in $\boldsymbol{z}^{(i,j)}$ and $\boldsymbol{\Phi}^{(j)}$ are permutations of the elements in $\boldsymbol{x}^{(i)}$ and $\boldsymbol{\Psi}_1$, respectively.

Without loss of generality, from here we suppose "+1" is transmitted for User j, i.e., $\alpha^{(j)} = +1$. Then, (4.17) becomes

$$
\begin{aligned}
y^{(j)} = \ & \underbrace{U^{(j,j)}}_{\text{required signal}} \\
& \underbrace{+ \sum_{\substack{i=1 \\ i \neq j}}^{N} \alpha^{(i)} V^{(j,i,j)} + \sum_{\substack{i=1 \\ i \neq j}}^{N} U^{(i,j)} + \sum_{\substack{n=1 \\ n \neq j}}^{N} \sum_{\substack{i=1 \\ i \neq j}}^{N} \alpha^{(i)} V^{(n,i,j)}}_{\text{co-channel interference}} \\
& \underbrace{+ \sum_{i=1}^{N} W^{(i,j)} + X^{(j,j)} + \sum_{\substack{i=1 \\ i \neq j}}^{N} \alpha^{(i)} X^{(i,j)} + Y^{(j)}}_{\text{noise}}
\end{aligned} \tag{4.20}
$$

where

$$
U^{(i,j)} = \boldsymbol{x}^{(i)} (\boldsymbol{x}^{(j)})^T = \sum_{k=1}^{\beta} x_k^{(i)} x_k^{(j)} \tag{4.21}
$$

$$V^{(n,i,j)} = \boldsymbol{x}^{(n)}(\boldsymbol{z}^{(i,j)})^T = \sum_{k=1}^{\beta} x_k^{(n)} z_k^{(i,j)} \tag{4.22}$$

$$W^{(i,j)} = \boldsymbol{x}^{(i)}(\boldsymbol{\Phi}^{(j)})^T = \sum_{k=1}^{\beta} x_k^{(i)} \phi_k^{(j)} \tag{4.23}$$

$$X^{(i,j)} = \boldsymbol{\Psi}_0(\boldsymbol{z}^{(i,j)})^T = \sum_{k=1}^{\beta} \xi_k z_k^{(i,j)} \tag{4.24}$$

$$Y^{(j)} = \boldsymbol{\Psi}_0(\boldsymbol{\Phi}^{(j)})^T = \sum_{k=1}^{\beta} \xi_k \phi_k^{(j)}. \tag{4.25}$$

Notice that the input to the detector consists of three components, namely required signal, co-channel interference and noise. The mean value of $y^{(j)}$ is given by

$$\begin{aligned}
\mathrm{E}[y^{(j)}] &= \mathrm{E}[U^{(j,j)}] + \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} \mathrm{E}[V^{(j,i,j)}] + \sum_{\substack{i=1 \\ i\neq j}}^{N} \mathrm{E}[U^{(i,j)}] \\
&\quad + \sum_{\substack{n=1 \\ n\neq j}}^{N} \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} \mathrm{E}[V^{(n,i,j)}] + \sum_{i=1}^{N} \mathrm{E}[W^{(i,j)}] + \mathrm{E}[X^{(j,j)}] \\
&\quad + \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} \mathrm{E}[X^{(i,j)}] + \mathrm{E}[Y^{(j)}] \\
&= \mathrm{E}[U^{(j,j)}] + \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} \mathrm{E}[V^{(j,i,j)}] \\
&\quad + \sum_{\substack{i=1 \\ i\neq j}}^{N} \mathrm{E}[U^{(i,j)}] + \sum_{\substack{n=1 \\ n\neq j}}^{N} \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} \mathrm{E}[V^{(n,i,j)}]
\end{aligned} \tag{4.26}$$

where $\mathrm{E}[\psi]$ denotes the mean value of ψ. The last equality holds because $\mathrm{E}[\xi_k]$ and $\mathrm{E}[\phi_k^{(j)}]$ are both zero. The variance of $y^{(j)}$ is found from [44]

$$\begin{aligned}
\mathrm{var}[y^{(j)}] &= \sum_{i=1}^{N} \mathrm{var}[U^{(i,j)}] + \sum_{n=1}^{N} \sum_{\substack{i=1 \\ i\neq j}}^{N} \mathrm{var}[V^{(n,i,j)}] + \sum_{i=1}^{N} \mathrm{var}[W^{(i,j)}] \\
&\quad + \sum_{i=1}^{N} \mathrm{var}[X^{(i,j)}] + \mathrm{var}[Y^{(j)}] \\
&\quad + \sum_{\substack{C \\ C\neq D}} \sum_{D} \mathrm{cov}[C, D]
\end{aligned} \tag{4.27}$$

where $C, D \in \{U^{(i,j)}\ (i = 1,\ldots,N);\ \alpha^{(i)}V^{(n,i,j)}\ (n = 1,\ldots,N; i = 1,\ldots,j-1,j+1,\ldots,N);\ W^{(i,j)}\ (i = 1,\ldots,N);\ X^{(j,j)};\ \alpha^{(i)}X^{(i,j)}\ (i = 1,\ldots,j-1,j+1,\ldots,N); Y^{(j)}\}$, $\mathrm{var}[\psi]$ denotes the variance of ψ, and $\mathrm{cov}[C, D]$ represents the covariance of C and D defined as

$$\mathrm{cov}[C, D] = \mathrm{E}[CD] - \mathrm{E}[C]\mathrm{E}[D]. \tag{4.28}$$

As discussed before, we assume that all users use the cubic map

$$x_{k+1} = g(x_k) = 4x_k^3 - 3x_k \tag{4.29}$$

to generate the chaotic sequences, each with a different initial condition. With this map, we obtain

$$\mathrm{E}[x_k] = 0 \tag{4.30}$$

$$\mathrm{E}[x_k^2] = 0.5 \tag{4.31}$$

$$\mathrm{var}[x_k^2] = 0.125 \tag{4.32}$$

according to the probability density function of cubic map orbits, as stated earlier in (2.1). Also, it can be readily shown that

$$\mathrm{E}[U^{(i,j)}] = \begin{cases} \beta\mathrm{E}[x_k^2] & \text{if } i = j \\ 0 & \text{otherwise} \end{cases} \tag{4.33}$$

$$\mathrm{E}[V^{(n,i,j)}] = 0. \tag{4.34}$$

Furthermore, the variances of the terms in (4.21) to (4.25) are given by

$$\mathrm{var}[U^{(i,j)}] = \begin{cases} \beta\mathrm{var}[x_k^2] & \text{if } i = j \\ \beta\mathrm{E}^2[x_k^2] & \text{otherwise} \end{cases} \tag{4.35}$$

$$\text{var}[V^{(n,i,j)}] = \begin{cases} \beta \mathrm{E}^2[x_k^2] & \text{for } i \neq j, i \neq n \\ \frac{\beta^2}{\beta-1}\mathrm{E}^2[x_k^2] \approx \beta \mathrm{E}^2[x_k^2] & \text{for } i \neq j, i = n \end{cases} \quad (4.36)$$

$$\text{var}[W^{(i,j)}] = \beta N_0 \mathrm{E}[x_k^2]/2 \quad (4.37)$$

$$\text{var}[X^{(i,j)}] = \beta N_0 \mathrm{E}[x_k^2]/2 \quad (4.38)$$

$$\text{var}[Y^{(j)}] = \beta N_0^2/4 \quad (4.39)$$

and the covariance terms in (4.27) can be shown to be zero. Thus, (4.26) and (4.27) can be simplified to

$$\mathrm{E}[y^{(j)}] = \beta \mathrm{E}[x_k^2] \quad (4.40)$$

$$\begin{aligned} \text{var}[y^{(j)}] &\approx \beta \text{var}[x_k^2] + (N-1)\beta \mathrm{E}^2[x_k^2] + (N^2 - N)\beta \mathrm{E}^2[x_k^2] \\ &\quad + N\beta N_0 \mathrm{E}[x_k^2]/2 + N\beta N_0 \mathrm{E}[x_k^2]/2 + \beta N_0^2/4 \\ &= \beta \text{var}[x_k^2] + (N^2-1)\beta \mathrm{E}^2[x_k^2] \\ &\quad + N\beta N_0 \mathrm{E}[x_k^2] + \beta N_0^2/4. \end{aligned} \quad (4.41)$$

Since $y^{(j)}$ is the sum of a large number of random variables, we may assume that it is approximately normal [1]. This assumption holds better for larger spreading factors. In the detection of the symbol, an error occurs if $y^{(j)} \leq 0$ when $\alpha^{(j)} = +1$ or $y^{(j)} > 0$ when $\alpha^{(j)} = -1$. As it can be shown that

$$\text{Prob}(y^{(j)} \leq 0 | (\alpha^{(j)} = +1)) = \text{Prob}(y^{(j)} > 0 | (\alpha^{(j)} = -1)), \quad (4.42)$$

[1]The actual probability distributions of these random variables are discussed in [45].

the bit error rate (BER) for User j can be computed from

$$\begin{aligned} \mathrm{BER}^{(j)} &= \mathrm{Prob}(y^{(j)} \leq 0 | (\alpha^{(j)} = +1)) \\ &= \frac{1}{2}\mathrm{erfc}\left(\frac{\mathrm{E}[y^{(j)}|(\alpha^{(j)} = +1)]}{\sqrt{2\mathrm{var}[y^{(j)}|(\alpha^{(j)} = +1)]}}\right) \end{aligned} \tag{4.43}$$

where the complementary error function [8], $\mathrm{erfc}(\psi)$, is defined as

$$\mathrm{erfc}(\psi) = \frac{2}{\sqrt{\pi}} \int_{\psi}^{\infty} e^{-\lambda^2} d\lambda. \tag{4.44}$$

Next we expand

$$\begin{aligned} & \frac{\mathrm{E}[y^{(j)}|(\alpha^{(j)} = +1)]}{\sqrt{2\mathrm{var}[y^{(j)}|(\alpha^{(j)} = +1)]}} \\ = & \frac{\beta \mathrm{E}[x_k^2]}{\sqrt{2(\beta \mathrm{var}[x_k^2] + (N^2-1)\beta \mathrm{E}^2[x_k^2] + N\beta N_0 \mathrm{E}[x_k^2] + \beta N_0^2/4)}} \\ = & \left[\frac{2\Omega}{\beta} + \frac{2(N^2-1)}{\beta} + 4N\left(\frac{E_b}{N_0}\right)^{-1} + 2\beta\left(\frac{E_b}{N_0}\right)^{-2}\right]^{-\frac{1}{2}} \end{aligned} \tag{4.45}$$

where E_b represents the average bit energy and Ω is a constant for the given chaotic sequence. They are given by

$$E_b = 2\beta \mathrm{E}[x_k^2] \tag{4.46}$$

$$\Omega = \frac{\mathrm{var}[x_k^2]}{\mathrm{E}^2[x_k^2]}. \tag{4.47}$$

Note that Ω is constant for a given chaotic sequence, regardless of the presence of any scaling factor of the sequence. This can be illustrated as follows. Suppose the chaotic sequence $\{x_k\}$ is multiplied by the factor ν before transmission and the average power of the signal is changed by ν^2 times, the value of Ω remains unchanged, i.e.,

$$\Omega = \frac{\mathrm{var}[(\nu x_k)^2]}{\mathrm{E}^2[(\nu x_k)^2]} = \frac{\mathrm{var}[\nu^2 x_k^2]}{\mathrm{E}^2[\nu^2 x_k^2]} = \frac{\nu^4 \mathrm{var}[x_k^2]}{\nu^4 \mathrm{E}^2[x_k^2]} = \frac{\mathrm{var}[x_k^2]}{\mathrm{E}^2[x_k^2]}. \tag{4.48}$$

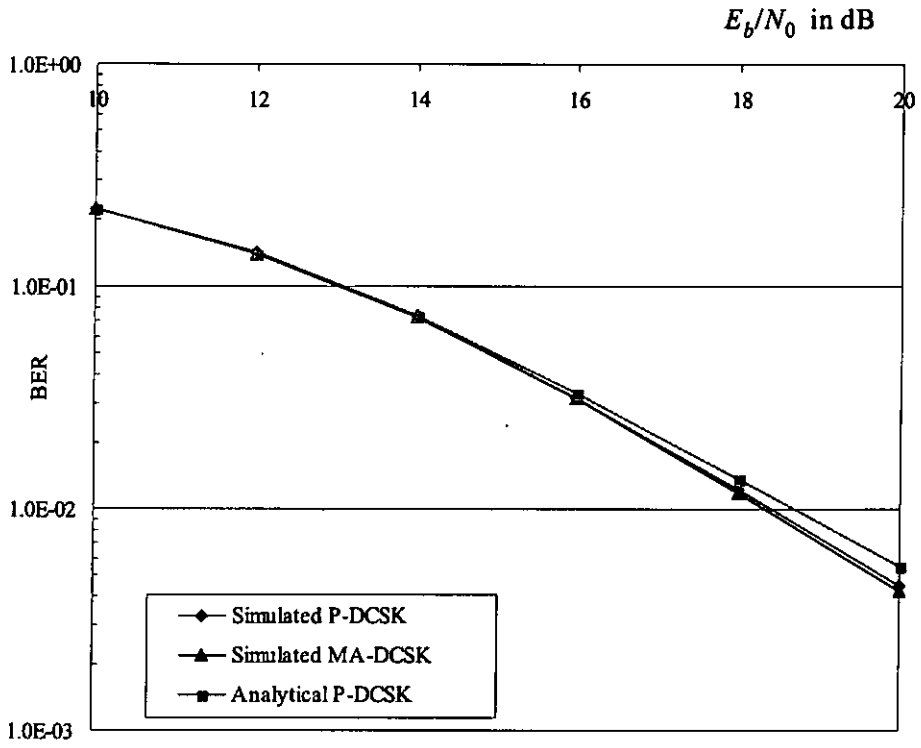

Figure 4.8: Simulated and analytical BERs of multiple access DCSK systems. Spreading factor $2\beta = 200$ and $N = 3$.

Finally, by putting (4.45) into (4.43), we obtain the analytical BER for the P-DCSK system. This analytical BER is an approximation obtained by modeling the random variables as Gaussian, and the results is acceptable only when the spreading factor of system is large enough. Figure 4.8 shows that, when the spreading factor is 200, the analytical BER agrees well with the simulation results. Also, in the simulations it is observed that the P-DCSK system achieves similar performance to the MA-DCSK system of [37].

Chapter 5

An M-ary Chaos-Based Communication System

5.1 Introduction

In this chapter an M-ary chaos-based communication system is proposed. To better utilize the large bandwidth occupied by the wideband chaotic signals, we transmit M-ary symbols instead of binary ones. The ordinary approach is to install M chaos generators at the transmitter to generate signals representing the M symbols. According to whether these chaotic signals can be reproduced at the receiver, coherent and noncoherent detections can be employed to decode the received signal. The main drawback of such an M-ary system is that the number of chaos generators increases with the symbol number M, which in turn increases

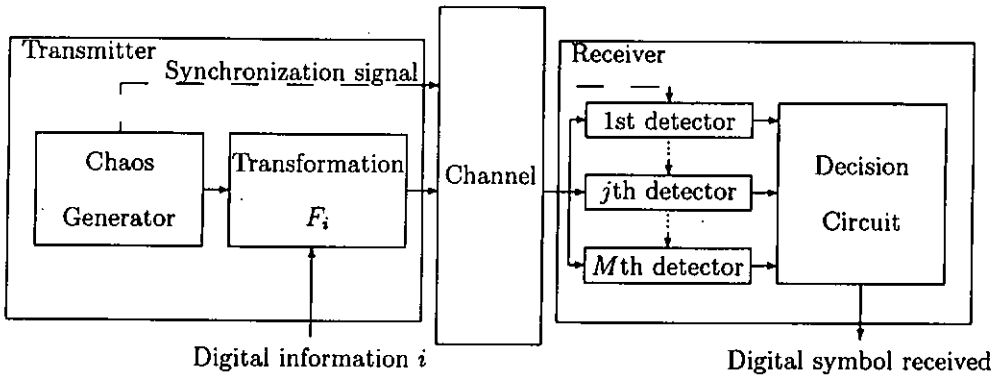

Figure 5.1: Block diagram of the coherent M-ary chaos-based communication system.

the complexity of the modulator and demodulator.

In this chapter, an M-ary transmission scheme which employs only one chaos generator is presented. In the scheme each block of chaotic samples undergoes a transformation process before it is transmitted. The transformation used for each symbol is different, thus allowing the symbol to be distinguished in the receiver which uses the appropriate inverse transformations for decoding the symbols. In our study, the set of transformations used are based on simple permutations similar to the ones described in the previous chapter. In the next two sections, a coherent scheme and a noncoherent scheme will be discussed respectively.

5.2 Description of the Coherent System

Figure 5.1 shows the block diagram of the coherent M-ary chaos communication system. On the transmitting side, each signal block produced by

the chaos generator undergoes a certain reversible transformation. Each symbol corresponds to a different transformation. Based on the incoming block, the receiver attempts to determine the most probable transformation that has been used in the transmitter and then decodes the symbol. A synchronization signal, shown as the dashed line in the diagram, is normally required for coherent detection.

Assume that the chaotic signal generated at the transmitter can be reproduced exactly at the receiver. Let the integer β be the spreading factor, defined as the number of chaotic samples sent for each M-ary symbol. Now let the chaos generator output be denoted by x_k at time k. During the first symbol duration, i.e., for time $k = 1, 2, \ldots, \beta$, the output block from the generator, denoted by $\boldsymbol{x}$, is given by

$$\boldsymbol{x} = (x_1 \;\; x_2 \;\; \cdots \;\; x_\beta). \tag{5.1}$$

This block will undergo a transformation before it is transmitted. The transformation is a permutation similar to those described in the previous chapter. For instance, to send the digital symbol $i \in \{1, 2, \cdots, M\}$, the block of chaotic samples first undergoes a transformation F_i, which gives a transformed block $\boldsymbol{u}$, i.e.,

$$\begin{aligned} \boldsymbol{u} &= F_i(\boldsymbol{x}) \\ &= \boldsymbol{x}\boldsymbol{Q}_\beta^{(i)} \end{aligned} \tag{5.2}$$

where $\boldsymbol{Q}_\beta^{(i)}$ is a permutation matrix as defined earlier in (4.13). The

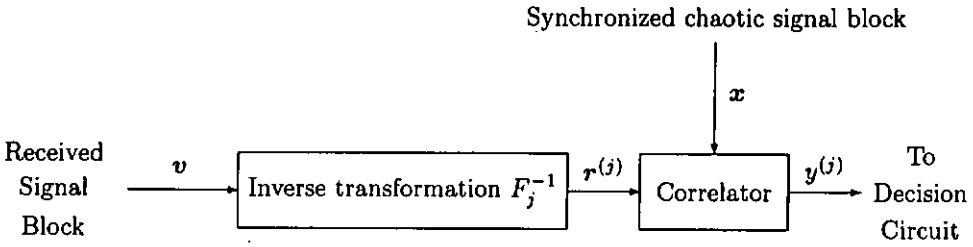

Figure 5.2: Block diagram of the jth detector in the coherent M-ary chaos-based communication system.

permutation performed ensures that the signals produced for different symbols have low correlations. Assuming an AWGN channel, the signal block collected by the receiver is

$$\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{\Psi}_0 \tag{5.3}$$

where $\boldsymbol{\Psi}_0$ is a sample noise vector as defined in (4.8). The job of the receiver now is to determine the received symbol from the received block $\boldsymbol{v}$. As shown in Figure 5.1, the received block $\boldsymbol{v}$ is sent to M detectors in parallel. Based on the detectors' outputs, the decision circuit determines the received symbol. Figure 5.2 shows the block diagram of the jth detector, which consists of an inverse transformation process and a correlator. The output of the inverse transformation is

$$\boldsymbol{r}^{(j)} = F_j^{-1}(\boldsymbol{v})$$

$$
\begin{aligned}
&= \boldsymbol{v}(\boldsymbol{Q}_\beta^{(j)})^{-1} \\
&= \boldsymbol{x}\boldsymbol{Q}_\beta^{(i)}(\boldsymbol{Q}_\beta^{(j)})^{-1} + \boldsymbol{\Psi}_0(\boldsymbol{Q}_\beta^{(j)})^{-1}. \qquad (5.4)
\end{aligned}
$$

The second part of the detector then calculates the correlation between $\boldsymbol{r}^{(j)}$ and $\boldsymbol{x}$. Denoting the transpose of $\boldsymbol{x}$ by $\boldsymbol{x}^T$, the output of the jth detector, $y^{(j)}$, is given by

$$
\begin{aligned}
y^{(j)} &= \boldsymbol{r}^{(j)}\boldsymbol{x}^T \\
&= \boldsymbol{x}\boldsymbol{Q}_\beta^{(i)}(\boldsymbol{Q}_\beta^{(j)})^{-1}\boldsymbol{x}^T + \boldsymbol{\Psi}_0(\boldsymbol{Q}_\beta^{(j)})^{-1}\boldsymbol{x}^T \\
&= \begin{cases} \boldsymbol{x}\boldsymbol{x}^T + \boldsymbol{\Psi}_0(\boldsymbol{Q}_\beta^{(j)})^{-1}\boldsymbol{x}^T & \text{when } j = i \\ \boldsymbol{x}\boldsymbol{Q}_\beta^{(i,j)}\boldsymbol{x}^T + \boldsymbol{\Psi}_0(\boldsymbol{Q}_\beta^{(j)})^{-1}\boldsymbol{x}^T & \text{when } j \neq i \end{cases} \qquad (5.5)
\end{aligned}
$$

where $\boldsymbol{Q}_\beta^{(i,j)} = \boldsymbol{Q}_\beta^{(i)}(\boldsymbol{Q}_\beta^{(j)})^{-1}$. As discussed in the last chapter, the construction of $\boldsymbol{Q}_\beta^{(i,j)}$ ensures low correlation between $\boldsymbol{x}\boldsymbol{Q}_\beta^{(i,j)}$ and $\boldsymbol{x}$, given that the elements of $\boldsymbol{x}$ can be assumed uncorrelated. Thus the correlator output $y^{(j)}$ in (5.5) for the case $j = i$ should be the largest and the symbol received can be decoded accordingly by the decision circuit.

5.3 Description of the Noncoherent System

Chaos synchronization is difficult to achieve when the channel has poor propagation condition. In such a case, a noncoherent scheme is preferred. The working principle of the noncoherent version of the M-ary

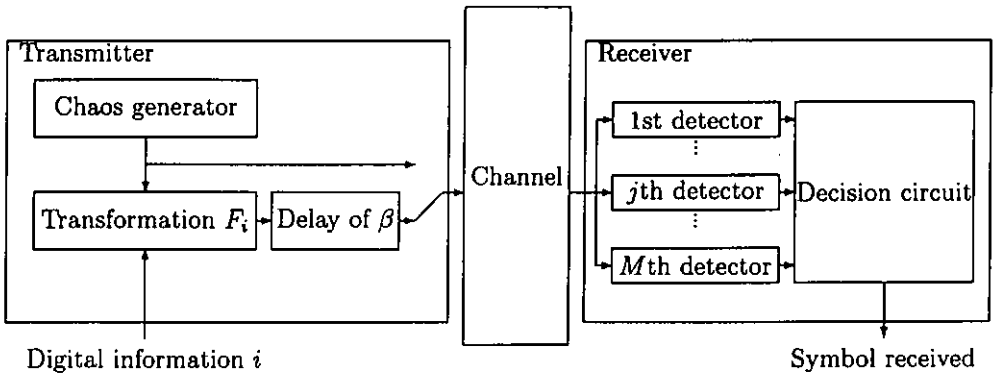

Figure 5.3: Block diagram of the noncoherent M-ary chaos-based communication system.

chaos communication system is similar to that used in the noncoherent DCSK system, in which the reference signal and the information-bearing signal are sent consecutively during a symbol duration. In our M-ary system, the reference signal block is a set of chaotic samples, while the information-bearing block is a permutation of the chaotic samples in the reference signal. Permutations are performed in exactly the same way as that of the coherent system described in the previous section. The decoding process is also the same, except that the reference block is used instead of the synchronized chaotic signal in the correlators.

For convenience, we denote the spreading factor by 2β in the noncoherent system. The block diagram of the noncoherent system is depicted in Figure 5.3. Using the same notations as in the previous section, the chaos generator generates a block of chaotic samples $\boldsymbol{x}$, which is used

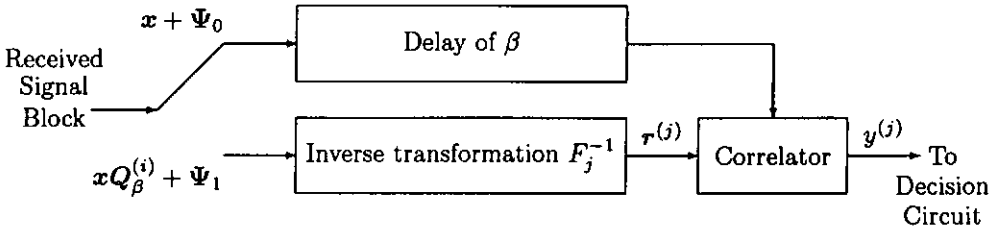

Figure 5.4: Block diagram of the jth detector in the noncoherent M-ary chaos-based communication system.

as the reference here. The sender then generates an information-bearing block by applying a transformation to the reference block according to the symbol being transmitted. Both the reference and the information-bearing blocks are sent to the channel, each occupying half of the symbol duration. Now suppose we are transmitting symbol i. The whole signal block sent to the channel during one symbol duration, denoted by $\boldsymbol{s}$, is given by

$$\begin{aligned} \boldsymbol{s} &= (\boldsymbol{x} \;\; F_i(\boldsymbol{x})) \\ &= (\boldsymbol{x} \;\; \boldsymbol{x}\boldsymbol{Q}_\beta^{(i)}). \end{aligned} \tag{5.6}$$

This time the received block $\boldsymbol{v}$ is

$$\begin{aligned} \boldsymbol{v} &= \boldsymbol{s} + (\boldsymbol{\Psi}_0 \;\; \boldsymbol{\Psi}_1) \\ &= (\boldsymbol{x} + \boldsymbol{\Psi}_0 \;\; \boldsymbol{x}\boldsymbol{Q}_\beta^{(i)} + \boldsymbol{\Psi}_1). \end{aligned} \tag{5.7}$$

In the receiver, as shown in Figure 5.4, the jth detector performs an

inverse transformation on the information-bearing part of the received signal. The output block of the inverse transformation, denoted by $\boldsymbol{r}^{(j)}$, is given by

$$\begin{aligned} \boldsymbol{r}^{(j)} &= F_j^{-1}(\boldsymbol{x}\boldsymbol{Q}_\beta^{(i)} + \boldsymbol{\Psi}_1) \\ &= \boldsymbol{x}\boldsymbol{Q}_\beta^{(i)}(\boldsymbol{Q}_\beta^{(j)})^{-1} + \boldsymbol{\Psi}_1(\boldsymbol{Q}_\beta^{(j)})^{-1} \\ &= \boldsymbol{x}\boldsymbol{Q}_\beta^{(i,j)} + \boldsymbol{\Psi}_1(\boldsymbol{Q}_\beta^{(j)})^{-1} \end{aligned} \tag{5.8}$$

where $\boldsymbol{Q}_\beta^{(i,j)} = \boldsymbol{Q}_\beta^{(i)}(\boldsymbol{Q}_\beta^{(j)})^{-1}$. Finally, the detector output $y^{(j)}$ is the correlation between $\boldsymbol{r}^{(j)}$ and the reference part of the received block, that is,

$$\begin{aligned} y^{(j)} &= \boldsymbol{r}^{(j)}(\boldsymbol{x} + \boldsymbol{\Psi}_0)^T \\ &= \boldsymbol{x}\boldsymbol{Q}_\beta^{(i,j)}\boldsymbol{x}^T + \boldsymbol{x}\boldsymbol{Q}_\beta^{(i,j)}\boldsymbol{\Psi}_0^T + \boldsymbol{\Psi}_1(\boldsymbol{Q}_\beta^{(j)})^{-1}\boldsymbol{x}^T \\ &\quad + \boldsymbol{\Psi}_1(\boldsymbol{Q}_\beta^{(j)})^{-1}\boldsymbol{\Psi}_0^T. \end{aligned} \tag{5.9}$$

From (5.9) it can be seen that the value of $y^{(j)}$ is small when $j \neq i$, and is large when $j = i$. The decision circuit can then identify the symbol according to this.

5.4 System Performance

In this section we study the performance of the proposed M-ary system by computer simulations. The map $T_2(x)$ in (1.3) is used to generate the chaotic samples. Denoting the number of chaotic samples transmitted for

one bit and the variance of the chaotic samples by γ and σ_s^2, respectively, the average bit energy (E_b) can be shown equal to $\gamma\sigma_s^2$. Also, the spreading factor of one symbol equals $\gamma \log_2 M$. In our case, the spreading factor is β and 2β in the coherent and noncoherent system, respectively. Thus E_b can be adjusted in terms of σ_s, β and M. System performance is shown by plotting the bit error rate (BER) against the average-bit-energy to noise-power-spectral-density ratio (E_b/N_0). For M-ary systems, the symbols are converted back to binary bits when measuring the BER.

We compare the performances of our M-ary systems for different values of M. For a fair comparison, we keep the number of chaotic samples used per bit to be identical in all cases, and we set $\gamma = 40$. Figures 5.5 and 5.6 show the simulation results for the coherent and noncoherent M-ary systems, respectively. As would be expected, the performance of the coherent system is superior to that of the noncoherent system. From the figures it can be observed that the performance of the M-ary system improves as M increases from 2 to 128. This shows that the use of an M-ary communication scheme can enhance the utilization of the channel. In Figure 5.7, the coherent system with $M = 128$ is compared with the conventional coherent M-ary FSK system [8] with the same M. We find that their performances are quite similar, with the M-ary FSK system slightly better. This is because in FSK systems orthogonal carriers are used to represent the digital symbols, while the

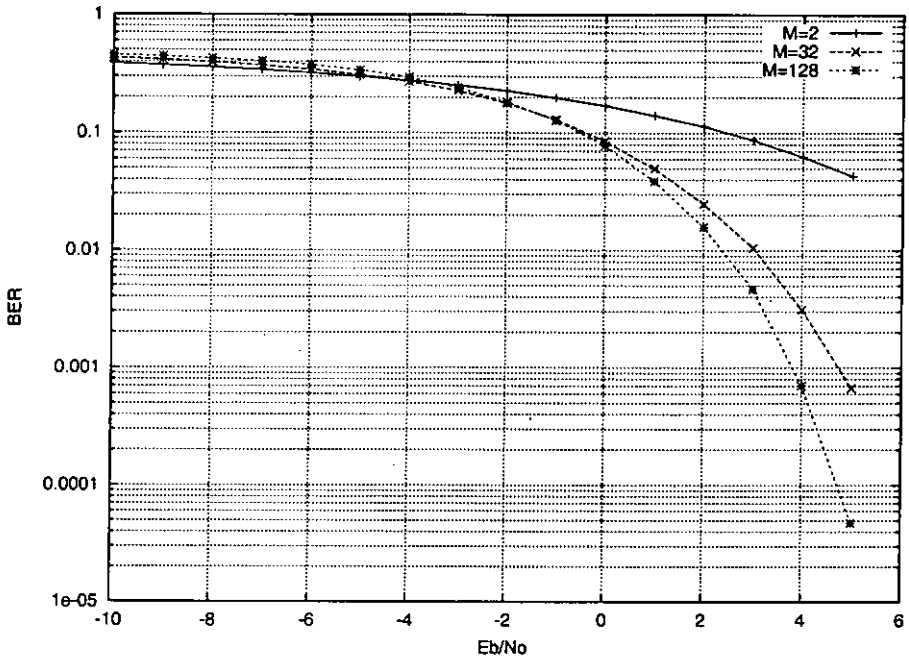

Figure 5.5: Bit error rates versus E_b/N_0 of the coherent M-ary chaos-based communication systems.

chaotic signal blocks used in the M-ary chaos communication system are only nearly orthogonal when the spreading factor is large enough.

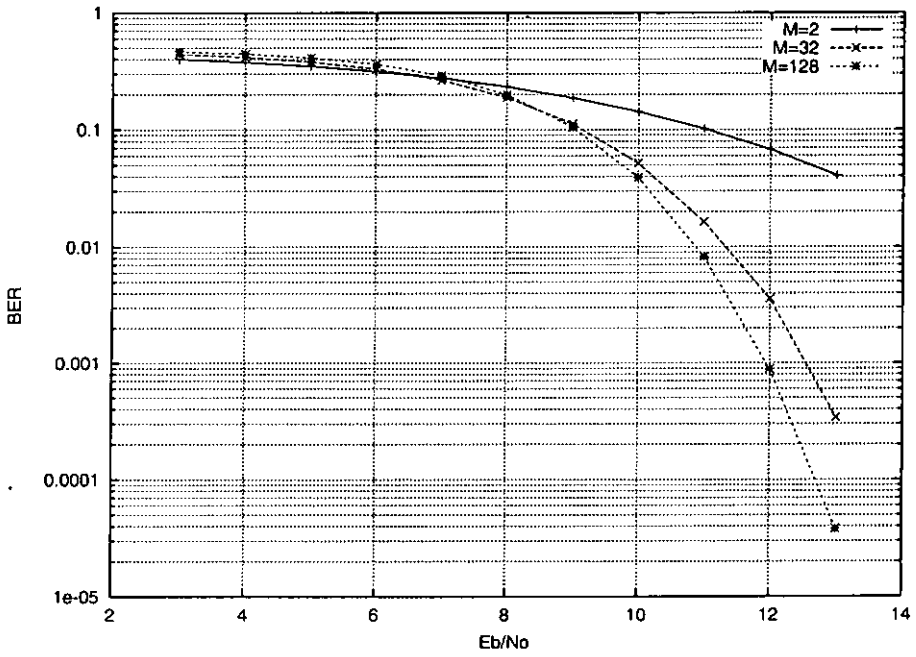

Figure 5.6: Bit error rates versus E_b/N_0 of the noncoherent M-ary chaos-based communication systems.

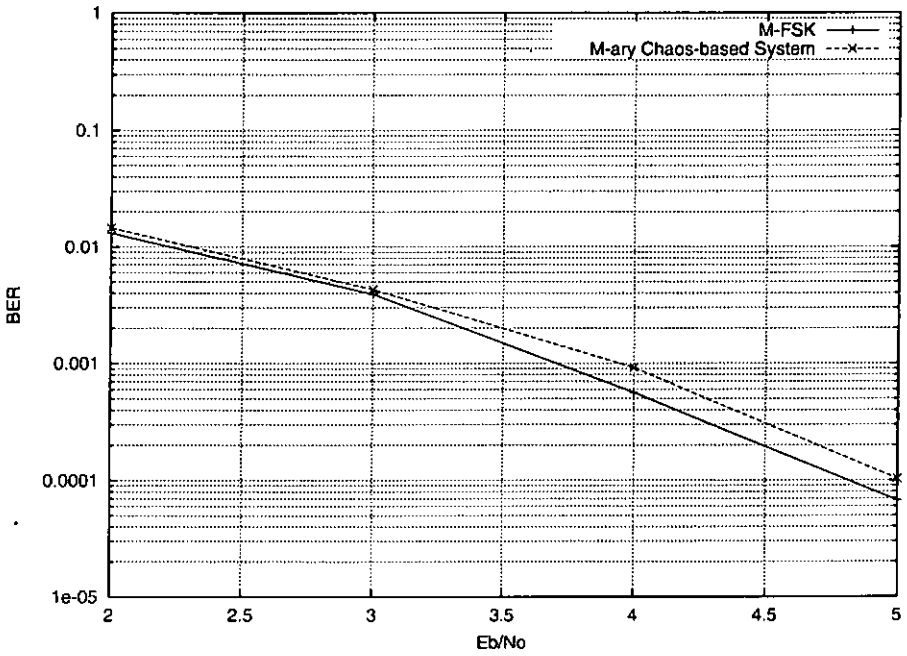

Figure 5.7: Bit error rates performances of the coherent M-ary chaos-based communication system and the conventional M-ary FSK system. $M = 128$ for both cases.

Chapter 6

Conclusions

In this thesis, we have discussed a few methods for detecting a chaotic attractor by observing its orbit as a signal. Among the orbit characteristics that could be used for identifying the chaotic dynamics behind, the return map seems to be more robust than the others in the presence of noise. It provides reasonable performance as a demodulation method for noncoherent CSK. In fact, the return map method is expected to be better because it makes use of the complete information about the dynamical systems that generate the signals. If the initial conditions of the dynamical systems are also known, coherent detection can be achieved. Without the initial conditions, the complete knowledge of the dynamics offers the second best solution, in the scenario of noncoherent CSK. Optimal detection can be achieved by the maximum likelihood approach expressed in (2.4). Unfortunately, practical implementations of this method are

still to be improved. Due to the sensitivity of the chaotic dynamics to the initial condition, the required step size in the numerical integration in (2.4) is unreasonably small. Therefore, the quest for better and more practical algorithms is still under way.

One major achievement of this thesis is the improvement of DCSK system security with the use of permutations. In this aspect, it is clear that the probability of detection by unintended listeners is lowered, but we have not inspected the system security against attackers with certain knowledge about the system. Analysis of such attacks is required before we can claim that the system is secure. Also, this improvement of security increases the difficulty for the intended demodulator to maintain signal block synchronization with the modulator. Further research may be conducted in this direction.

With the use of permutations, two approaches for improving the utilization of channel in chaos communication are presented in this thesis. In both the multiple access P-DCSK system and the M-ary communication system, strict orthogonality is not achieved for the concerned signals. System performances are thus affected, especially in the multiple access P-DCSK system, in which the BER increases rapidly with the number of users. The generation of orthogonal chaotic signals may be an important task in future research.

In this thesis, a channel of AWGN is always assumed in the system

models. Other types of channel defects such as multipath fading can be investigated in the future.

Bibliography

[1] E.N. Lorenz, *The essence of chaos,* London: UCL Press, 1993.

[2] E.N. Lorenz, "Deterministic nonperiodic flow," *Journal of the Atmospheric Sciences,* vol. 20, no. 2, pp. 130–141, 1963.

[3] T.Y. Li and J.A. Yorke, "Period three implies chaos," *American Mathematical Monthly,* vol. 82, no. 10, pp. 985–992, 1975.

[4] R. Brown and L.O. Chua, "Clarifying chaos: Examples and counterexamples," *International Journal of Bifurcation and Chaos,* vol. 6, no. 2, pp. 219–249, 1996.

[5] R. Brown and L.O. Chua, "Clarifying chaos II: Bernoulli chaos, zero Lyapunov exponents and strange attractors," *International Journal of Bifurcation and Chaos,* vol. 8, no. 1, pp. 1–32, 1998.

[6] R. Brown and L.O. Chua, "Clarifying chaos III: Chaotic and stochastic processes, chaotic resonance, and number theory," *International Journal of Bifurcation and Chaos,* vol. 9, no. 5, pp. 785–803, 1999.

[7] R.L. Devaney, *An introduction to chaotic dynamical systems,* Reading, Mass.: Addison-Wesley Pub. Co., 1989.

[8] S.S. Haykin, *Communication systems,* New York: Wiley, 2001.

[9] A.J. Viterbi, *CDMA: Principles of spread spectrum communication,* Reading, Mass.: Addison-Wesley Pub. Co., 1995.

[10] M.P. Kennedy, R. Rovatti and G. Setti (eds.), *Chaotic electronics in telecommunications,* Boca Raton FL: CRC Press, 2000.

[11] F.C.M. Lau and C.K. Tse, *Chaos-based digital communication systems,* Berlin; New York: Springer, 2003.

[12] A. Abel and W. Schwarz, "Chaos-communication – Principles, schemes, and system analysis," *Proceedings of the IEEE,* vol. 90, no. 5, pp. 691–710, 2002.

[13] M. Hasler and T. Schimming, "Optimal and suboptimal chaos receivers," *Proceedings of IEEE,* vol. 90, no. 5, pp. 733–746, 2002.

[14] L.M. Pecaro and T.L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters,* vol. 64, no. 8, pp. 821–824, 1990.

[15] G. Kolumbán, M.P. Kennedy and L.O. Chua, "The role of synchronization in digital communications using chaos – Part II: Chaotic

modulation and chaotic synchronization," *IEEE Transactions on Circuit and Systems - I,* vol. 45, no. 11, pp. 1129–1140, 1998.

[16] A. Okşaşoğlu and T. Akgui, "A linear inverse system approach in the context of chaotic communication," *IEEE Transactions on Circuit and Systems - I,* vol. 44, no. 1, pp. 75–79, 1997.

[17] H. Leung and J. Lam, "Design of demodulator for the chaotic modulation communication system," *IEEE Transactions on Circuit and Systems - I,* vol. 44, no. 3, pp. 262–267, 1997.

[18] M.P. Kennedy and G. Kolumbán, "Digital communication using chaos" in *Controlling chaos and bifurcation in engineering systems,* G. Chen (ed.), Boca Raton FL: CRC Press, pp. 477–500, 2000.

[19] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuit and Systems Magazine,* vol. 1, no. 3, pp. 6–21, 2001.

[20] G. Kolumbán, M.P. Kennedy, Z. Jákó and G. Kis, "Chaotic communications with correlator receivers: Theory and performance limits," *Proceedings of IEEE,* vol. 90, no. 5, pp. 711–732, 2002.

[21] A. Fleming-Dahl, "A chaotic system that communicates through unlimited propagation losses and/or transmitter gain," in *Proceedings, IEEE-ICC'2000,* vol. II, New Orleans, USA, Jun. 18–22, 2000, pp. 783–790.

[22] T. Geisel and V. Fairen, "Statistical properties of chaos in Chebyshev maps," *Physics Letters,* vol. 105A, no. 6, pp. 236–266, 1984.

[23] H. Dedieu and A. Kisel, "Communications with chaotic time series: probabilistic methods for noise reduction," *International Journal of Circuit Theory and Applications,* vol. 27, no. 6, pp. 577–587, 1999.

[24] A. Kisel, H. Dedieu and T. Schimming, "Maximum likelihood approaches for noncoherent communications with chaotic carriers," *IEEE Transactions on Circuit and Systems - I,* vol. 48, no. 5, pp. 533–542, 2001.

[25] C.K. Tse, F.C.M. Lau, K.Y. Cheong and S.F. Hau, "Return-map-based approaches for noncoherent detection in chaotic digital communications," *IEEE Transactions on Circuit and Systems - I,* vol. 49, no. 10, pp. 1495–1499, 2002.

[26] C.K. Tse and F.C.M. Lau, "A return map regression approach for noncoherent detection in chaotic digital communications," *International Journal of Bifurcation and Chaos,* vol. 13, no. 3, pp. 685–690, 2003.

[27] G. Kolumbán, "Exact analytical expression for the noise performance of FM-DCSK," in *Proceedings, NOLTA'2000,* Dresden, Germany, Sept. 17–21, 2000, pp. 735–738.

[28] M.P. Kennedy and G. Kolumbán, "Elaboration of system specification for a WLAN FM-DCSK telecommunications system," in *Proceedings, NDES'2000,* Catania, Italy, May 18–20, 2000, pp. 160–164.

[29] G. Kis, "Evaluation of interference performance of FM-DCSK communications system," in *Proceedings, NDES'2000,* Catania, Italy, May 18–20, 2000, pp. 204–207.

[30] G. Heidari-Bateni and C.D. McGillem, "A chaotic direct-sequence spread-spectrum communication system," *IEEE Transactions on Communications,* vol. 42, no. 2/3/4, pp. 1524–1527, 1994.

[31] M. Itoh, "Chaos-based spread spectrum communication systems," in *Proceedings, IEEE–ISIE'1998,* vol. II, Pertoria, South Africa, Jul. 7–10, 1998, pp. 430–435.

[32] S. Callegari, M. Dondini and G. Setti, "Adaptive median thresholding for the generation of high-data-rate random-like unpredictable binary sequences with chaos," in *Proceedings, IEEE–ISCAS'2001,* vol. III, Sydney, Australia, May 6–9, 2001, pp. 221–224.

[33] F. Agnelli, G. Mazzini, R. Rovatti and G. Setti, "A first experimental verification of optimal MAI reduction in chaos-based DS-CDMA systems," in *Proceedings, IEEE–ISCAS'2001,* vol. III, Sydney, Australia, May 6–9, 2001, pp. 137–140.

[34] T. Yang and L.O. Chua, "Chaotic digital code-division multiple access (CDMA) communication systems," *International Journal of Bifurcation and Chaos,* vol. 7, no. 12, pp. 2789–2805, 1997.

[35] J. Schweizer and M. Hasler, "Multiple access communications using chaotic signals," in *Proceedings, IEEE–ISCAS'1996,* vol. III, Atlanta, USA, May 12–15, 1996, pp. 108–111.

[36] F.C.M. Lau, M.M. Yip, C.K. Tse and S.F. Hau, "A multiple-access technique for differential chaos shift keying," *IEEE Transactions on Circuit and Systems - I,* vol. 49, no. 1, pp. 96–103, 2002.

[37] W.M. Tam, F.C.M. Lau and C.K. Tse, "Analysis of bit error rates for multiple access CSK and DCSK communication systems," *IEEE Transactions on Circuit and Systems - I,* vol. 50, no. 5, pp. 702–707, 2003.

[38] G. Kolumbán, M.P. Kennedy and G. Kis, "Multilevel differential chaos shift keying," in *Proceedings, NDES'1997,* Moscow, Russia, Jun. 26–27, 1997, pp. 191–196.

[39] B.B. Mandelbrot, *The fractal geometry of nature,* New York: W.H. Freeman, 1983.

[40] K.T. Alligood, T.D. Sauer and J.A. Yorke, *Chaos: An introduction to Dynamical systems,* New York: Springer, 1996.

[41] E. Ott, *Chaos in dynamical systems,* Cambridge: Cambridge University Press, 1993.

[42] F.C.M. Lau, K.Y. Cheong and C.K. Tse, *Permutation-based DCSK and multiple access DCSK systems, IEEE Transactions on Circuit and Systems - I,* vol. 50, no. 6, pp. 733–742, 2003.

[43] G.W. Stewart, *Matrix algorithms,* Philadelphia: Society for Industrial and Applied Mathematics, 1998.

[44] S.M. Ross, *Introduction to probability models,* New York: Academic Press, 1993.

[45] G. Kolumbán, *Theoretical Noise Performance of Correlator-Based Chaotic Communications Schemes, IEEE Transactions on Circuit and Systems - I,* vol. 47, no. 12, pp. 1692–1701, 2000.